RESEARCH PROPOSAL

Background Communication complexity seeks to understand complexity of computation by characterizing the amount of communication that must occur to compute the output of a function whose inputs are distributed among separate parties communicating on a broadcast channel. Aside from seeing only a portion of the input, players have unlimited computational resources. In the two-party variant, players Alice and Bob are given inputs x and y, respectively, each of size n. Their task is to jointly compute the output of some function $f(x,y)$ by following a protocol Π. At each step of the computation, the protocol dictates whose turn it is to send a message and what message they will send as a function of their input, previous messages sent, and perhaps shared and/or private randomness. In the multiparty ("number-on-forehead") variant, players 1 through t are assigned inputs $x_1,\ldots,x_t$, again of size n, but now can see all inputs except their own. In both models, the cost of a protocol as a function of n is the worst-case number of bits that must be sent f. The communication cost of a function is the cost of the best protocol for f. See [5] for full definitions.

Communication complexity is of some inherent interest, but more important is that bounds in the communication model are often amenable both to tractable proof and ready transfer to other models. In addition to applications where communication is obviously relevant (e.g. distributed algorithms), results have been transfered to e.g. space bounds for data stream algorithms, circuit size and depth lower bounds, time-space trade-offs for Turing machines, area-time tradeoffs for VLSI, and communication lower bounds for combinatorial auction algorithms.

As in much of complexity, reductions between problems are common, so research tends to focus on a few particular functions. In particular, we will here often be concerned with the set-disjointness function DISJ, wherein players treat their inputs as characteristic functions of subsets of $\{1,\ldots,n\}$ and must output 1 if and only if their sets are disjoint. We also often express DISJ in composed form as $\text{DISJ} = \text{OR} \circ \text{AND}$. DISJ plays a role for communication similar to that of SAT in much of complexity. In addition to its importance within communication complexity, lower bounds for two-party DISJ directly imply lower bounds for communication in combinatorial auctions, and are used in [1] to prove striking new barrier results. Lower bounds for multiparty DISJ directly imply exponential size lower bounds for a wide class of proof systems not presently accessible by any other methods, and work on multiparty disjointness lower bounds has also resulted in techniques that hold promise for separating NP from ACC^0, an important circuit class.

Proposed Work The two-party complexity of DISJ is well-understood, but a deep understanding of its multiparty complexity remains an open problem. I propose a program of attacks in multiparty communication complexity, with connections to DISJ.

Protocols for Composed Functions As hinted above, finding a function in NP that requires $(\log n)^{\Omega(1)}$ communication for $(\log n)^{\Omega(1)}$ players would separate NP and ACC^0. [2] rules out a large class of candidate functions, including DISJ, by supplying efficient protocols for $t > 1 + \log n$ players for functions of the form $f \circ g$, where f satisfies a strong symmetry condition.

I intend to explore protocols for similar functions where we relax the symmetry condition on f. In [2], one class of such functions is proposed as a target for potential generalizations, providing a logical place to start an attack. Thus, we would begin by attempting to extend the protocols in [2]: I conjecture and intend to verify that there exist both nontrivial extensions of their protocols and perhaps also nontrivial reductions to them from less-symmetric functions. Along with improving our arsenal of communication protocols, a deeper understanding of the extent of the applicability of their techniques will aid in the search for hard functions to accomplish the separation of ACC^0 and NP.

Relations Among Multiparty Lower-Bound Techniques Essentially all known lower-bound techniques in the two-player model are expressible as optima of particular linear programs. The authors of [4] introduce a new LP-based lower-bound technique and employ these LP characterizations to prove their technique optimal among almost all known techniques. Thus, (with the exception of new information-theoretic bounds), relationships among two-player bounds are well-understood.

On the other hand, recent work in [6] has vastly improved existing lower bounds on multiparty DISJ, but at the cost of significant technical complication. This and the success of the LP based project on the two-player side motivate my proposal to investigate LP formulations of and relationships among multiparty lower-bound techniques. The first question is whether existing multiparty lower bounds can be expressed as optima of LPs; an answer to this question (at least for simple techniques) seems well within reach. With such LPs available, we will be able to attempt both new proofs of relationships between existing methods and a search for new multiparty techniques by manipulating LP constraints. Additionally, LP formulations of lower bounds are likely deepen our understanding of the applications of such techniques to DISJ and related functions; indeed, some of the recent improvements in bounds for multiparty DISJ already rely on some LP and polynomial duality arguments (for example [3]), a hint that further work to formulate bounds in these terms may prove fruitful. A deepening of our understanding here may also result in progress towards finding candidate functions for the separation discussed above.

Broader Impacts I will briefly discuss ways in which I will use my research experience to effect wider benefit. I have mentioned elsewhere in this application my intention to continue and expand my current outreach activities. Though I am interested in bringing a wide variety of math and computer science to schools, I have a soft spot for my own field. Complexity also has the advantage that the intuitions behind many of its best results and hardest problems can be given to high-schoolers. To that end, I am interested in developing a publicly-available complexity curriculum at the high-school level, which could be used by outreach programs and high-school teachers to introduce students to mathematics far more interesting and just as intuitive as AP calculus.

I am also interested in theory of computation curriculum design at the college level. It is all too common to see undergraduate theory of computation courses stuck in the eighties, never escaping the tyranny of NP-completeness reductions. Such courses fail to expose students to the depth of understanding that has been achieved in the last twenty-five years by viewing computation through lenses besides the Turing machine: proofs, circuits, polynomials, etc. Theory can be among the most exciting courses in the undergraduate curriculum if only we devote attention to at very least intuitive accounts of e.g., IP = PSPACE, or Merlin-Arthur games, or the PCP theorems, or even communication complexity. I will take advantage of opportunities to lead undergraduate topics seminars aiming to expose students to concepts closer to the frontiers of complexity (or at very least from a more recent decade than NP completeness) as early as mathematically possible.

References

[1] S. Aaronson and A. Wigderson. Algebrization: A new barrier in complexity theory. *STOC*, 2008.

[2] A. Ada, A. Chattopadhyay, O. Fawzi, and P. Nguyen. The nof multiparty communication complexity of composed functions. *ECCC*, TR11-155.

[3] P. Beame and T. Huynh. Multiparty communication complexity and threshold circuit size of ACC^0. *FOCS*, 2009.

[4] R. Jain and H. Klauck. The partition bound for classical communication complexity and query complexity. *IEEE CCC*, 2010.

[5] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1st edition, 1997.

[6] A. Sherstov. The multiparty complexity of set disjointness. *STOC*, 2012.