On Query-to-Communication Lifting for Quantum Adversaries

Anurag Anshu
University of California, Berkeley
anuraganshu@berkeley.edu

Shalev Ben-David
University of Waterloo
shalev.b@uwaterloo.ca

Srijita Kundu
National University of Singapore
srijita.kundu@u.nus.edu

Communication complexity is an important model of computation with deep connections to many parts of theoretical computer science [KN96]. In communication complexity, two parties, called Alice and Bob, receive inputs x and y from sets $\mathcal{X}$ and $\mathcal{Y}$ respectively, and wish to compute some joint function $F\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ on their inputs. Alice and Bob cooperate together, and their goal is to minimize the number of bits they must exchange before determining $F(x,y)$.

Recently, a lot of attention has been devoted to connections between communication complexity and query complexity. In particular, query-to-communication "lifting" theorems are powerful tools which convert lower bounds in query complexity into lower bounds in communication complexity in a black-box manner. Since query lower bounds are typically much easier to prove than communication lower bounds, these tools are highly useful for the study of communication complexity, and often come together with new communication complexity results (such as separations between different communication complexity models). For example, see [Göö15; GLM+16; GPW18; GPW20].

Lifting theorems are known for many models of computation, including deterministic [GPW18] and randomized [GPW20] algorithms. Notably, however, a lifting theorem for quantum query complexity is not known; the closest thing available is a lifting theorem for approximate degree (also known as the polynomial method), which lifts to approximate logrank [She11]. This allows quantum query lower bounds proved via the polynomial method to be turned into quantum communication lower bounds, but a similar statement is not known even for the positive-weight quantum adversary method [Amb02; ŠS06].

In this work, we investigate lifting theorems for the adversary method and related models.

Lifting the classical adversary

Our first contribution is a lifting theorem for the classical adversary bound $\mathrm{CAdv}(f)$. We lift it to a lower bound on randomized communication complexity using a constant-sized gadget.

Theorem 1. *There is an explicitly given function $G\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ such that for any (possibly partial) Boolean function f,*

$$\mathrm{R}^{\mathrm{CC}}(f \circ G) = \Omega(\mathrm{CAdv}(f)).$$

We note that [GP18] provided a lifting theorem that has a similar form, only with the measure $\mathrm{cbs}(f)$ in place of $\mathrm{CAdv}(f)$. To compare the two theorems, we should compare the two query measures. We have the following theorem.

Lemma 2. *For all (possibly partial) Boolean functions f, $\mathrm{CAdv}(f) = \Omega(\mathrm{cbs}(f))$. Moreover, there is a family of total functions f for which $\mathrm{CAdv}(f) = \Omega(\mathrm{cbs}(f)^{3/2})$.*

Lemma 2 says that $\mathrm{CAdv}(f)$ is a strictly stronger lower bound technique than $\mathrm{cbs}(f)$, and hence Theorem 1 is stronger than the lifting theorem of [GP18] (though our constant-sized gadget is larger).

We note that the lifting theorem of [GP18] for the measure $\mathrm{cbs}(f)$ also works when f is a *relation*, which is a more general setting than partial functions; indeed, most of their applications for the lifting theorem were for relations f rather than functions. We extend Theorem 1 to relations as well, and also show that $\mathrm{CAdv}(f) = \Omega(\mathrm{cbs}(f))$ for all relations. In fact, it turns out that for partial functions, $\mathrm{CAdv}(f)$ is equal to a fractional version of $\mathrm{cbs}(f)$, which we denote $\mathrm{cfbs}(f)$; however, for relations, $\mathrm{CAdv}(f)$ is a stronger lower bound technique than $\mathrm{cfbs}(f)$ (which in turn is stronger than $\mathrm{cbs}(f)$).

Lifting quantum measures

Our first quantum result says that $\mathrm{CAdv}(f)$ lifts to a lower bound on bounded-round quantum communication protocols. This may seem surprising, as $\mathrm{CAdv}(f)$ does not lower bound quantum algorithms in query complexity; however, one can show that $\mathrm{CAdv}(f)$ does lower bound *non-adaptive* quantum query complexity, or even quantum query algorithms with limited adaptivity. This motivates the following result.

Theorem 3. *There is an explicitly given function $G\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ such that for any (possibly partial) Boolean function f,*

$$\mathrm{QCC}^r(f \circ G) = \Omega(\mathrm{CAdv}(f)/r^2).$$

Here $\mathrm{QCC}^r(\cdot)$ denotes the quantum communication complexity for an r-round quantum protocol with shared entanglement.

We note that since any r-round protocol has communication cost at least r, we actually get a lower bound of $\mathrm{CAdv}(f)/r^2 + r$. Minimizing over r yields a lower bound of $\mathrm{CAdv}(f)^{1/3}$ even on unbounded-round protocols. This may not seem very useful, since $\mathrm{CAdv}(f)^{1/3}$ is smaller than $\widetilde{\deg}(f)$, a measure we know how to lift [She11]. However, we can generalize this result to relations. For relations, we do not know how to compare $\mathrm{CAdv}(f)^{1/3}$ to $\widetilde{\deg}(f)$, and therefore our lifting theorem gives something new.

Corollary 4. *There is an explicitly given function $G\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ such that for any relation f,*

$$\mathrm{QCC}(f \circ G) = \Omega(\mathrm{CAdv}(f)^{1/3}).$$

We next turn our attention to lower bounding unbounded-round quantum communication protocols by lifting a quantum adversary method. Instead of aiming for the positive-weight adversary bound, we instead work with a simplified version, studied in [ABK+20], which we denote $\mathrm{Adv}_1(f)$. This measure is a restriction of Adv to a pairs of inputs with a single bit of difference.

We have $\mathrm{Adv}_1(f) \le \mathrm{Adv}(f)$, and [ABK+20] showed that $\mathrm{Adv}_1(f) = O(\widetilde{\deg}(f))$. However, their proof of the latter fact is tricky, and we do not use it here; we give a direct lifting of $\mathrm{Adv}_1(f)$ (under a certain assumption), and we argue that the techniques we use are likely to generalize to lifting $\mathrm{Adv}(f)$ in the future.

We prove the following theorem.

Theorem 5. *For any (possibly partial) Boolean function f and any communication function G which contains both AND_2 and OR_2 as subfunctions, we have*

$$\mathrm{QCC}(f \circ G) = \Omega(\mathrm{Adv}_1(f)\,\mathrm{QICZ}(G)).$$

This also holds for relations f.

At first glance, this theorem might look very strong: not only does it lift the simplified adversary bound for a single gadget G, it even does so for all G with a dependence on G. Unfortunately, there is a catch: the measure $\mathrm{QICZ}(G)$ may be 0 for some communication functions G. In fact, we cannot rule out the possibility that $\mathrm{QICZ}(G) = 0$ for *all* communication functions G, in which case Theorem 5 does not say anything. On the other hand, note that if $\mathrm{QICZ}(G) > 0$ for even a single function G, then Theorem 5 gives a lifting theorem for $\mathrm{Adv}_1(f)$ with a constant-sized gadget, which works even for relations (since that single G can have no dependence on the input size of f).

We give an interpretation of the measure $\mathrm{QICZ}(G)$ in terms of a cryptographic primitive called secure 2-party computation. In such a primitive, Alice and Bob want to compute a function G on their inputs x and y, but they do not want to reveal their inputs to the other party. Indeed, Alice wants to hide everything about x from Bob and Bob wants to hide everything about y from Alice, with the exception of the final function value $G(x, y)$ (which they are both expected to know at the end of the protocol). We also seek information-theoretic security: there are no limits on the computational power of Alice and Bob.

Secure 2-party computation is known to be impossible in general. However, in our case, we care about an "honest but curious" version of the primitive, in which Alice and Bob trust each other to execute the protocol faithfully, but they still do not trust each other not to try to learn the others' input. In the quantum setting, it is a bit difficult to define such an honest-but-curious model: after all, if Alice and Bob are honest, they might be forbidden by the protocol from ever executing intermediate measurements, and the protocol might even tell them to "uncompute" everything except for the final answer, to ensure all other information gets deleted. Hence it would seem that honest parties can trivially do secure 2-party computation.

However, we are interested in a setting in which Alice and Bob measure the amount of communication transmitted using the quantum information cost, denoted QIC, of the protocol, a measure which was introduced in [Tou15]. Alice and Bob want a protocol Π such that for any distribution μ that has support only on 0-inputs (or only on 1-inputs), $\mathrm{QIC}(\Pi, \mu)$ is small. This will ensure that Alice and Bob learn nothing about each others' inputs when conditioned on the output of the function. The question then becomes: does such a secure protocol Π exists for computing any fixed communication function G? If so, we can lift $\mathrm{Adv}_1(f)$ with a constant-sized gadget, and our techniques have the potential to generalize to other adversary methods.

New query relations

Finally, our study of the classical adversary bound led to some new relations in query complexity that are likely to be of independent interest.

Theorem 6. *For all (possibly partial) Boolean functions f,*

$$\mathrm{Adv}(f) = O(\widetilde{\deg}(f)^2).$$

Here $\widetilde{\deg}(f)$ is the approximate degree of f to bounded error.

Theorem 7. *For all (possibly partial) Boolean functions f, $\widetilde{\deg}_\epsilon(f) \geq \sqrt{(1-2\epsilon)\,\mathrm{CAdv}(f)}/\pi$.*

This version of the theorem is stronger, since $\mathrm{Adv}(f) \leq \mathrm{CAdv}(f)$. Finally, we prove a quadratic relationship between the classical and quantum (positive-weight) adversary bounds.

Theorem 8. *For all (possibly partial) Boolean functions f, $\mathrm{Adv}(f) \leq \mathrm{CAdv}(f) \leq 2\,\mathrm{Adv}(f)^2$.*

We note that all of these new relations hold even for partial functions. This is unusual in query complexity, where most relations hold only for total functions, and where most pairs of measures can be exponentially separated in the partial function setting.

References

[ABK+20] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem. Preprint, 2020. arXiv: 2010.12629 (p. 2).

[Amb02] Andris Ambainis. Quantum Lower Bounds by Quantum Arguments. *Journal of Computer and System Sciences* (2002). Previous version in STOC 2000. DOI: 10.1006/jcss.2002.1826. arXiv: quant-ph/0002066 (p. 1).

[GLM+16] Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles Are Nonnegative Juntas. *SIAM Journal on Computing* (2016). Previous version in STOC 2015. DOI: 10.1137/15M103145X. ECCC: 2014/147 (p. 1).

[Göö15] Mika Göös. Lower bounds for clique vs. independent set. *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 2015. DOI: 10.1109/FOCS.2015.69. ECCC: 2015/012 (p. 1).

[GP18] Mika Göös and Toniann Pitassi. Communication Lower Bounds via Critical Block Sensitivity. *SIAM Journal on Computing* (2018). Previous version in STOC 2014. DOI: 10.1137/16m1082007. arXiv: 1311.2355 (pp. 1, 2).

[GPW18] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic Communication vs. Partition Number. *SIAM Journal on Computing* (2018). Previous version in FOCS 2015. DOI: 10.1137/16M1059369. ECCC: 2015/050 (p. 1).

[GPW20] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-Communication Lifting for BPP. *SIAM Journal on Computing* (2020). Previous version in FOCS 2017. DOI: 10.1137/17m115339x. arXiv: 1703.07666 (p. 1).

[KN96] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1996. ISBN: 9780511574948. DOI: 10.1017/cbo9780511574948 (p. 1).

[She11] Alexander A. Sherstov. The Pattern Matrix Method. *SIAM Journal on Computing* (2011). Previous version in STOC 2008. DOI: 10.1137/080733644. arXiv: 0906.4291 (pp. 1, 2).

[ŠS06] Robert Špalek and Mario Szegedy. All Quantum Adversary Methods are Equivalent. *Theory of Computing* (2006). Previous version in ICALP 2005. DOI: 10.4086/toc.2006.v002a001. arXiv: quant-ph/0409116 (p. 1).

[Tou15] Dave Touchette. Quantum Information Complexity. *Proceedings of the 47th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*. 2015. DOI: 10.1145/2746539.2746613. arXiv: 1404.3733 (p. 3).