Tight Limits on Nonlocality from Nontrivial Communication Complexity

Noah Shutty *†‡ Mary Wootters *§ Patrick Hayden *†¶

November 20, 2020

Note: A preliminary version of this paper was submitted to QIP 2019 with much weaker results. Afterwards we significantly developed our ideas to obtain stronger new results that addressed the original question. Rather than writing a new paper, we decided to simply update the manuscript as the scientific motivation was the same and the old results were subsumed by the new results. The present version of this work appeared in FOCS 2020. We mention the results from the original manuscript in more detail in Section 1.2 of our Technical Manuscript.

A proposed information-theoretic axiom for distinguishing quantum mechanics from incorrect theories of physics is that "communication complexity is nontrivial". That is, two parties with inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ respectively should not be able to compute arbitrary functions $f(x, y)$ with high probability, using only a constant amount of communication (independent of n). Such a requirement is satisfied by quantum mechanics, and is also known to rule out superquantum success at certain *nonlocal games.* For example, consider the famous *CHSH game.*[1] The two players, Alice and Bob, cannot communicate. Alice and Bob receive independent random bits x and y respectively. Their goal is to output bits a and b, respectively, so that $a \oplus b = x \wedge y$.

In a classical world, Alice and Bob can win the CHSH game with probability 3/4 (*e.g.* by outputting $a, b = 0$) and cannot do any better; thus the classical value of the CHSH game is $\omega_C(CHSH) = \frac{3}{4}$. If Alice and Bob have access to any *nonsignalling* correlation—that is, they can produce correlated bits a and b in any way they like as long as they do not gain the ability to communicate—then they can win the CHSH game with probability 1; we say that the nonsignalling value of the CHSH game is $\omega_{NS}(CHSH) = 1$. If instead Alice and Bob share quantum entanglement, they can do something in between ω_C and ω_{NS}: it turns out that the quantum value of the CHSH game is [Cir80]

$$\omega_Q(CHSH) = \frac{1}{2} + \frac{1}{\sqrt{8}} \approx 0.8536.$$

†Department of Physics, Stanford University.
‡N.S. was supported in part by NSF DGE-1656518.
§Departments of Computer Science and Electrical Engineering, Stanford University. M.W. was supported in part by NSF CAREER CCF-1844628.

¶P.H. was supported by AFOSR (FA9550-16-1-0082), CIFAR and the Simons Foundation

[1]This game is named after Clauser, Horne, Shimony, and Holt and was introduced implicitly in their paper [CHSH69].

Work of van Dam [vD13], and independently Cleve [Cle], showed that if Alice and Bob could win the CHSH game with probability 1, then communication complexity would become trivial. This was extended by Brassard *et al.* [BBL+06], who showed that if Alice and Bob could win the CHSH game with probability greater than $\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908$ then communication complexity would become trivial. Thus, the axiom "communication complexity is nontrivial" in some sense explains why $\omega_Q(CHSH) < 0.908$. Other works have extended the set of nonlocal correlations known to collapse communication complexity [FWW09, BS09, HR10].

However, so far the axiom "communication complexity is nontrivial" had not pinned down the exact quantum value for any nonlocal game. For example, in the CHSH game, there is a gap between the threshold of approximately 0.908 that Brassard *et al.* obtain and the true quantum value $\omega_Q(CHSH) \approx 0.853$.

We address this question: can the axiom "communication complexity is nontrivial" be used to explain the quantum value of certain nonlocal games? Along the way, we formalize a connection to the theory of reliable computation for (classical) circuits with noisy gates, and our results for nonlocal games correspond to new results for reliable classical computation. We outline our contributions in both areas below.

Contributions

First, we address the extent to which the axiom "communication complexity is nontrivial" can explain the quantum value of nonlocal games.

(1) We exhibit a nonlocal game G, for which

$$\omega_C(G) < \omega_Q(G) < \omega_{NS}(G),$$

and for which the axiom "communication complexity is not trivial" precisely pins down the value $\omega_Q(G)$. Our game G is "complete", in the sense that if communication complexity is trivial in any superquantum theory S, then there is (a version of) our game G so that $\omega_S(G) > \omega_Q(G)$. That is, a superquantum advantage at the game G makes communication complexity trivial and, meanwhile, any universe in which communication complexity is trivial offers a superquantum advantage at the game G.

(2) We provide evidence that the axiom "communication complexity is nontrivial" is in fact *not* sufficient to pin down the quantum value of the CHSH game itself. In more detail, in [BBL+06], Brassard *et al.* use the ability to succeed at the CHSH game essentially as a noisy AND gate. They show that reliable computation is possible when these noisy AND gates are used along with noiseless XOR gates (which correspond to certain local operations for Alice and Bob). This leads to protocols that collapse communication complexity. We show that this strategy cannot be pursued further: the threshold of 0.908 is tight for this model of computation. While this

result is only a barrier against one line of attack, it does suggest that the axiom "communication complexity is nontrivial" may not suffice to explain $\omega_Q(CHSH)$.

As alluded to in our contribution (2) above, there is a connection to reliable computation with noisy gates. In that area, we make the following contributions.

(3) Our contribution (2) above can be seen as a result about reliable computation. Consider the following circuit model with noisy gates. Let $\wedge_\varepsilon$ denote a 2-input AND gate which, for any input produces an incorrect answer with probability ε, and let $\oplus_0$ denote a (noiseless) 2-input XOR gate.[2] Let $\mathcal{C}_\varepsilon$ be the collection of formulas[3] defined on the gate set $\{\wedge_\varepsilon, \oplus_0\}$, where the noise in each $\wedge_\varepsilon$ gate is independent.

Our main technical result is that the noise threshold for reliable computation for this model is precisely $\varepsilon = 1/6$. That is, when $\varepsilon < 1/6$, it is possible to compute any function using a formula in $\mathcal{C}_\varepsilon$ with error probability bounded away from 1/2 for each possible input. On the other hand, for any $\varepsilon \geq 1/6$, there is some function for which this is impossible.

There has been a great deal of work on pinning down noise thresholds for reliable computation. However, most prior work has focused on *symmetric noise,* where the noise rate is the same across all gate types. Extending these results to asymmetric noise—and in particular to include noiseless gates—raises several new challenges.

Beyond our primary motivation in quantum mechanics, we believe that the case of asymmetric gate noise is an independently interesting direction in fault-tolerant computation. We hope that our techniques and results may spur future research in this direction.

(4) We formalize an equivalence between reliable computation and *amplification.* Informally, an amplifier is a function $f : \{0,1\}^d \to \{0,1\}$ so that when f is fed in random bits $x \in \{0,1\}^d$ with a slight bias away from 1/2, the output $f(x)$ amplifies that bias. While a relationship between reliable computation and amplification had been present in prior work, nailing down an equivalence is a bit subtle, and requires considering the *convex hull* of circuit classes; to the best of our knowledge ours is the first work to do this.

Our equivalence between reliable computation and amplification is required to establish the threshold in our contribution (3) above. Further, it leads to the definition and analysis of our game G from contribution (1) whose quantum value is pinned down by the nontriviality of communication complexity.

[2]For a gate g, g_ε refers to a version of g which fails with probability ε.

[3]A *formula* is a circuit where every gate has fan-out 1 (that is, the graph underlying the circuit is a tree and each input variable may appear at one or more leaves of this tree).

References

[ABL+09] Jonathan Allcock, Nicolas Brunner, Noah Linden, Sandu Popescu, Paul Skrzypczyk, and Tamás Vértesi. Closed sets of nonlocal correlations. *Physical Review A*, 80(6):062107, 2009.

[Ara02a] P. K. Aravind. Bell's theorem without inequalities and only two distant observers. *Foundations of Physics Letters*, 15(4):397–405, 2002.

[Ara02b] PK Aravind. A simple demonstration of bell's theorem involving two observers and no probabilities or inequalities. *arXiv preprint quant-ph/0206070*, 2002.

[Ara04] Padmanabhan K Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72(10):1303–1307, 2004.

[BBL+06] Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96(25):250401, 2006.

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005.

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71:022101, Feb 2005.

[BS09] Nicolas Brunner and Paul Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Physical review letters*, 102(16):160403, 2009.

[CHSH69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[Cir80] Boris S Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[Cle] Richard Cleve. personal communication.

[CVDNT98] Richard Cleve, Wim Van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *NASA International Conference on Quantum Computing and Quantum Communications*, pages 61–74. Springer, 1998.

[DO77] Roland L'vovich Dobrushin and SI Ortyukov. Upper bound on the redundancy of self-correcting arrangements of unreliable functional elements. *Problemy Peredachi Informatsii*, 13(3):56–76, 1977.

[DW08] Dejan D Dukaric and Stefan Wolf. A limit on non-locality distillation. *arXiv preprint arXiv:0808.3317*, 2008.

[EP98] William Evans and Nicholas Pippenger. On the maximum tolerable noise for reliable computation by formulas. *IEEE Transactions on Information Theory*, 44(3):1299–1305, 1998.

[ES99] William S Evans and Leonard J Schulman. Signal propagation and noisy circuits. *IEEE Transactions on Information Theory*, 45(7):2367–2373, 1999.

[ES03] William S Evans and Leonard J Schulman. On the maximum tolerable noise of k-input gates for reliable computation by formulas. *IEEE Transactions on Information Theory*, 49(11):3094–3098, 2003.

[FGL18] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 743–754. IEEE, 2018.

[For11] Manuel Forster. Bounds for nonlocality distillation protocols. *Phys. Rev. A*, 83:062114, Jun 2011.

[FWW09] Manuel Forster, Severin Winkler, and Stefan Wolf. Distilling nonlocality. *Physical review letters*, 102(12):120401, 2009.

[Got14] Daniel Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Information & Computation*, 14(15-16):1338–1372, 2014.

[Har01] Lucien Hardy. Quantum theory from five reasonable axioms. *arXiv preprint quant-ph/0101012*, 2001.

[HR10] Peter Høyer and Jibran Rashid. Optimal protocols for nonlocality distillation. *Physical Review A*, 82(4):042118, 2010.

[HW91] Bruce Hajek and Timothy Weller. On the maximum tolerable noise for reliable computation by formulas. *IEEE Transactions on Information Theory*, 37(2):388–391, 1991.

[LPSW07] Noah Linden, Sandu Popescu, Anthony J Short, and Andreas Winter. Quantum nonlocality and beyond: limits from nonlocal computation. *Physical review letters*, 99(18):180502, 2007.

[LVN14] Ben Lang, Tamás Vértesi, and Miguel Navascués. Closed sets of correlations: answers from the zoo. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424029, 2014.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990.

[Mer93] N David Mermin. Hidden variables and the two theorems of john bell. *Reviews of Modern Physics*, 65(3):803, 1993.

[MM16] Markus P Mueller and Lluis Masanes. Information-theoretic postulates for quantum theory. In *Quantum Theory: Informational Foundations and Foils*, pages 139–170. Springer, 2016.

[NGHA15] Miguel Navascués, Yelena Guryanova, Matty J Hoban, and Antonio Acín. Almost quantum correlations. *Nature communications*, 6:6288, 2015.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107 – 108, 1990.

[Pip85] Nicholas Pippenger. On networks of noisy gates. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, pages 30–38. IEEE, 1985.

[Pip88] Nicholas Pippenger. Reliable computation by formulas in the presence of noise. *IEEE Transactions on Information Theory*, 34(2):194–197, 1988.

[Sho09] Anthony J. Short. No deterministic purification for two copies of a noisy entangled state. *Phys. Rev. Lett.*, 102:180502, May 2009.

[Ung07] Falk Unger. Noise threshold for universality of 2-input gates. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1901–1905. IEEE, 2007.

[Ung10] Falk Unger. Better gates can make fault-tolerant computation impossible. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 17, page 164, 2010.

[vD13] Wim van Dam. Implausible consequences of superstrong nonlocality. *Natural Computing*, 12(1):9–12, 2013.

[VHP05] S Virmani, Susana F Huelga, and Martin B Plenio. Classical simulability, entanglement breaking, and quantum computation thresholds. *Physical Review A*, 71(4):042328, 2005.

[vN56] John von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Automata studies*, 34:43–98, 1956.