Lower bounds on non-local quantum computation from controllable correlation

Richard Cleve and Alex May

Introduction: Suppose that Alice and Bob begin with systems A and B respectively, which they would like to interact under unitary U_{AB}. To do this, one possibility is for Alice and Bob to carry their systems and meet somewhere, then directly interact their systems. Alternatively, they can execute a *non-local quantum computation* (NLQC) protocol, as shown in figure 1. In that setting, Alice and Bob share entanglement, act locally in their own labs, exchange a single simultaneous round of quantum communication, then act locally again. This way, A and B never come together, but entanglement and communication allows the simulation of a local interaction between them.

Non-local quantum computation addresses a basic trade-off between resources in quantum information theory; interactions are exchanged with entanglement in this setting. More concretely, NLQC has been related to a long list of applications: quantum position-verification [1, 2], quantum gravity [3–5], complexity theory [6–8], classical information-theoretic cryptography [9, 10], Hamiltonian complexity [11], and uncloneable cryptography [12]. In all of these applications, understanding the entanglement cost of implementing a NLQC is the key relevant technical question. For instance, entanglement lower bounds are needed to establish security of quantum position-verification schemes and uncloneable secret sharing, lead to lower bounds on complexity, and lead to constraints on primitives studied in classical information-theoretic cryptography. Finally, entanglement lower bounds lead to constraints on gravity via the AdS/CFT correspondence, as argued in [4, 13].

Previous work: Lower bounds on NLQC have proven difficult to develop, with the strongest (unconditional) lower bounds being linear in the input size. Further, even such linear lower bounds have only been proven in scattered cases. For a hidden basis task, a proof that entanglement is necessary was given in [2]. A parallel repetition for the same task was proven in [14]; in particular they showed that repeating this task n times leads to a success probability like β^n, $\beta < 1$ when not using entanglement. This leads to a linear lower bound on entanglement cost via standard arguments [3, 4]. For f-routing, a related task where a qubit should be redirected based on classical inputs, a lower bound on the dimension of the ancilla was given in [15], for random choices of function and in a purified model. In [16], this is improved on by, for instance, allowing general channels rather than unitaries in the attack model. In [10] an entanglement lower bound linear in the classical input size was proven for some explicit, simple, choices of function f, although this relies on an assumption that the protocol is perfect in either $f(x, y) = 0$ or $f(x, y) = 1$ instances. Another approach instead considers the complexity of operations needed in the NLQC, which was lower bounded in [17].

Regarding bounds that are tight when including numerical factors, [18] gives a lower bound of $n - O(\log(n))$ for a protocol with an upper bound of n, although their lower bound is only against attackers using classical communication. Also in the classical communication setting the ability of a gate to create entanglement is a lower bound on it's entanglement cost [19]. Our bounds are similar in spirit to this idea, but apply in the case where quantum communication is allowed.

While these existing results give some insight into entanglement cost in NLQC, a general understanding of this problem remains largely open. For instance, we did not previously have an understanding of the entanglement cost of even the CNOT gate, arguably the simplest quantum interaction gate. More generally, the approach thus far has been to design interactions for which we can prove lower bounds, but generic approaches for bounding the entanglement of any interaction have been missing.

Main results: In this work we give two new (related) lower bound techniques for NLQC. We refer to these as the *controllable correlation* and *controllable entanglement* lower bounds. The starting point for the lower bounds is the set-up shown in figure 2. Consider the two input wires to the unitary of interest. Consider a correlated state P_{QA}. We refer to Q as the reference system, A as the input, and B as the control. Then, we are interested in the total correlation or entanglement between Q

and A after we run the circuit. If the total correlation in this state can be varied by adjusting the input to the control wire B, then we obtain a lower bound. Further, if the entanglement in this state can be varied sufficiently by adjusting the input to the control wire B, then we obtain a lower bound, which in some cases is tighter than the correlation based bound.

In more detail, in the *controllable correlation* technique we are interested in a unitary U_{AB} and how much we can vary the total correlation in $Q:A$ by adjusting the input to B. We choose any choice of initial correlated state P_{QA}. Then, defining

$$\begin{aligned}\lambda_1 &= \max_{\phi^1} I(Q:A)_{U_{AB}(P_{QA}\otimes\phi^1)U_{AB}^\dagger},\\ \lambda_2 &= \min_{\phi^2} I(Q:A)_{U_{AB}(P_{QA}\otimes\phi^2)U_{AB}^\dagger},\end{aligned} \tag{1}$$

we find that

$$\boxed{E_f(L:R)_\Psi \geq \frac{\lambda_1-\lambda_2}{2}} \tag{2}$$

where $E_f(L:R)_\Psi$ is the entanglement of formation in the distributed resource system Ψ used in the NLQC protocol. The right hand side can be maximized over choices of state P_{QA} to obtain the best possible bound.

In the *controllable entanglement* technique we are interested again in a unitary U_{AB} and making the entanglement of formation in $Q:A$ large on one input to the control wire, and then the state on $Q:A$ close (in trace distance) to separable on a second input. More specifically, we always take the reference and input to be maximally entangled, $P_{QA}=\Psi_{QA}^+$, and define

$$\lambda_1 := \max_{\phi^1} E_f(Q:A)_{\mathcal{N}_{AB}(\Psi^+\otimes\phi_B^1)}, \qquad \lambda_2 := \min_{\phi^2}\min_{\sigma\in SEP} \|\operatorname{tr}_B \mathcal{N}_{AB}(\Psi_{QA}^+\otimes\phi_B^1)-\sigma_{QA}\|_1.$$

With these definitions, we obtain the lower bound

$$\boxed{E_f(L:R)_\Psi \geq \lambda_1 - \sqrt{2}\lambda_2^{1/4}} \tag{3}$$

under the assumption that $\lambda_2 \leq 1/4$.

Both this and the bound from the controllable correlation can be adapted to bound noisy implementations of the relevant unitary. We give the full bounds with error terms in the main text.

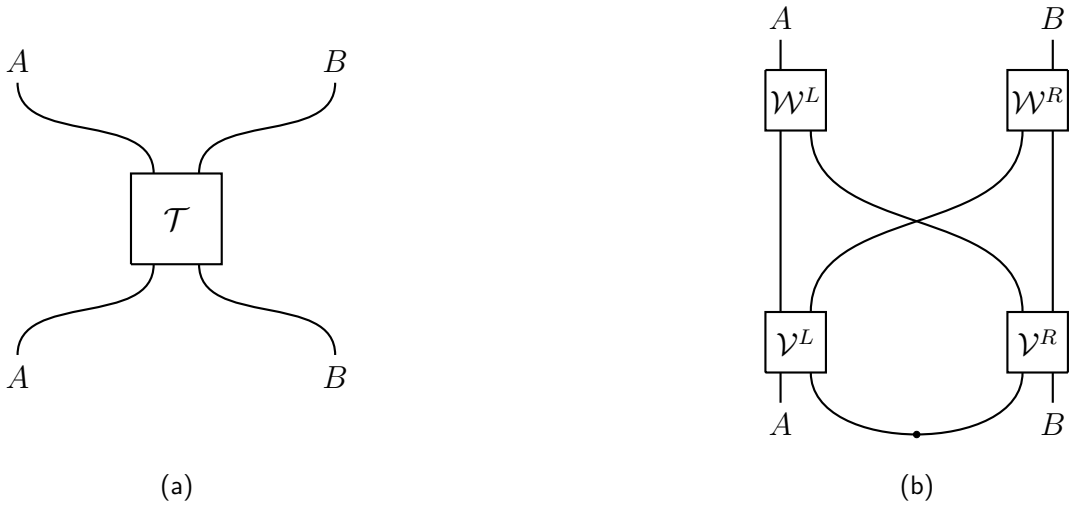

Figure 1: Local and non-local computations. a) A unitary U_{AB} is implemented by directly interacting the input systems. b) A non-local quantum computation. The goal is for the action of this circuit on the AB systems to approximate U_{AB}.

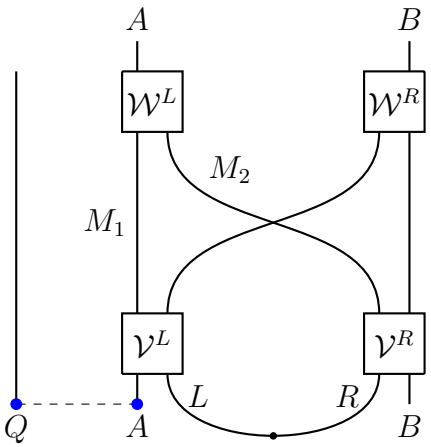

Figure 2: A non-local quantum computation implementing a unitary U_{AB}. To prove lower bounds on the entanglement cost, we consider placing the input system A in a state P_{QA} correlated with a reference system Q, indicated with the dashed line. The state P_{QA} need not be pure. We find that if adjusting the input on B changes the amount of correlation between A and Q in the final state, that $L : R$ must be entangled.

Both lower bound techniques have parallel repetition properties. For the controllable correlation, if G has lower bound $\Delta\lambda \equiv (\lambda_1 - \lambda_2)/2$ then we find $G^{\otimes n}$ has lower bound at least $n\Delta\lambda$. For the controllable entanglement, because of the requirement that $\lambda_2 \leq 1/4$, parallel repetition only holds when $\lambda_2 = 0$. In this case though, a lower bound of λ_1 on a unitary G implies a lower bound of $n\lambda_1$ on $G^{\otimes n}$. This contrasts with earlier results, where parallel repetition was known only in a small number of cases and required involved techniques.

Example applications: The controllable correlation and controllable entanglement techniques are complimentary, and combine to give robust insight into entanglement cost in NLQC.

A strength of the controllable correlation technique is that it appears to be generic: we computed the corresponding lower bound for 100,000 two-qubit unitaries drawn from the Haar distribution, and find that in every case we obtain a strictly positive lower bound. The only cases we have found which do not obtain a finite lower using the controllable correlation technique are the SWAP and identity gates, which have zero entanglement cost. We leave as an open problem if the controllable correlation is faithful in the sense that it is positive whenever the entanglement cost is positive. We also evaluate the controllable correlation for many commonly studied two qubit gates and find positive lower bounds; a table is included in the main text listing the gates and their bounds. Previously, lower bounds were not known for any of the examples shown in the table.

The controllable correlation lower bound does not seem to be tight when considering numerical factors. Thus for example the CNOT gate obtains a lower bound of $E_f \geq 1/2$, but the best known upper bound is $E_f = 1$. For CNOT the controllable entanglement technique addresses this: there we obtain $\lambda_1 = 1, \lambda_2 = 0$, so we get a tight lower bound $E_f \geq 1$. For the parallel repeated case of implementing $\text{CNOT}^{\otimes n}$, we obtain $E_f(L : R)_\Psi \geq n - 2\gamma_n^{1/8}$ where γ_n is the overall error (in diamond norm) of implementing $\text{CNOT}^{\otimes n}$ gate.[1]

Summary: We introduce two techniques for lower bounding entanglement cost in non-local quantum computation. While previously only a small list of quantum operations were known to have entanglement lower bounds, the controllable correlation technique can be applied generically and lower bounds entanglement cost for most unitaries, including common gates of interest. As well the controllable entanglement technique provides a tight lower bound on the entanglement cost of the CNOT gate.

[1]Note that γ_n must be below a threshold for this bound to work, so we cannot apply the above when we allow finite error γ in the implementation of each CNOT gate. Obtaining a bound like $E_f \geq \alpha\, n(1-\gamma)$ where γ is the error in a single implementation remains an important goal.

References

[1] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84 (1):012326, 2011. doi:https://doi.org/10.1103/PhysRevA.84.012326.

[2] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014. doi:https://doi.org/10.1137/130913687.

[3] Alex May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10):1–39, 2019. doi:https://doi.org/10.1007/JHEP10(2019)233.

[4] Alex May, Geoff Penington, and Jonathan Sorce. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics*, 2020(8):1–34, 2020. doi:https://doi.org/10.1007/JHEP08(2020)132.

[5] Alex May and Michelle Xu. Non-local computation and the black hole interior. *arXiv preprint arXiv:2304.11184*, 2023. doi:https://doi.org/10.48550/arXiv.2304.11184.

[6] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013. doi:https://doi.org/10.1145/2422436.2422455.

[7] Sam Cree and Alex May. Code-routing: a new attack on position-verification. *arXiv preprint arXiv:2202.07812*, 2022. doi:https://doi.org/10.48550/arXiv.2202.07812.

[8] Florian Speelman. Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits. In Anne Broadbent, editor, *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:24, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 978-3-95977-019-4. doi:10.4230/LIPIcs.TQC.2016.9. URL http://drops.dagstuhl.de/opus/volltexte/2016/6690.

[9] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8: 1387, 2024. doi:https://doi.org/10.22331/q-2024-06-27-1387.

[10] Vahid R Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation. *arXiv preprint arXiv:2402.18647*, 2024. doi:https://doi.org/10.48550/arXiv.2402.18647.

[11] Harriet Apel, Toby Cubitt, Patrick Hayden, Tamara Kohler, and David Pérez-García. Security of quantum position-verification limits hamiltonian simulation via holography. *Journal of High Energy Physics*, 2024(8):1–40, 2024. doi:https://doi.org/10.1007/JHEP08(2024)152.

[12] Prabhanjan Ananth, Vipul Goyal, Jiahui Liu, and Qipeng Liu. Unclonable secret sharing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 129–157. Springer, 2024. doi:https://doi.org/10.1007/978-981-96-0947-5_5.

[13] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, 2022. doi:https://doi.org/10.22331/q-2022-11-28-864.

[14] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.

[15] Andreas Bluhm, Matthias Christandl, and Florian Speelman. Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks. *arXiv preprint arXiv:2104.06301*, 2021. doi:https://doi.org/10.48550/arXiv.2104.06301.

[16] Wen Yu Kon, Ignatius William Primaatmaja, Kaushik Chakraborty, and Charles Lim. Quantum secure key exchange with position-based credentials. *arXiv preprint arXiv:2506.03549*, 2025. doi:https://doi.org/10.48550/arXiv.2506.03549.

[17] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification. *Quantum*, 9:1604, 2025. doi:https://doi.org/10.22331/q-2025-01-21-1604.

[18] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the BB84-states quantum-position-verification protocol. *arXiv preprint arXiv:1504.07171*, 2015. doi:https://doi.org/10.48550/arXiv.1504.07171.

[19] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2019.