Energy-constrained discrimination of unitaries, quantum speed limits and a Gaussian Solovay–Kitaev theorem

Simon Becker, Nilanjana Datta, Ludovico Lami, and Cambyse Rouzé

Preprint arXiv:2006.06659

Introduction. Distinguishing objects is a critically important task in experimental science. The recent approaches in quantum information theory advocate the fundamental status of quantum channels rather than quantum states; far from being a merely abstract consideration, this also reflects our technological effort to build quantum circuits that implement desired operations. In this context, binary channel discrimination is thus to be regarded as a basic primitive. While most of the recent literature on the topic has focused primarily on finite-dimensional systems, the continuous-variable platforms that are playing a major role in the field of quantum communication (typically, electromagnetic modes travelling along optical fibers) are intrinsically infinite-dimensional. However, from an experimental point of view, we can only probe the unknown channel by means of finite-energy states. Adding a mean energy bound with respect to some reference Hamiltonian singles out the energy-constrained (EC) diamond norm distance as the relevant figure of merit for binary channel discrimination [58**?**]. In this article, we investigate the EC diamond norm distance between two unitary channels, and apply our findings to a wealth of operationally relevant scenarios.

Main results. First, we establish quantitative bounds on the EC diamond norm distance between the unitary time evolution channels generated by any two different Hamiltonians

Theorem 1. *Let H, H' be self-adjoint operators. Without loss of generality, assume that 0 is in the spectrum of H. Let the 'relative boundedness' inequality $\|(H-H')\,|\psi\rangle\| \leqslant \alpha\,\|H\,|\psi\rangle\| + \beta$ hold for some constants $\alpha, \beta > 0$ and for all (normalised) states $|\psi\rangle$. Then the unitary channels*

$$\mathscr{U}_t(\cdot) := e^{-iHt}(\cdot)e^{iHt}, \quad \mathscr{V}_t(\cdot) := e^{-iH't}(\cdot)e^{iH't} \tag{1}$$

satisfy the following: for all $t \geqslant 0$ and $E > 0$, $\|\mathscr{U}_t - \mathscr{V}_t\|_\diamond^{|H|,E} \leqslant 2\sqrt{2}\sqrt{\alpha E t} + \sqrt{2}\beta t$.

We also show a similar result for a unitary time evolution channel and an open-system quantum dynamical semigroup with generator $\mathscr{L}$ whose action on a trace class operator X is given as follows:

$$\mathscr{L}(X) = -i[H,X] + \frac{1}{2}\sum_\ell \left(2L_\ell X L_\ell^\dagger - L_\ell^\dagger L_\ell X - X L_\ell^\dagger L_\ell\right).$$

Here, H is the internal Hamiltonian, while the *Lindblad operators* L_ℓ ($\ell = 1, 2, \dots$) model dissipative processes. In our approach these can be unbounded, and hence our results significantly generalise previous works on quantum speed limits in open systems [**?**].

Theorem 2. *Let H be a self-adjoint operator with 0 in its spectrum, and set $\mathscr{U}_t(\cdot) := e^{-iHt}(\cdot)e^{iHt}$. Let $(\Lambda_t)_{t\geqslant 0}$ be a QDS whose generator $\mathscr{L}$ is of GKLS-type and satisfies the relative boundedness condition*

$$\frac{1}{2}\left\|\sum\nolimits_\ell L_\ell^\dagger L_\ell\,|\psi\rangle\right\| \leqslant \alpha\,\|H\,|\psi\rangle\| + \beta \tag{2}$$

for all (normalised) states $|\psi\rangle$, where $\beta \geqslant 0$ and $0 \leqslant \alpha < 1$ are two constants. Then it holds that

$$\|\mathscr{U}_t - \Lambda_t\|_\diamond^{|H|,E} \leqslant 4\left(\sqrt{\sqrt{2}\alpha E t} + \beta t\right) \tag{3}$$

for all $t \geqslant 0$ and $E > 0$.

Notably, both theorems above can be recast in the form of new quantum speed limits.

We then prove that optimal discrimination between two unitaries can be achieved without the need for entangled ancillary systems, which greatly simplifies the experimentalists' task. In addition, we show that perfect (i.e., zero-error) discrimination can be realized even in this EC setting by invoking a finite number of parallel queries of the unknown unitary channel. This extends a celebrated result by Acín [1] (subsequently improved by Duan et al. [20]).

Theorem 3. *Let* U, V *be two unitaries acting on a Hilbert space of dimension* $\dim\mathcal{H} \geqslant 3$*, and call* $\mathscr{U}(\cdot) := U(\cdot)U^\dagger$*,* $\mathscr{V}(\cdot) := V(\cdot)V^\dagger$ *the associated channels. Let* H *be a grounded Hamiltonian, and fix* $E > 0$*. There exists a positive integer* n *such that* n *parallel uses of* $\mathscr{U}$ *and* $\mathscr{V}$ *can be discriminated perfectly using inputs of finite total energy* E*, i.e.*

$$\left\|\mathscr{U}^{\otimes n} - \mathscr{V}^{\otimes n}\right\|_\diamond^{H_{(n)},\,E} = 2\,, \tag{4}$$

where $H_{(n)} := \sum_{j=1}^{n} H_j$ *is the* n*-copy Hamiltonian, and* $H_j := I \otimes \cdots I \otimes H \otimes I \cdots \otimes I$*, with the* H *in the* j^{th} *location.*

Applications of our results: Our discrimination results bear an immediate impact on the experimentally relevant problem of benchmarking a quantum system whose internal dynamics is unknown. Our final application concerns quantum computation with continuous-variable systems. In this setting, Gaussian unitaries, that is, unitaries induced by Hamiltonians that are quadratic in the canonical operators, are of outstanding technological relevance. For example, together with single-photon sources and photodetectors, they are known to enable universal quantum computation via the so-called KLM scheme [**?**]. Here, we extend a fundamental result of quantum computation, the Solovay-Kitaev theorem [**?**] to the case of Gaussian unitary channels, establishing that any finite set of Gaussian unitaries (gates) that is sufficiently powerful to generate arbitrarily accurate approximations of any desired Gaussian unitary does that efficiently, i.e., by means of short gate sequences. In our result, the approximation error is quantified in an operationally meaningful way by means of the EC diamond norm. Like the standard Solovay-Kitaev theorem, our Gaussian extension is potentially useful because it guarantees that quantum algorithms can be efficiently compiled, i.e., simplified so as to include only gates from a fixed base set.

Theorem 4. *Let* $m \in \mathbb{N}$*,* $r > 0$*,* $E > 0$ *and define* $\widetilde{\mathrm{Sp}}^{r}_{2m}(\mathbb{R})$ *to be the set of all symplectic transformations* S *such that* $\|S\|_\infty \leqslant r$*. Then, given a set* $\mathscr{G}$ *of gates that is closed under inverses and generates a dense subset of* $\widetilde{\mathrm{Sp}}^{r}_{2m}(\mathbb{R})$*, there exists a constant* $C = C(r) < (3{+}r)(47r^2{+}198r{+}203)$ *such that, for any symplectic transformation* $S \in \widetilde{\mathrm{Sp}}^{r}_{2m}(\mathbb{R})$ *and every* $0 < \delta$*, there exists a finite concatenation* S' *of* $\mathrm{poly}(\log\delta^{-1})$ *elements from* $\mathscr{G}$*, which can be found in time* $\mathrm{poly}(\log\delta^{-1})$ *and such that*

$$\|\mathscr{U}_S - \mathscr{U}_{S'}\|_\diamond^{N,E} \leqslant F(m)G(r)\sqrt{E+1}\sqrt{\delta}\ , \tag{5}$$

where $\mathscr{U}_S(\cdot) := U_S(\cdot)U_S^\dagger$*, and* F *and* G *are explicit functions.*

Conclusion. In this article, we uncovered useful properties of the EC diamond norm distance between unitary channels, and applied our results to establish new quantum speed limits, study channel discrimination under energy constraints, and to extend the important Solovay-Kitaev theorem to the Gaussian unitary setting.

[1] A. Acín. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.*, 87:177901, 2001.
[2] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 20–30, New York, NY, USA, 1998. ACM.
[3] Y.-H. Au-Yeung and Y.-T. Poon. A remark on the convexity and positive definiteness concerning hermitian matrices. *Southeast Asian Bull. Math.*, 3:85–92, 1979.
[4] Y.-H. Au-Yeung and N.-K. Tsing. An extension of the Hausdorff-Toeplitz theorem on the numerical range. *Proceedings of the American Mathematical Society*, 89(2):215–218, 1983.
[5] K. M. R. Audenaert and N. Datta. alpha-z-relative renyi entropies. *Jour. Math. Phys.*, 56:022202, 2015.
[6] S. Becker and N. Datta. Convergence rates for quantum evolution and entropic continuity bounds in infinite dimensions. *Communications in Mathematical Physics*, 374(2):823–871, 2020.
[7] M. Berta, F. Furrer, and V. B. Scholz. The smooth entropy formalism for von neumann algebras. *Journal of Mathematical Physics*, 57(1):015213, 2016.
[8] M. Berta, C. Hirche, E. Kaur, and M. M. Wilde. Amortized channel divergence for asymptotic quantum channel discrimination. *arXiv preprint arXiv:1808.01498*, 2018.
[9] P. Binding. Hermitian forms and the fibration of spheres. *Proc. Am. Math. Soc.*, 94(4):581–584, 1985.
[10] A. Bouland and M. Ozols. Trading inverses for an irrep in the solovay-kitaev theorem. *arXiv preprint arXiv:1712.09798*, 2017.
[11] F. G. Brandao and N. Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57(3):1754–1760, 2011.
[12] F. Buscemi and N. Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, 2010.
[13] F. Caruso, J. Eisert, V. Giovannetti, and A. S. Holevo. Multi-mode bosonic gaussian channels. *New Journal of Physics*, 10(8):083030, 2008.
[14] A. M. Childs, Y. Su, M. C. Tran, N. Wiebe, and S. Zhu. A theory of trotter error. *arXiv preprint arXiv:1912.08854*, 2019.
[15] T. Cooney, M. Mosonyi, and M. M. Wilde. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Communications in Mathematical Physics*, 344(3):797–829, 2016.
[16] N. Datta. Min-and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, 2009.
[17] Datta, Nilanjana and Pautrat, Yan and Rouzé, Cambyse. Second order asymptotics for the error exponent in asymmetric quantum hypothesis testing for separable Hilbert spaces. *Unpublished notes*, 2018.
[18] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm. *arXiv preprint quant-ph/0505030*, 2005.
[19] M. A. De Gosson. *Symplectic methods in harmonic analysis and in mathematical physics*, volume 7. Springer Science & Business Media, 2011.
[20] R. Duan, Y. Feng, and M. Ying. Entanglement is not necessary for perfect discrimination between unitary operations. *Phys. Rev. Lett.*, 98:100503, 2007.
[21] R. Duan, Y. Feng, and M. Ying. Local distinguishability of multipartite unitary operations. *Phys. Rev. Lett.*, 100:020503, 2008.
[22] R. Duan, Y. Feng, and M. Ying. Perfect distinguishability of quantum operations. *Phys. Rev. Lett.*, 103:210501, 2009.
[23] K. Fang, O. Fawzi, R. Renner, and D. Sutter. Chain rule for the quantum relative entropy. *Physical Review Letters*, 124(10):100501, 2020.
[24] C. A. Fuchs and J. Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.
[25] F. Furrer, J. Åberg, and R. Renner. Min-and max-entropy in infinite dimensions. *Communications in Mathematical Physics*, 306(1):165–186, 2011.
[26] V. Giovannetti, A. S. Holevo, and R. Garcia-Patron. A solution of gaussian optimizer conjecture for quantum channels. *Communications in Mathematical Physics*, 334(3):1553–1571, 2015.

[27] B. C. Hall. *Quantum Theory for Mathematicians*. Graduate Texts in Mathematics. Springer New York, 2013.

[28] A. Harrow. *Quantum compiling*. PhD thesis, Citeseer, 2001.

[29] A. W. Harrow, B. Recht, and I. L. Chuang. Efficient discrete approximations of quantum gates. *Journal of Mathematical Physics*, 43(9):4445–4451, 2002.

[30] F. Hausdorff. Der Wertvorrat einer Bilinearform. *Math. Z.*, 3(1):314–316, 1919.

[31] T. Heinosaari, A. S. Holevo, and M. M. Wolf. The semigroup structure of Gaussian channels. *preprint*, 0909.0408(ii):1–20, 2009.

[32] A. S. Holevo and M. E. Shirokov. Continuous ensembles and the capacity of infinite-dimensional quantum channels. *Theory Probab. Its Appl.*, 50(1):86–98, 2006.

[33] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Topics in Matrix Analysis. Cambridge University Press, 1994.

[34] J. Hou and X. Qi. Fidelity of states in infinite-dimensional quantum systems. *Science China Physics, Mechanics and Astronomy*, 55(10):1820–1827, 2012.

[35] E. Kaur and M. M. Wilde. Upper bounds on secret-key agreement over lossy thermal bosonic channels. *Physical Review A*, 96(6):062318, 2017.

[36] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Uspekhi Matematicheskikh Nauk*, 52(6):53–112, 1997.

[37] M. Kliesch, T. Barthel, C. Gogolin, M. Kastoryano, and J. Eisert. Dissipative quantum church-turing theorem. *Physical review letters*, 107(12):120501, 2011.

[38] A. W. Knapp. *Representation theory of semisimple groups: an overview based on examples*, volume 36. Princeton university press, 2001.

[39] R. Kukulski, P. Lewandowska, and Ł. Pawela. Perturbation of the numerical range of unitary matrices. *arXiv preprint arXiv:2002.05553*, 2020.

[40] G. Kuperberg. How hard is it to approximate the jones polynomial? *Theory of Computing*, 11(1):183–219, 2015.

[41] K. Li et al. Second-order asymptotics for quantum hypothesis testing. *The Annals of Statistics*, 42(1):171–189, 2014.

[42] G. Lindblad. Expectations and entropy inequalities for finite quantum systems. *Communications in Mathematical Physics*, 39(2):111–119, 1974.

[43] W. Matthews and S. Wehner. Finite blocklength converse bounds for quantum channels. *IEEE Transactions on Information Theory*, 60(11):7317–7329, 2014.

[44] I. Nechita, Z. Puchała, Ł. Pawela, and K. Życzkowski. Almost all quantum channels are equidistant. *J. Math. Phys.*, 59(5):052201, 2018.

[45] M. A. Nielsen and I. Chuang. Quantum computation and quantum information, 2002.

[46] A. Serafini. *Quantum continuous variables: a primer of theoretical methods*. CRC Press, 2017.

[47] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka. Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic gaussian channels. *New Journal of Physics*, 20(6):063025, 2018.

[48] M. Shirokov. Energy-constrained diamond norms and their applications in quantum information theory. *J. Phys. A*, 52(1):14001–33, 2019.

[49] R. Solovay. Lie groups and quantum circuits. *preprint*, 1999.

[50] O. Toeplitz. Das algebraische Analogon zu einem Satze von Fejér. *Math. Z.*, 2:187–197, 1918.

[51] M. Tomamichel. A framework for non-asymptotic quantum information theory. *arXiv preprint arXiv:1203.2142*, 2012.

[52] M. Tomamichel and M. Hayashi. A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks. *Journal of Mathematical Physics*, 53(12):122205, 2012.

[53] V. S. Varadarajan. *Lie groups, Lie algebras, and their representations*, volume 102. Springer Science & Business Media, 2013.

[54] L. Wang and R. Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, 2012.

[55] X. Wang and M. M. Wilde. Resource theory of asymmetric distinguishability for quantum channels. *Physical Review Research*, 1(3):033169, 2019.

[56] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[57] A. Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative

entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, 2016.

[58] A. Winter. Energy-constrained diamond norm with applications to the uniform continuity of continuous variable channel capacities. *arXiv preprint arXiv:1712.10267*, 2017.