Grover Search and the No-Signaling Principle

Ning Bao, Adam Bouland, and Stephen P. Jordan

Phys. Rev. Lett. **117**, 120501 — Published 14 September 2016

DOI: 10.1103/PhysRevLett.117.120501

Grover search and the no-signaling principle

Ning Bao
Institute for Quantum Information and Matter and
Walter Burke Institute for Theoretical Physics,
California Institute of Technology 452-48, Pasadena, CA 91125, USA

Adam Bouland
Computer Science and Artificial Intelligence Laboratory,
Massachusetts Institute of Technology, Cambridge, MA

Stephen P. Jordan
National Institute of Standards and Technology, Gaithersburg, MD and
Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD

(Dated: August 9, 2016)

Two of the key properties of quantum physics are the no-signaling principle and the Grover search lower bound. That is, despite admitting stronger-than-classical correlations, quantum mechanics does not imply superluminal signaling, and despite a form of exponential parallelism, quantum mechanics does not imply polynomial-time brute force solution of NP-complete problems. Here, we investigate the degree to which these two properties are connected. We examine four classes of deviations from quantum mechanics, for which we draw inspiration from the literature on the black hole information paradox. We show that in these models, the physical resources required to send a superluminal signal scale polynomially with the resources needed to speed up Grover's algorithm. Hence the no-signaling principle is equivalent to the inability to solve NP-hard problems efficiently by brute force within the classes of theories analyzed.

PACS numbers: 03.67.-a, 03.65.-w, 04.70.Dy

INTRODUCTION

Recently the firewalls paradox [1, 2] has shown that our understanding of quantum mechanics and general relativity appear to be inconsistent at the event horizon of a black hole. Many of the leading proposals to resolve the paradox involve modifying quantum mechanics. For example, the final-state projection model of Horowitz and Maldecena [3] and the state dependence model of Papadodimas and Raju [4] are modifications to quantum theory which might resolve the inconsistency.

One reason to be skeptical of such modifications of quantum mechanics is that they can often give rise to superluminal signals, and hence introduce acausality into the model. For example, Weinberg nonlinearities allow for superluminal signaling [5, 6]. This is generally seen as unphysical. In contrast, in standard quantum theory, entanglement does not give rise to superluminal signaling.

Another startling feature of such models is that they might allow one to construct computers far more powerful even than conventional quantum computers. In particular, they may allow one to solve NP-hard problems in polynomial time. NP-hard problems refer to those problems for which the solution can be *verified* in polynomial time, but for which there are exponentially many possible solutions. It is impossible for standard quantum computers to solve NP-hard problems efficiently by searching over all possible solutions. This is a consequence of the query complexity lower bound of Bennett, Bernstein, Brassard and Vazirani [7], which shows one cannot search an unstructured list of 2^n items in fewer than $2^{n/2}$ queries with a quantum computer. (Here a *query* is an application of a function f whose output indicates if you have found a solution. The *query complexity* of search is the minimum number of queries to f, possibly in superposition, required to find a solution.) This bound is achieved by Grover's search algorithm [8]. In contrast, many modifications of quantum theory allow quantum computers to search an exponentially large solution space in polynomial time. For example, quantum computers equipped with postselection [9], Deutschian closed timelike curves [10–12], or nonlinearities [13–17] all admit poly-time solution of NP-hard problems by brute force search.

In this paper we explore the degree to which superluminal signaling and speedups over Grover's algorithm are connected. We consider several modifications of quantum mechanics which are inspired by resolutions of the firewalls paradox. For each modification, we show that the theory admits superluminal signaling if and only if it admits a query complexity speedup over Grover search. Furthermore, we establish a *quantative* relationship between superluminal signaling and speedups over Grover's algorithm. More precisely, we show that if one can transmit one classical bit of information superluminally using n qubits and m operations, then one can speed up Grover search on a system of $\mathrm{poly}(n,m)$ qubits with $\mathrm{poly}(n,m)$ operations, and vice versa. In other words, the ability to send a superluminal signal with a reasonable amount of physical resources is equivalent to the ability to violate the Grover lower bound with a reasonable amount of physical resources. Therefore the no-signaling principle is equivalent to the inability to solve NP-hard problems efficiently by brute force within the classes of theories analyzed.

Note that in the presence of nonlinear dynamics, density matrices are no longer equivalent to ensembles of pure states. Here, we consider measurements to produce probabilistic ensembles of post-measurement pure states and compute the dynamics of each of these pure states separately. Alternative formulations, in particular Everettian treatment of measurements as entangling unitaries, lead in some cases to different conclusions about superluminal signaling. See e.g. [18].

RESULTS

We consider four modifications of quantum mechanics, which are inspired by resolutions of the firewalls paradox. The first two are "continuous" modifications in the sense that they have a tunable parameter δ which quantifies the deviation from quantum mechanics. The second two are "discrete" modifications in which standard quantum mechanics is supplemented by one additional operation.

Final state projection

The first "continuous" modification of quantum theory we consider is the final state projection model of Horowitz and Maldecena [3], in which the black hole singularity projects the wavefunction onto a specific quantum state. This can be thought of as a projective measurement with postselection, which induces a linear (but not necessarily unitary) map on the projective Hilbert space. (In some cases it is possible for the Horowitz-Maldecena final state projection model to induce a perfectly unitary process S for the black hole, but in general interactions between the collapsing body and infalling Hawking radiation inside the event horizon induce deviations from unitarity [19].) Such linear but non-unitary maps allow both superluminal signaling and speedups over Grover search. Any non-unitary map M of condition number $1+\delta$ allows for superluminal signaling with channel capacity $O(\delta^2)$ with a single application of M. The protocol for signaling is simple - suppose Alice has the ability to apply M, and suppose Alice and Bob share the entangled state

$$\frac{1}{\sqrt{2}}\left(|\phi_0\rangle|0\rangle + |\phi_1\rangle|1\rangle\right). \qquad (1)$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are the minimum/maximum singular vectors of M, respectively. If Alice chooses to apply M or not, then Bob will see a change in his half of the state, which which allows signaling with channel capacity $\sim \delta^2$. Furthermore, it is also possible for Bob to signal superluminally to Alice with the same state - if Bob chooses to measure or not to measure his half of the state, it will also affect the state of Alice's system after Alice applies M. So this signaling is bidirectional, even if only one party has access to the non-unitary map. In the context of this black hole information paradox, this implies the acausality in the final state projection model could be present even far away from the black hole. Also, assuming one can apply the same M multiple times, one can perform single-query Grover search using $\sim 1/\delta$ applications of M using the methods of [9, 13]. More detailed proofs of these results are provided in Section A of the supplementary material [20].

We next examine the way in which these results are connected. First, assuming one can speed up Grover search, by a generalization of the hybrid argument of [7], there is a lower bound on the deviation from unitarity required to achieve the speedup. By our previous results this implies a lower bound on the superluminal signaling capacity of the map M. More specifically, suppose that one can search an unstructured list of N items using q queries, with possibly non-unitary operations applied between queries. Then, the same non-unitary dynamics must be capable of transmitting superluminal signals with channel capacity C using shared entangled states, where

$$C = \Omega\left(\left(\frac{\eta}{2q^2} - \frac{2}{N}\right)^2\right) \tag{2}$$

Here η is a constant which is roughly ~ 0.42. In particular, solving NP-hard problems in polynomial time by unstructured search would imply superluminal signaling with inverse polynomial channel capacity. This can be regarded as evidence against the possibility of using black hole dynamics to efficiently solve NP-hard problems of reasonable size. A proof of this fact is provided in Section A of the supplementary material [20].

In the other direction, assuming one can send a superluminal signal with channel capacity C, there is a lower bound on the deviation from unitarity which was applied. The proof is provided in Section A of the supplementary material [20]. Again by our previous result, this implies one could solve the Grover search problem on a database of size N using a single query and

$$O\left(\frac{\log(N)}{\log(1+C^2)}\right) \tag{3}$$

applications of the nonlinear map. Combining these results, this implies that if one can send a superluminal signal with n applications of M, then one can beat Grover's algorithm with $O(n)$ applications of M as well, and vice versa. This shows that in these models, the resources required to observe an exponential speedup over Grover search is polynomially related to the resources needed to send a superluminal signal. Hence an operational version of the no-signaling principle (such as "one cannot observe superluminal signaling in reasonable-sized experiments") is equivalent to an operational version of the Grover lower bound ("one cannot observe violations of the Grover lower bound in reasonable-sized experiments").

Modification of the Born Rule

The next continuous modification of quantum mechanics we consider is modification of the Born rule. Suppose that quantum states evolve by unitary transformations, but upon measurement one sees outcome x with probability proportional to some function $f(\alpha_x)$ of the amplitude α_x on x. That is, one sees x with probability

$$\frac{f(\alpha_x)}{\sum_y f(\alpha_y)} \tag{4}$$

Note we have added a normalization factor to ensure this induces a valid probability distribution on outcomes. This is loosely inspired by Marolf and Polchinski's work [21] which suggests that the "state-dependence" resolution of the firewalls paradox [4] gives rise to violations of the Born rule. First, assuming some reasonable conditions on f (namely, that f is differentiable, f' changes signs a finite number of times in $[0,1]$, and the measurement statistics of f do not depend on the normalization of the state), we must have $f(\alpha_x) = |\alpha_x|^p$ for some p. The proof is provided in Section B of the supplementary material [20].

Next we study the impact of such modified Born rules with $p = 2+\delta$ for small δ. Aaronson [9] previously showed that such models allow for single-query Grover search in polynomial time while incurring a multiplicative overhead $1/|\delta|$, and also allow for superluminal signaling using shared entangled states of $\sim 1/|\delta|$ qubits. (His result further generalizes to the harder problem of *counting* the number of solutions to an NP-hard problem, which is a $\#\mathsf{P}$-hard problem). We find that these relationships hold in the opposite directions as well. Specifically, we show if one can send a superluminal signal with an entangled state on m qubits with probability ϵ, then we must have $\delta = \Omega(\epsilon/m)$. By the results of Aaronson [9] this implies one can search a list of N items using $O(\frac{m}{\epsilon}\log N)$ time. Hence having the ability to send a superluminal signal using m qubits implies the ability to perform an exponential speedup of Grover's algorithm with multiplicative overhead m.

In the other direction, if one can achieve even a constant-factor speedup over Grover's algorithm using a system of m qubits, we show $|\delta|$ is at least $1/m$ as well. More precisely, by a generalization of the hybrid argument of [7], if there is an algorithm to search an unordered list of N items with Q queries using m qubits, then

$$\frac{1}{6} \leq \frac{2Q}{\sqrt{N}} + |\delta|\log(M) + O(\delta^2). \tag{5}$$

So if $Q < \sqrt{N}/24$, then we must have $|\delta| \geq \frac{1}{12m}$. The proofs of these facts are provided in Section B of the supplementary material [20].

Combining these results shows that the number of qubits required to observe superluminal signaling or even a modest speedup over Grover's algorithm are polynomially related. Hence one can derive an operational version of the no-signaling principle from the Grover lower bound and vice versa. This quantitative result is in some sense stronger than the result we achieve for the final-state projection model, because here we require only a mild speedup over Grover search to derive superluminal signaling.

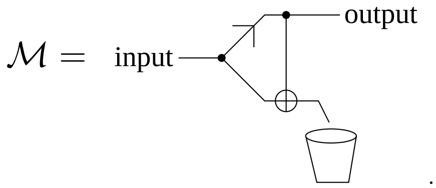

FIG. 1. Gadget used to show that cloning allows the poly-time solution of NP-hard problems.

Cloning, Postselection, and Generic Nonlinearities

We next consider two "discrete" modifications of quantum mechanics in which standard quantum mechanics is supplemented by one additional operation. We show that both modifications admit both superluminal signaling with O(1) qubits and exponential speedups over Grover search.

First, we consider a model in which one can clone single qubits. This model can be easily seen to admit superluminal signaling using entangled states, as pointed out by Aaronson, Bouland, Fitzsimons and Lee [22]. Indeed, suppose two parties Alice and Bob share the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If Alice measures her half of the state, and Bob clones his state k times and measures each copy in the computational basis, then Bob will either see either 0^k or 1^k as his output. On the other hand, if Alice does not measure her half of the state, and Bob does the same experiment, his outcomes will be a random string in $\{0,1\}^k$. Bob can distinguish these two cases with an error probability which scales inverse exponentially with k, and thus receive a signal faster than light. In addition to admitting superluminal signaling with entangled states, this model also allows the solution of NP-hard problems (and even #P-hard problems) using a single query to the oracle. This follows by considering the following gadget: given a state ρ on a single qubit, suppose one makes two copies of ρ, performs a Controlled-NOT gate between the copies, and discards one of the copies. This is summarized with the following circuit diagram.

This performs a non-linear operation $\mathcal{M}$ on the space of density matrices, and following the techniques of Abrams and Lloyd [13], one can use this operation to "pry apart" quantum states which are exponentially close using polynomially many applications of the gadget. The proof is provided in Section C of the supplementary material [20]. This answers an open problem of [22] about the power of quantum computers that can clone. Therefore, adding cloning to quantum mechanics allows for both the poly-time solution of NP-hard problems by brute force search, and the ability to efficiently send superluminal signals.

Second, inspired by the final state projection model [3], we consider a model in which one can postselect on a generic state $|\psi\rangle$ of n qubits. Although Aaronson [9] previously showed that allowing for postselection on a single qubit suffices to solve NP-hard and #P-hard problems using a single oracle query, this does not immediately imply that postselecting on a larger state has the same property, because performing the unitary which rotates $|0\rangle^n$ to $|\psi\rangle$ will in general require exponentially many gates. Despite this limitation, this model indeed allows the polynomial-time solution of NP-hard problems (as well as #P-hard problems) and superluminal signaling. To see this, first note that given a gadget to postselect on $|\psi\rangle$, one can obtain multiple copies of $|\psi\rangle$ by inputting the maximally entangled state $\sum_i |i\rangle|i\rangle$ into the circuit and postselecting one register on the state $|\psi\rangle$. So consider creating two copies of $|\psi\rangle$, and applying the gadget shown in Figure 2, where the bottom register is postselected onto $|\psi\rangle$, an operation we denote by —$\boxed{|\psi\rangle}$—. For Haar-random $|\psi\rangle$, one can show the quantity $\langle\psi|Z\otimes I|\psi\rangle$ is exponentially small, so this gadget simulates postselection on $|0\rangle$ on the first qubit. The complete proof is provided in Section D of the supplementary

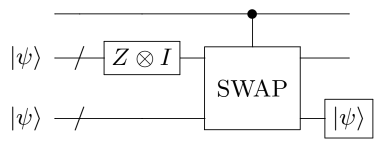

FIG. 2. Gadget showing postselection onto generic $|\psi\rangle$ is equivalent to postselection onto $|0\rangle$.

material [20]. Therefore, allowing postselection onto generic states is at least as powerful as allowing postselection onto the state $|0\rangle$, so by Aaronson's results [9] this model admits both superluminal signaling and exponential speedups over Grover search.

In addition, we address an open question from [13] regarding the computational implications of general nonlinear maps on pure states. In [13], Abrams and Lloyd argued that generic nonlinear maps allow for the solution of NP-hard problems and $\#\mathsf{P}$-hard problems in polynomial time, except possibly for pathological examples. In Section E of the supplementary material [20], we prove this result rigorously in the case the map is differentiable. Thus any pathological examples, if they exist, must fail to be differentiable. (Here we assume the nonlinearity maps pure states to pure states; as a result it does not subsume our results on quantum computers which can clone, as the cloning operation may map pure states to mixed states. A detailed discussion is provided in Section C of the supplementary material [20].) Unfortunately, the action of general nonlinear maps on subsystems of entangled states are not well-defined, essentially because they interact poorly with the linearity of the tensor product. We discuss this in detail in Section F of the supplementary material [20]. Hence we are unable to connect this result to signaling in the general case.

DISCUSSION

The central question in complexity theory is which computational problems can be solved efficiently and which cannot. Through experience, computer scientists have found that the most fruitful way to formalize the notion of efficient is by demanding that the resources, such as time and memory, used to solve a problem must scale at most polynomially with the size of the problem instance (i.e. the size of the input in bits). A widely held conjecture, called the quantum Church-Turing thesis, states that the set of computational problems solvable in-principle with polynomial resources in our universe is equal to BQP, defined mathematically as the set of decision problems answerable using quantum circuits of polynomially many gates [23]. So far, this conjecture has held up remarkably well. Physical processes which conceivably might be more computationally powerful that quantum Turing machines, such as various quantum many-body dynamics of Fermions, Bosons, and anyons, as well as scattering processes in relativistic quantum field theories, can all be simulated with polynomial overhead by quantum circuits [24–28].

The strongest challenge to the quantum Church-Turing thesis comes from quantum gravity. Indeed, many of the recent quantum gravity models proposed in relation the black hole firewalls paradox involve nonlinear behavior of wavefunctions [3, 4] and thus appear to suggest computational power beyond that of polynomial-size quantum circuits. In particular, the prior work of Abrams and Lloyd suggest that such nonlinearities generically enable polynomial-time solution to NP-hard problems, a dramatic possibility, that standard quantum circuits are not generally expected to admit [13, 29]. Here, we have investigated several models and found a remarkably consistent pattern; in each case, if the modification to quantum mechanics is in a parameter regime allowing polynomial-time solution to NP-hard problems through brute-force search, then it also allows the transmission of superluminal signals through entangled states. Such signaling allows causality to be broken at locations arbitrarily far removed from the vicinity of the black hole, thereby raising serious questions as to the consistency of the models. Thus, the quantum Church-Turing thesis appears to be remarkably robust, depending not in a sensitive way on the complete Hilbert-space formalism of quantum mechanics, but rather derivable from more foundational operational principles such as the impossibility of superluminal signaling. Some more concrete conjectures on these lines are discussed in Section G of the supplementary material [20].

ACKNOWLEDGMENTS

We thank Patrick Hayden, Daniel Harlow, David Meyer, Andrew Childs and Debbie Leung for useful discussions. Portions of this paper are a contribution of NIST, an agency of the US government, and are not subject to US copyright. This material is based upon work supported by the DuBridge Postdoctoral Fellowship, by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028), by the U.S. Department of Energy, Office of Science, Office of High Energy Physics, under

Award Number DE-SC0011632, by the NSF Graduate Research Fellowship under grant no. 1122374, and by the NSF Alan T. Waterman award under grant no. 1249349. N. B. and A. B. would also like to thank QuICS for their hospitality during the completion of this project.

[1] Almheiri, A., Marolf, D., Polchinski, J. & Sully, J. Black holes: Complementarity or firewalls? *Journal of High Energy Physics* **1302**, 062 (2013). ArXiv:1207.3123.

[2] Braunstein, S. L., Pirandola, S. & Życzkowski, K. Better late than never: Information retrieval from black holes. *Physical Review Letters* **110**, 101301 (2013).

[3] Horowitz, G. T. & Maldecena, J. The black hole final state. *Journal of High Energy Physics* **0402**, 008 (2004). ArXiv:hep-th/0310281.

[4] Papadodimas, K. & Raju, S. State-dependent bulk-boundary maps and black hole complementarity. *Physical Review D* **89**, 086010 (2014). ArXiv:1310.6335.

[5] Gisin, N. Weinberg's non-linear quantum mechanics and supraluminal communications. *Physics Letters A* **143**, 1–2 (1990).

[6] Polchinski, J. Weinbergs nonlinear quantum mechanics and the Einstein-Podolsky-Rosen paradox. *Physical Review Letters* **66**, 397 (1991).

[7] Bennett, C. H., Bernstein, E., Brassard, G. & Vazirani, U. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing* **26**, 1510–1523 (1997).

[8] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC)*, 212–219 (1996). ArXiv:quant-ph/9605043.

[9] Aaronson, S. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A* **461**, 3473 (2005). ArXiv:quant-ph/0412187.

[10] Brun, T. Computers with closed timelike curves can solve hard problems. *Foundations of Physics Letters* **16**, 245–253 (2003). ArXiv:gr-qc/0209061.

[11] Aaronson, S. & Watrous, J. Closed timelike curves make quantum and classical computing equivalent. *Proceedings of the Royal Society A* **465**, 631–647 (2009).

[12] Bennett, C. H., Leung, D., Smith, G. & Smolin, J. A. Can closed timelike curves or nonlinear quantum mechanics improve quantum state discrimination or help solve hard problems? *Physical Review Letters* **103**, 170502 (2009).

[13] Abrams, D. S. & Lloyd, S. Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. *Physical Review Letters* **81**, 3992 (1998). ArXiv:quant-ph/9801041.

[14] Meyer, D. A. & Wong, T. G. Quantum search with general nonlinearities. *Physical Review A* **89**, 012312 (2014). ArXiv:1310.7301.

[15] Meyer, D. A. & Wong, T. G. Completeness is unnecessary for fast nonlinear quantum search (2015). ArXiv:1502.06281.

[16] Meyer, D. A. & Wong, T. G. Nonlinear quantum search using the Gross-Pitaevskii equation. *New Journal of Physics* **15**, 063014 (2013). ArXiv:1303.0371.

[17] Childs, A. M. & Young, J. Optimal state discrimination and unstructured search in nonlinear quantum mechanics (2015). ArXiv:1507.06334.

[18] Deutsch, D. Quantum mechanics near closed timelike lines. *Physical Review D* **44**, 3197–3217 (1991).

[19] Gottesman, D. & Preskill, J. Comment on "The black hole final state". *Journal of High Energy Physics* **0403**, 026 (2004). ArXiv:hep-th/0311269.

[20] See supplemental material at [url will be inserted by publisher] for detailed proofs of these claims, which includes refs. [30–48]. .

[21] Marolf, D. & Polchinski, J. Violations of the Born rule in cool state-dependent horizons (2015). ArXiv:1506.01337.

[22] Aaronson, S., Bouland, A., Fitzsimons, J. & Lee, M. The Space "Just Above" BQP. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, ITCS '16, 271–280 (ACM, New York, NY, USA, 2016).

[23] Kaye, P., Laflamme, R. & Mosca, M. *An Introduction to Quantum Computing* (Oxford University Press, Oxford, 2007).

[24] Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, 333–342 (ACM, New York, NY, USA, 2011).

[25] Freedman, M. H., Kitaev, A. & Wang, Z. Simulation of topological field theories by quantum computers. *Commun. Math. Phys.* **227**, 587–603 (2002).

[26] Jordan, S. P., Lee, K. S. M. & Preskill, J. Quantum algorithms for quantum field theories. *Science* **336**, 1130–1133 (2012).

[27] Jordan, S. P., Lee, K. S. M. & Preskill, J. Quantum computation of scattering in scalar quantum field theories. *Quantum Information and Computation* **14**, 1014–1080 (2014).

[28] Jordan, S. P., Lee, K. S. M. & Preskill, J. Quantum algorithms for fermionic quantum field theories (2014). ArXiv:1404.7115.

[29] Aaronson, S. Is quantum mechanics an island in theoryspace? In *Proceedings of the Växjö Conference "Quantum Theory: Reconsideration of Foundations"* (2004).

[30] Leslie, M. `http://mathoverflow.net/questions/96493` (2012).

[31] Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Uni-

versity Press, 2000).

[32] Cover, T. M. & Thomas, J. A. *Elements of Information Theory* (Wiley, Hoboken, New Jersey, 1991).

[33] Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters* **70**, 1895 (1993).

[34] Zalka, C. Grover's quantum searching algorithm is optimal. *Physical Review A* **60**, 2746–2751 (1999). ArXiv:quant-ph/9711070.

[35] Valiant, L. & Vazirani, U. NP is as easy as detecting unique solutions. *Theoretical Computer Science* **47**, 85–93 (1986).

[36] Collins, B. & Sniady, P. Integration with respect to the Haar measure on unitary, orthogonal, and symplectic group. *Communications in Mathematical Physics* **264**, 773–795 (2006).

[37] Harlow, D. Jerusalem lectures on black holes and quantum information (2014). ArXiv:1409.1231.

[38] Aaronson, S. NP-complete problems and physical reality. *ACM SIGACT News* **36**, 30–52 (2005). ArXiv:quant-ph/0502072.

[39] Wigner, E. P. *Gruppentheorie und ihre Anwendung auf die Quanten mechanik der Atomspektren*, 251–254 (Friedrich Vieweg und Sohn, 1931).

[40] Aharonov, D. A simple proof that Toffoli and Hadamard are quantum universal (2003). ArXiv:quant-ph/0301040.

[41] Bae, J., Hwang, W.-Y. & Han, Y.-D. No-signaling principle can determine optimal quantum state discrimination. *Physical Review Letters* **107**, 170403 (2011). ArXiv:1102.0361.

[42] Barrett, J. Information processing in generalized probabilistic theories. *Physical Review A* **75**, 032304 (2005). ArXiv:quant-ph/0508211.

[43] Abramsky, S. & Coecke, B. Categorical quantum mechanics. In Engesser, K., Gabbay, D. & Lehmann, D. (eds.) *Handbook of Quantum Logic and Quantum Structures*, vol. 2, 261–325 (Elsevier, 2008). ArXiv:0808.1023.

[44] Ruffini, R. & Bonazzola, S. Systems of self-gravitating particles in general relativity and the concept of an equation of state. *Physical Review* **187**, 1767 (1969).

[45] Adler, S. L. *Quaternionic Quantum Mechanics and Quantum Fields* (Oxford University Press, Oxford, 1995).

[46] Harlow, D. Aspects of the Papadodimas-Raju proposal for the black hole interior. *Journal of High Energy Physics* 1411 (2014). ArXiv:1405.1995.

[47] Harlow, D. & Hayden, P. Quantum computation vs. firewalls. *Journal of High Energy Physics* **1013:85** (2013). ArXiv:1301.4504.

[48] Harlow, D. Personal communication.