Computation in generalised probabilistic theories

Ciarán M. Lee
University of Oxford
Oxford, UK
ciaran.lee@cs.ox.ac.uk

Jonathan Barrett
University of Oxford
Oxford, UK

From the general difficulty of simulating quantum systems using classical systems, and in particular the existence of an efficient quantum algorithm for factoring, it is likely that quantum computation is intrinsically more powerful than classical computation. At present, the best upper bound known for the power of quantum computation is that **BQP** $\subseteq$ **AWPP**, where **AWPP** is a classical complexity class (known to be included in **PP**, hence **PSPACE**). This work investigates limits on computational power that are imposed by simple physical, or information theoretic, principles. To this end, we define a circuit-based model of computation in a class of operationally-defined theories more general than quantum theory, and ask: what is the minimal set of physical assumptions under which the above inclusions still hold? We show that given only an assumption of tomographic locality (roughly, that multipartite states and transformations can be characterised by local measurements), efficient computations are contained in **AWPP**. This inclusion still holds even without assuming a basic notion of causality (where the notion is, roughly, that probabilities for outcomes cannot depend on future measurement choices). Following Aaronson, we extend the computational model by allowing post-selection on measurement outcomes. Aaronson showed that the corresponding quantum complexity class, **PostBQP**, is equal to **PP**. Given only the assumption of tomographic locality, the inclusion in **PP** still holds for post-selected computation in general theories. Hence in a world with post-selection, quantum theory is optimal for computation in the space of all operational theories. We then consider whether one can obtain relativised complexity results for general theories. It is not obvious how to define a sensible notion of a computational oracle in the general framework that reduces to the standard notion in the quantum case. Nevertheless, it is possible to define computation relative to a 'classical oracle'. Then, we show there exists a classical oracle relative to which efficient computation in any theory satisfying the causality assumption does not include **NP**. This provides some degree of evidence that **NP**-complete problems cannot be solved efficiently in any theory satisfying tomographic locality and causality.

Description of results

The following is an extended abstract of the paper [Lee, C. M., & Barrett, J. (2014). Computation in generalised probabilistic theories. arXiv preprint arXiv:1412.8671].

Quantum theory offers dramatic new advantages for various information theoretic tasks [1]. This raises the general question of what broad relationships exist between physical principles, which a theory like quantum theory may or may not satisfy, and information theoretic advantages. Much progress has already been made in understanding the connections between physical principles and some tasks, such as cryptography and communication complexity problems. It is now known that the degree of non-locality in a theory is related to its ability to solve communication complexity problems [2] and to its ability to perform super-dense coding, teleportation and entanglement swapping [3]. Teleportation and no-broadcasting are now better understood than they were when investigated solely from the viewpoint of quantum theory [4, 5]. Cryptographic protocols have been developed whose security relies not on aspects of the quantum formalism, but on general physical principles. For example, device-independent key

Submitted to:
QPL 2015

© C. M. Lee & J. Barrett
This work is licensed under the Creative Commons Attribution-No Derivative Works License.

distribution schemes have been developed that are secure against attacks by post-quantum eavesdroppers limited only by the no-signalling principle [6].

By comparison, relatively little has been learned about the connections between physical principles and computation. It was shown in [7] that a maximally non-local theory has no non-trivial reversible dynamics and, thus, any reversible computation in such a theory can be efficiently simulated on a classical computer. Aside from this result, most previous investigations into computation beyond the usual quantum formalism have centred around non-standard theories involving modifications of quantum theory. These theories often appear to have immense computational power and entail unreasonable physical consequences. For example, non-linear quantum theory appears to be able to solve **NP**-complete problems in polynomial time [8], as does quantum theory in the presence of closed timelike curves [9, 17]. Aaronson has considered other modifications of quantum theory, such as a hidden variable model in which the history of hidden states can be read out by the observer [11], and these have also been shown to entail computational speedups over the usual quantum formalism.

This work considers computation in a framework suitable for describing essentially arbitrary operational theories, where an operational theory specifies a set of laboratory devices that can be connected together in different ways, and assigns probabilities to experimental outcomes. Theories within this framework can be described that are different from classical or quantum theories, but which nonetheless make good operational sense and do not involve peculiarities like closed timelike curves. We work in the circuit framework for operationally defined theories [1] theories developed by Hardy in [15, 16] and Chiribella, D'Ariano and Perinotti in [12, 13]. This framework suggests a natural model of computation, analogous to the classical and quantum circuit models, which we define rigorously in the arXiv version of this work.

The strongest known non-relativised upper bound for the power of quantum computation is that the class **BQP** of problems efficiently solvable by a quantum computer is contained in the classical complexity class **AWPP**, this was proved by Fortnow and Rogers in [18]. The class **AWPP** has a slightly obscure definition, but is well known to be contained in **PP**, hence **PSPACE**. It is shown in the arXiv version of this work that the same result holds for any theory in the operational framework that satisfies the principle of tomographic locality, where this means, roughly, that transformations can be completely characterised by product states and effects. That is, if the complexity class of problems that can be efficiently solved by a specific theory **G** is denoted schematically **BGP**, then for tomographically local theories, $\mathbf{BGP} \subseteq \mathbf{AWPP}$. Once suitable definitions are in place, the proof is essentially the same as the proof for the quantum case: the idea is that this proof can be cast in a theory-independent manner, and be seen to follow from a very minimal set of assumptions on the structure of a physical theory. In fact, the containment $\mathbf{BGP} \subseteq \mathbf{AWPP}$ still holds even in the absence of a basic principle of causality (which, if it does hold, ensures that there can be no signalling from future to past).

One possible interpretation of that fact that the best known upper bounds on efficient computation in quantum theory follow from very weak assumptions on any operationally defined theory is that we should *in principle* be able to derive stronger upper bounds for the class **BQP**. Thus our results point out that the 'quantum' proofs of these upper bounds do not exploit any of the structure unique to quantum theory.

It was suggested in [14] that quantum theory achieves, in some sense, an optimal balance between its set of states and its dynamics, and that this balance entails that quantum theory is powerful for computation by comparison with most theories in the space of operational theories. Although the status of this suggestion is unknown, it turns out to be exactly correct in the context of a world allowing post-selection

[1] called generalised probabilistic theories in the literature.

of measurement outcomes. Aaronson showed that the class of problems efficiently solvable by a quantum computer with the ability to post-select measurement outcomes is equal to the class **PP** [10]. In the full paper we extend the idea of computation with post-selection to general theories, and shows that given (as always) tomographic locality, problems efficiently solvable by any theory with post-selection are contained in **PP**. In other words: any problem efficiently solvable in a tomographically local theory with post-selection, is also efficiently solvable by a quantum computer with post-selection.

Finally, oracles play a special role in quantum computation, forming the basis of most known computational speed-ups over classical computation. The last section of the full paper discusses the problem of defining a sensible notion of oracle in the general framework, that reduces to the standard definition in quantum theory. This problem may not have a solution that is completely general, hence we introduce instead a notion of 'classical oracle' that can be defined in any theory that satisfies the causality principle. Given this definition, we show that there exists a classical oracle such that relative to this oracle, **NP** is not contained in **BGP** for any theory **G** satisfying tomographic locality and causality . This might be seen as some kind of evidence that **NP**-complete problems cannot be solved efficiently by general theories satisfying these two constraints.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and Quanum information*. Cambridge University press, 2000.

[2] W. van Dam, *Implausible consequences of superstrong nonlocality*. arXiv:quant-ph/0501159, 2005.

[3] A. J. Short and J. Barrett, *Strong nonlocality: A trade-off between states and measurements*. New Journal of Physics 12, 033034, 2010.

[4] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, *Teleportation in General Probabilistic theories*. arXiv:quant-ph/0805.3553, 2008.

[5] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, *A generalized no-braodcasting theorem*. Phys. Rev. Lett 99.240501, 2007.

[6] J. Barrett, L. Hardy, and A. Kent, *No Signalling and Quantum key Distribution*. Phys. Rev. Lett 95, 010503, 2005.

[7] D. Gross, M. Mueller, R. Colbeck, and O. Dahlsten, *All reversible dynamics in maximal non-local theories are trivial*. Phys. Rev. Lett. 104, 080402, 2010.

[8] D. S. Abrams and S. Lloyd, *Nonlinear quantum mechanics implies polynomial-time solution for NP-complete problems*. Phys. Rev. Lett 81, 3992-3995, 1998.

[9] D. Bacon, *Quantum computational complexity in the presence of closed timelike curves*. Phys. Rev. A 70, 032309, 2004.

[10] S. Aaronson, *Quantum computing, postselection and probabilistic polynomial time*. arXiv:quant-ph/0412187v1, 2004.

[11] S. Aaronson, *Quantum Computing and Hidden Variables II: The Complexity of Sampling Histories*. arXiv:quant-ph/0408119, 2004.

[12] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Probabilistic theories with purification*. Phys. Rev. A 81, 062348, 2010.

[13] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Informational derivavtion of Quantum Theory*. Phys. Rev. A 84, 012311, 2011.

[14] J. Barrett, *Information processing in generalised probabilitic theories*. Phys. Rev. A 75 No. 3, 032304, 2007.

[15] L. Hardy, *Quantum theory from five reasonable axioms*. arXiv:quant-ph/0101012v4, 2001.

[16] L. Hardy, *Reformulating and reconstructing quantum theory*. arXiv:quant-ph/1104.2066v3, 2011.

[17] J. Allen, *Treating time travel quantum mechanically*. Phys. Rev. A 90(4) 042107, 2014.

[18] L. Fortnow and J. Rogers, *Complexity limitations on quantum computation*. arXiv:cs/9811023v1, 1998.