Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy

Michael J. Bremner[1], Richard Jozsa[2] and Dan J. Shepherd[3]

[1] *Institut für Theoretische Physik, Leibniz Universität Hannover,
Appelstrasse 2, 30167 Hannover, Germany.*

[2] *DAMTP, Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge CB3 0WA, U.K.*

[3] *CESG, Hubble Road, Cheltenham GL51 0EX, U.K.*

Abstract

We consider quantum computations comprising only commuting gates, known as IQP computations, and provide compelling evidence that the task of sampling their output probability distributions is unlikely to be achievable by any efficient classical means. More specifically we introduce the class post-IQP of languages decided with bounded error by uniform families of IQP circuits with post-selection, and prove first that post-IQP equals the classical class PP. Using this result we show that if the output distributions of uniform IQP circuit families could be classically efficiently sampled, either exactly in total variation distance or even approximately up to 41% multiplicative error in the probabilities, then the infinite tower of classical complexity classes known as the polynomial hierarchy, would collapse to its third level. We mention some further results on the classical simulation properties of IQP circuit families, in particular showing that if the output distribution results from measurements on only $O(\log n)$ lines then it may in fact, be classically efficiently sampled.

See [1] (arXiv:1005.1407) for the technical version and [2] (arXiv:1005.1744) for closely related work.

From a pragmatic point of view the field of quantum computing is driven by the expectation that quantum algorithms can offer some computational complexity benefits transcending the possibilities of classical computing. But this expectation can be challenged both theoretically and experimentally: (a) there is yet no theoretical proof that any quantum algorithm outperforms the best classical algorithm for the task, in the standard computational setting of polynomial vs. exponential running time (without inclusion of further constructs, such as use of oracles, or consideration of distributed computing and the role of communication; in both these scenarios there are indeed proofs of exponential complexity benefits); (b) experimentally there are well documented difficulties associated with building a quantum computer that is suitably fault tolerant and sufficiently scalable to manifestly demonstrate a complexity benefit.

However both (a) and (b) can, to some extent, be redressed by further examination: the criticism in (a) can be attributed to limitations of *classical* complexity theory – we do have interesting quantum algorithms (such as Shor's factoring algorithm) for problems widely believed to be classically hard but there is no proof of the latter. Proof of classical hardness is a notoriously difficult issue (cf the famous P vs. NP question) and it has become popular to resort to providing only evidence of hardness, as follows: we prove that if a certain problem were classically easy then this would entail consequences that are highly implausible (although also generally unproven) e.g. collapse of an entire complexity class (such as entailing that P = NP). For (b) we could seek to devise a computational task that, on the one hand is expected to be classically hard (as above) yet on the other hand, can be implemented using suitably simple (sub-universal) quantum computational elements that are especially easily or fault-tolerantly implementable within some specific experimental scheme. In this paper we develop a family of such computational tasks (that amount to sampling from suitably prescribed probability distributions).

Recently Aaronson and Arkhipov have built a compelling alternate approach to similar issues [3, 4]. More generally there has been increasing interest in physically restricted forms of quantum computing and a study of associated complexity classes [5, 6, 7, 8, 9]. interesting

We consider so-called temporally unstructured quantum computations (also known as IQP or "instantaneous" quantum computation) introduced in [10, 7]. Our main result is to demonstrate that if quantum circuits comprising 2-qubit *commuting* gates could be simulated classically (even up to a generous multiplicative error tolerance as described below and in [1]) then the infinite tower of complexity classes known as the polynomial hierarchy (PH), would collapse to its third level (see theorem 2 and corollary 1 in [1]). While not implying that P=NP, such a collapse is nevertheless widely regarded as being similarly implausible. Apart from their tantalising theoretical simplicity, such circuits of only commuting gates are known to be of significance for super- and semi-conductor qubit implementations, where it has recently been shown [11] that they are much simpler to implement fault-tolerantly than gates drawn from a fully universal set. IQP computations can can also be implemented as non-adaptive measurement-based quantum computations [7] .

A significant ingredient in our derivations will be the notion of a post-selected quantum computation. Aaronson [12] has shown that if post-selection is included with universal polynomial time quantum computation then the computational power is boosted from BQP to the classical class PP. We will show that, somewhat surprisingly, post-selection boosts the power of the much weaker class of polynomial time IQP computations to PP too. It is worth noting that the methods used to prove our main result can be applied to any class of circuits that similarly goes to PP under post-selection in order to show analogous simulation hardness results.

While our main theorem holds equivalently for IQP circuits as well as generic polynomial time quantum circuits, we see a clear deviation in complexity emerge if the size of the output register is restricted. We prove that if the output register of a polynomial time IQP computation (with $O(\text{poly}(n))$ qubits) is restricted to $O(\log n)$ qubits then it is always efficiently classically simulable (see theorem 3 in [1] also theorems 4, 5, 6 and 7 in [2] for alternate, and stronger, proofs which utilize connections between IQP computations and the evaluation of Tutte polynomials). This is in stark contrast to the corresponding situation for generic polynomial time quantum circuits where such a result would imply that BQP=BPP. Put together, our results suggest a distinction between the classical simulability of IQP bounded error decision problems versus IQP sampling problems which is unlikely to occur for more powerful classes (for instance BQP versus SampBQP).

The notion of classical simulation that applies in our main result is an especially weak one – broadly speaking (cf precise definitions in [1]) given a description of a quantum circuit we ask for a classical process that can provide a sample of a probability distribution, that approximates the output distribution of the quantum process to a suitable multiplicative accuracy. A more commonly used notion of approximation for probability distributions is that of an *additive* approximation (or approximation in total variation distance) which often features in the analysis of imperfections in physical implementations. However there appears to be no useful relationship between additive and multiplicative tolerances, and the proof of our main result remains valid in the context of additive approximations only if the classical simulation is required to be *exact*. The admissability of multiplicative, in contrast to additive, approximation arises from our use of post-selection cf. theorem 2 in [1]. By alternately focusing on *counting problems* instead of decision problems Aaronson and Arkhipov have recently given a persuasive argument that the efficient classical simulation of sampling from linear (quantum) optical circuits to within an additive bound would lead to a similar collapse in the polynomial hierarchy as presented here, providing two conjectures hold true [3, 4].

A very much stronger notion of simulation sometimes used in the literature (which we shall call a strong simulation) is to ask for a classical efficient computation of the *value* of any marginal or total output probability, to exponential precision. Previously it was known [13, 14] that the existence of such strong simulations for some classes of quantum computations would imply the collapse of the polynomial hierarchy. Our result contrasts with these works in the striking simplicity of the quantum processes being considered and in the very much weaker requirements in the classical simulation.

References

[1] M. J. Bremner, R. Jozsa and D. Shepherd *Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. R. Soc. A* Published online before print, doi: 10.1098/rspa.2010.0301 (2010). arXiv:1005.1407.

[2] D. Shepherd, *Binary matroids and quantum probability distributions* (2010), arXiv:1005.1744.

[3] S. Aaronson and A. Arkhipov, *New evidence that quantum mechanics is hard to simulate on classical computers*, talk at QIP2010, Zürich, January 2010.

[4] S. Aaronson and A. Arkhipov, *The Computational Complexity of Linear Optics* (2010), arXiv:1011.3245.

[5] D. Browne, E. Kashefi and S. Perdrix, *Computational depth complexity of measurement-based quantum computation*, arXiv:0909.4673

[6] S. Jordan, *Permutational quantum computing*, arXiv:0906.2508.

[7] D. Shepherd and M. J. Bremner, *Temporally unstructured quantum computation*, *Proc. R. Soc. A* **465**, 1413-1439 (2009). arXiv:0809.0847.

[8] M. Van den Nest, *Simulating Quantum Computers With Probabilistic Methods*, arXiv:0911.1624

[9] R. Jozsa, B. Kraus, A. Miyake and J. Watrous, *Matchgate and space-bounded quantum computations are equivalent*, *Proc. R. Soc. A* **466**, 809-830 (2010). arXiv:0908.1467.

[10] D. J. Shepherd, *Quantum complexity: restrictions on algorithms and architectures*, PhD thesis, University of Bristol 2009.

[11] P. Aliferis, F. Brito, D. P. DiVincenzo, J. Preskill, M. Steffen, and B. M. Terhal, *Fault-Tolerant Computing With Biased-Noise Superconducting Qubits*, New J. Phys. **11** (2009) 013061, arXiv:0806.0383.

[12] S. Aaronson, *Quantum computing, post-selection and probabilistic polynomial time*, *Proc. R. Soc. A* **461**, 3473-3483 (2005). arXiv:quant-ph/0412.187.

[13] B. Terhal and D. DiVincenzo, *Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games*, *Quant. Inf. Comp.* **4**, 134-145 (2004). arXiv:quant-ph/0205133.

[14] S. Fenner, F. Green, S. Homer and Y. Zhang, *Bounds on the power of constant-depth quantum circuits*, *Proc. 15*$^{\text{th}}$ *Int. Symp. on F. C. T.* p44-55, 2005, arXiv:quant-ph/0312209.