Exponential Quantum Speed-ups are Generic

Fernando G.S.L. Brandão and Michał Horodecki

I. ABSTRACT

A central problem in quantum computation is to understand which quantum circuits are useful for exponential speed-ups over classical computation. We address this question in the setting of query complexity and show that for almost any sufficiently long quantum circuit one can construct a black-box problem which is solved by the circuit with a constant number of quantum queries, but which requires exponentially many classical queries, even if the classical machine has the ability to postselect.

We prove the result in two steps. In the first, we show that almost any element of an approximate unitary 3-design is useful to solve a certain black-box problem efficiently. The problem is based on a recent oracle construction of Aaronson [1] and gives an exponential separation between quantum and classical bounded-error with postselection query complexities.

In the second step, which may be of independent interest, we prove that linear-sized random quantum circuits give an approximate unitary 3-design. The key ingredient in the proof is a technique from quantum many-body theory to lower bound the spectral gap of local quantum Hamiltonians.

II. BACKGROUND AND MOTIVATION

In a recent breakthrough in quantum query-complexity, Aaronson [1] proposed a new oracle problem as a candidate to put BQP outside the polynomial hierarchy (PH). Although the usefulness of this oracle for the BQP vs. PH question still has to be elucidated, the problem was shown to have a huge separation of quantum and classical query complexities: it can be solved by a constant number of quantum queries, while it requires exponentially many queries by a classical machine, even if we give the classical machine the – extremely powerful – ability to *postselect* on a given result of the computation. This problem can also be used to prove all known oracle separations of BQP and classical complexity classes.

Aaronson's problem, named Fourier Checking, is the following: We are given two boolean functions $f, g : \{0,1\}^n \to \{-1,1\}$ with the promise that either

- f and g are chosen uniformly at random, or
- for a vector $v \in \mathbb{R}^{2^n}$ with entries v_x drawn independently from a normal distribution of mean 0 and variance 1, the functions are chosen as $f(x) = \text{sgn}(v_x)$ and $g(x) = \text{sgn}(\hat{v}_x)$. Here the vector $\hat{v}$ is the Fourier transform over $\mathbb{Z}_2^n$ of v and is given by
$$\hat{v}_x = \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} v_y. \tag{1}$$

The task is to decide which is the case. In words, we should determine if the two functions are not correlated at all or if one of them is well correlated with the Fourier transform of the other.

Considering how well this problem fleshes out the superiority of quantum computation to classical, it is worthwhile to try to understand what exactly gives its strength. For instance, what is the role played by the Fourier transform, both the the definition of the problem and in the quantum algorithm solving it? Can we replace it by some other transformation? One of the contributions of our work is to shed light on these questions.

From a broader perspective, we are concerned with the following question, central to our understanding of the computational capabilities offered by quantum mechanics: What is the set of quantum circuits which provide large quantum speed-ups? More precisely, for which quantum circuits can we construct black-box problems which are solved by the circuit with only a few queries to the black-box, but which require a large number of queries for randomized classical computation? This question is in a sense a converse to the well-studied problem of characterizing the class of black-box problem whose solutions have significant quantum speed-ups (see e.g. [2, 3]).

III. OUR RESULTS

In our paper [4] we generalize the Fourier Checking problem [1] and show that the Fourier transform, both in the definition of the problem and in the quantum algorithm solving it, can be replaced by a large class of quantum circuits. These include both the Fourier transform over *any* (possibly non-abelian) finite group and *almost any* sufficiently long quantum circuit from a natural distribution on the set of quantum circuits. We obtain *exponential* separations of quantum and postselected classical query complexities for all such circuits.

Our result is of a similar flavor to Harrow and Hallgren's generalization of the resursive fourier sampling problem to generic circuits [5]. However, while they could only show a constant vs. linear separation of quantum and classical query complexities (which can be boosted to a polynomial versus superpolynomial one by recursion), we are able to show a *constant* vs. *exponential* separation, even allowing the classical machine the ability to postselect on computation outcomes.

Flat circuits imply exponential separation: In more detail, we first introduce a simple new measure of flatness, or dispersiveness, of a unitary U on n qubits, denoted $C(U)$. It is defined as the minimal *min-entropy* of the outcome probability distribution of a computational basis measurement on $U|j\rangle$. It thus measures the worst-case dispersiveness of states obtained by applying U to computational basis states.

Then we define the black-box problem U-CIRCUIT CHECKING, a variant of fourier checking in which the Fourier transform in the definition of the vector $\hat{v}$ (given by Eq. (1)) is replaced by U. On a quantum computer we can solve U-CIRCUIT CHECKING as follows: we prepare each qubit in the $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ state, forming the uniform superposition over the computational basis. Then we query the f function, apply the circuit U, query the g function, and measure each qubit in the Hadamard basis, accepting if all of them are found in the $|+\rangle$ state.

Theorem I *For any circuit U acting on n qubits for which $C(U) = \Omega(n)$ the problem* U-CIRCUIT CHECKING *shows an exponential separation of quantum and postselected classical query complexities.*

Therefore we can identity the *flatness* of the circuit U, represented by a large $C(U)$, as the crucial property behind the quantum speed-ups in U-CIRCUIT CHECKING.

We then proceed by giving two classes of unitaries with $C(U) = \Omega(n)$.

Theorem II

> *(i) Let $U_{\text{QFT}}(G)$ be the quantum Fourier transform over the finite group G. Then $C(U_{\text{QFT}}(G)) \geq \frac{1}{2}\log|G|$.*
>
> *(ii) Given any 2^{-3tn}-approximate unitary t-design on n qubits, all but a $2^{-(t(1-\beta)-2)n+1}$ fraction of its elements have $C(U) \geq \beta n$.*

In particular, we find that for 2^{-9n}-approximate unitary 3-designs, all but a $2^{-n/2+1}$ fraction of its element have $C(U) \geq n/6$. We note that our construction do not work for approximate unitary 2-design and thus gives the first application of a unitary 3-design.

Random circuits are unitary 3-designs: A unitary t-design is an ensemble of unitaries $\{\mu(dU), U\}$, for a measure μ on the set of unitaries, such that the average (over μ) of any t-degree polynomial on the entries of U and their complex conjugates is equal to the average over the Haar measure. An approximate unitary t-design is a relaxed version of the previous definition, in which we only require that the averages are ε-close to each other.

In a series of papers it was established that polynomially long random quantum circuits (with each step given by an application of a random two-qtubit gate to two randomly chosen qubits) constitute an approximate unitary 2-design. Although there is evidence that random quantum circuits of polynomial lenght are unitary t-design for every $t = \mathrm{poly}(n)$, this has not been rigorously proved so far, even for the 3-design case.

Here we prove that random quantum circuits are indeed approximate unitary 3-designs.

Theorem III *$O(n \log(1/\varepsilon))$-size random quantum circuits form an ε-approximate unitary 3-design.*

The proof of Theorem III is based on a reduction connecting the convergence rate of moments of the random quantum circuit to the spectral gap of a quantum local Hamiltonian. Our main contribution is to show that we can obtain a lower bound on this spectral gap employing a technique from quantum many-body theory used e.g. in [6–8].

In particular, we are able to reduce the problem of bounding the spectral gap of the random walk on n qubits induced by the random circuit, to bounding the spectral gap of the same random walk, but now only defined on *three* neighbouring qubits. Then it suffices to bound the convergence time of the second and third moments of the latter random walk in order to prove that the random circuit constitute a 3-design. We believe our approach is promising also for higher values of t and might pave the way to a proof that random quantum circuits are approximate unitary t-designs for all $t = \mathrm{poly}(n)$.

Combining Theorems III and II we obtain our main result that almost any quadratic-sized quantum circuit is useful for exponential quantum speed-ups.

Theorem IV *For the distribution induced by a random quantum circuit of length $O(n^2)$ on n qubits, all but an exponential small fraction of quantum circuits U are such that* U-CIRCUIT CHECKING *shows an exponential gap in the quantum and the postselected classical query complexities.*

The role of $C(U)$ and classical efficient solution for sparse unitaries: We have seen that dispersive unitaries U with large $C(U)$ give an exponential speed-up in U-CIRCUIT CHECKING. Is a large $C(U)$ always required for a speed-up? We present two results indicating that this is indeed the case.

First we show that with a modified notion of oracle access in which a different independent realization of the random parameters of the oracle is chosen in each query, a linear $C(U)$ is also *necessary* for an exponential speed-up. Second we consider the U-CIRCUIT CHECKING problem for *approximately-sparse U*, defined as unitaries which can be approximated (in operator norm) by a sparse matrix with only polynomially many non-zero entries in each row and column, and show the randomized classical query complexity to be polynomial in this case.

[1] S. Aaronson. BQP and the Polynomial Hierarchy. *FOCS 2010*. arXiv:0910.4698v1.

[2] R. Beals, H. Buhrman, R. Cleve, M. Mosca and R. de Wolf. Quantum Lower Bounds by Polynomials. J. ACM **48**, 778 (2001).

[3] S. Aaronson and A. Ambainis. The Need for Structure in Quantum Speedups. arXiv:0911.0996.

[4] F.G.S.L. Brandão and M. Horodecki. Exponential Quantum Speed-ups are Generic. arXiv:1010.XXX.

[5] S. Hallgren and A.W. Harrow. Superpolynomial speedups based on almost any quantum circuit. *In Proc. of the 35th International Colloquium on Automata, Languages and Programming (ICALP 2008), LNCS 5125, pp. 782-795*. arXiv:0805.0007

[6] M. Fannes, B. Nachtergaele, and R. F. Werner. Finitely correlated states on quantum spin chains. Comm. Math. Phys. **144**, 443 (1992).

[7] D. Perez-Garcia, F. Verstraete, M.M. Wolf, and J.I. Cirac. Quantum Inf. Comput. **7**, 401 (2007).

[8] R. Alicki, M. Fannes and M. Horodecki. On thermalization in Kitaev's 2D model. J. Phys. A: Math. Theor. **42**, 065303 (2009)