Non-Identity Check Remains QMA-Complete for Short Circuits

Zhengfeng Ji
Perimeter Institute for Theoretical Physics, Waterloo Ontario, Canada.

Xiaodi Wu
Institute for Quantum Computing, University of Waterloo, Ontario, Canada,
Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, USA.

June 30, 2008

The Non-Identity Check problem asks whether a given a quantum circuit is far away from the identity or not. It is
well known that this problem is QMA-Complete [14]. In this note, it is shown that the Non-Identity Check problem
remains QMA-Complete for circuits of short depth. Specifically, we prove that for constant depth quantum circuit in
which each gate is given to at least $\Omega(\log n)$ bits of precision, the Non-Identity Check problem is QMA-Complete. It
also follows that the hardness of the problem remains for polylogarithmic depth circuit consisting of only gates from
any universal gate set and for logarithmic depth circuit using some specific universal gate set.

1 Introduction

Quantum circuit is the natural quantum analog of classical circuit and an important model [30] to analyze the power of
quantum computation. A quantum circuit is an acyclic network of quantum gates connected by wires. The quantum
gates represent feasible quantum operations (unitary operations in our model), involving constant numbers of qubits.
The depth of a circuit is the maximum number of quantum gates affecting on any qubit from input to output.

Much of the difficulty in implementing quantum computation is the decoherence effect of the qubits which happens
in a very short time. Short depth quantum circuit seems to provide a way to implement as much quantum computation
as possible in very limited available time due to the decoherence effect. Thus, analyzing the power of short depth
quantum circuit is of significant interest.

A few examples about the power of logarithmic depth quantum circuit have been proposed in the past few
years [8, 22]. Besides, a systematic procedure has also been discovered [6] to parallelize a class of quantum cir-
cuits to logarithmic depth. The investigation of the power of constant depth quantum circuit has also been started
recently [12, 27]. In this paper, we prove the hardness of the Non-Identity Check problem for such short depth quan-
tum circuits.

The Non-Identity Check problem is to decide if a quantum circuit is far away from the identity, given a classical
description of the circuit. More generally, one can ask whether two quantum circuits $U$ and $V$ are equivalent or not.

But is it easy to see that the equivalence problem can be reduced to the identity check problem of $UV^\dagger$. Classically,
similar problems [5, 26, 31] determine whether two given classical circuits are equivalent or not. It turns out that the
classical problem can be solved efficiently using a randomized algorithm. That is, the classical problem is in BPP.

In contrast, we know that the quantum Non-Identity Check problem is QMA-Complete [14]. This means that the
problem is hard even for quantum computers. Moreover, as will be shown in this paper, the hardness remains even
when only short depth circuits are considered.

The complexity class QMA is the quantum version of NP. It differs from NP in that the witness can be a quantum
state and that the verifier has the power of performing polynomial time quantum computation. A lot has been known
about this complexity class. One of the most important facts is that it has a complete problem which naturally gen-
eralizes the Boolean Satisfiability problem. The first proof of it by Kitaev [18] serves as the quantum analog of the
Cook-Levin theorem [9, 19]. The survey [3] may also be helpful in understanding the original proof.

TheLocal Hamiltonian problem has been the first known important complete problem for QMA and has also
turned out to be the most studied one. In fact, the last few years have witnessed a series of improvements on it [14,
16, 15, 23, 1], culminating in the result that the problem remains complete even for 1-D local Hamiltonian. Another
complete problem for QMA is Non-Identity Check [14], which is also the main topic of this paper. There haven’t been
many QMA-Complete problems found. In addition to the Local Hamiltonian and Non-Identity Check problem, we also know that the Local Consistency problem and related variants \cite{20,21,29} and the Quantum Clique Problem \cite{4} are QMA-Complete.

The main result of this paper is that Non-Identity Check for short quantum circuits remains QMA-Complete. Formally, we have:

**Theorem 1.** Non-Identity Check of constant depth quantum circuit on \( n \) qubits is QMA-Complete if the encoding of the circuit describes each gate to at least \( \Omega(\log n) \) bit of precision.

When a circuit is restricted to consisting of only gates from a finite universal gate set, we can have the following Corollary, which is a direct application of the Solovay-Kitaev Theorem \cite{10}.

**Corollary 1.** Non-Identity Check is QMA-Complete for \( O(\log^5(n)) \)-depth quantum circuits of an arbitrary universal gate set on \( n \) qubits where \( \delta \approx 3 \).

Interestingly, there are more efficient universal gate sets as shown in Ref. \cite{13}. With these special universal gate sets, we could have even shorter depth quantum circuits. Precisely,

**Corollary 2.** There exists a universal gate set such that Non-Identity Check is QMA-Complete for logarithmic depth quantum circuits using this particular universal gate set.

In previous works where the depth is not an issue, it is not necessary to distinguish whether the encoding of the circuit uses a fixed universal gate set or not. But this subtlety is the key point that makes the difference in Theorem 1 and Corollary 1 and 2.

To prove Theorem 1, we will employ the 1-D local Hamilton problem (QMA-Complete) as our starting point, and reduce it to a short circuit Non-Identity Check problem. The reminder of the paper is organized as follows. In the next section, some definitions and notations are summarized. In Section 3, our main result is proved. We conclude with Section 4.

## 2 Preliminary

In this section, we explain the notions used in the rest of the paper.

The spectral norm \( \|A\| \) of matrix \( A \) is defined as

\[
\|A\| = \max_{|\psi⟩} \frac{\|A|\psi⟩\|}{\||\psi⟩\|},
\]

and the trace norm \( \|A\|_{\text{tr}} \) defined as

\[
\|A\|_{\text{tr}} = \text{tr} \sqrt{A^†A}.
\]

The numerical range of a matrix \( A \) is the subset of the complex plain \( \{⟨\psi|A|\psi⟩\} \) and is known to be a convex set. In particular, for normal matrices the numerical range is simply the convex hull of all eigenvalues. For any Hermitian matrix \( H \), \( \lambda_{\max}(H) \) and \( \lambda_{\min}(H) \) are the largest and smallest eigenvalue of \( H \). Denote the eigenvalue range of \( H \) by \( \lambda(H) = \lambda_{\max}(H) - \lambda_{\min}(H). \)

The eigenvalues of a unitary matrix \( U \) lie on the unit circle of the complex plain. The distribution of the eigenvalues is important to characterize the closeness of \( U \) to identity \( I \). See for example the illustration made in Figure \[1\] where the eigenvalues of \( U \) are marked on the unit circle as small hollow circles. Use \( \alpha_{\max}(U) \) and \( \alpha_{\min}(U) \) to denote the maximal and minimal value of the arguments of eigenvalues of \( U \) taken in the interval \( (-\pi, \pi] \). They correspond to the argument of point \( A \) and \( C \) in Figure \[1\]. Let \( \tilde{\alpha}(U) \) be the length of the shortest arc that contains all eigenvalues of \( U \) (which corresponds to arc \( AC \) in the figure). It was known that \( U \) is perfectly distinguishable from \( I \) if and only if \( \tilde{\alpha}(U) \geq \pi \) \[11\]. Define a new quantity called phase range as

\[
\alpha(U) = \min\{\pi, \tilde{\alpha}(U)\},
\]

and extend it to be defined on two unitary operations \( U \) and \( V \) as

\[
\alpha(U, V) = \alpha(U^†V).
\]
The diamond norm \([17]\) serves as a good way of measuring distance of quantum operations. For a superoperator \(\Phi\) mapping operators acting on Hilbert space \(\mathcal{H}_1\) to operators acting on Hilbert space \(\mathcal{H}_2\), define the diamond norm of \(\Phi\) as
\[
\|\Phi\|_\Diamond = \max_\rho \|\Phi \otimes I_{\mathcal{H}_1}(\rho)\|_\text{tr},
\]
where the maximum is take over density matrices \(\rho\).

Let \(U\) be the quantum operation corresponding to unitary \(U\) as
\[
U(\rho) = U\rho U^\dagger.
\]
It was known that \([28]\)
\[
\|U - I\|_\Diamond = 2\sqrt{1 - \nu^2(U)},
\]
where \(I\) is the identity operation and \(\nu(U)\) is the minimum distance of the zero point to the numerical range of \(U\). As \(U\) is normal, its numerical range is the convex hull of all of its eigenvalues and the diamond norm is exactly the length of segment \(AC\) in Figure 1. Therefore, we have
\[
\|U - I\|_\Diamond = 2\sin \frac{\alpha(U)}{2}.
\]

Another way to measure the closeness of \(U\) and \(I\) is the following quantity \([14]\):
\[
\min_{\varphi} \|U - e^{i\varphi}I\|.
\]
We can also visualize the idea of the definition in Figure 1. The minimum in Eq. (4) will be achieved when \(\varphi\) is the argument of point \(B\) in the middle of the arc connection \(A\) and \(C\), and the minimum value is the length of segment \(AB\). Its relation with phase range \(\alpha\) when \(\alpha(U) < \pi\) is
\[
\min_{\varphi} \|U - e^{i\varphi}I\| = 2\sin \frac{\alpha(U)}{4}.
\]
When \(\alpha(U) = \pi\), they are not related but we will always have
\[
\min_{\varphi} \|U - e^{i\varphi}I\| \geq 2\sin \frac{\alpha(U)}{4}.
\]

In the rest of this section, we give the definition of complexity class \(\text{QMA}\) and some of its complete problems.

Let \(\Sigma\) be the alphabet \(\{0, 1\}\) and denote by \(|x|\) the length of string \(x\). A family of unitary quantum circuits \(\{U_x, x \in \Sigma^*\}\) is said to be generated in polynomial-time if there is a classical deterministic Turing machine which, on input \(x\), outputs the encoding of circuit \(U_x\) in time polynomial in \(|x|\). A circuit accepts its input state if the first output qubit is measured to be “1”.

The complexity class \(\text{QMA}\) can be defined as follows.

**Definition 1 (QMA).** A language \(L\) is in \(\text{QMA}\) if there is a family of circuits \(\{U_x, x \in \Sigma^*\}\) generated in polynomial-time together with a polynomial \(m\) such that \(U_x\) acts on \(m + k\) qubits and the following holds:
1. If $x \in L$, there exists an $m(|x|)$-qubit state $|\psi\rangle$ such that $\Pr[U_x \text{ accepts } |\psi\rangle \otimes |0\rangle^{\otimes k(|x|)}] \geq 2/3$;

2. If $x \notin L$, for all $m(|x|)$-qubit state $|\psi\rangle$, $\Pr[U_x \text{ accepts } |\psi\rangle \otimes |0\rangle^{\otimes k(|x|)}] \leq 1/3$.

QMA has complete problems. We will make use of the completeness of the Local Hamiltonian problem, especially its 1-D version. Therefore, it will be discussed in more detail although the main focus of this paper is the Non-Identity Check problem.

Consider a Hamiltonian $H$ of an $n$-particle system with constant local dimension. $H$ is called $k$-local if it is the sum $\sum_i H_i$ where each $H_i$ acts non-trivially only on $k$ particles. Sometimes, there is also an underlying layout of the particles in the problem, for example 1-D chain or 2-D lattice, such that each local term $H_i$ acts only on neighbouring particles corresponding to the layout. We will call them $k$-D Hamiltonian for units $k$-D local Hamiltonian problem respectively. For 1-D Hamiltonian $H = \sum H_i$, the particles are arranged on a line, and each local term $H_i$ acts non-trivially only on two neighbouring particles.

The general Local Hamiltonian problem can be formalized as in the following definition.

**Definition 2** (Local Hamiltonian Problem). Given a $k$-local Hamiltonian $H = \sum_{i=1}^{r} H_i$ of $n$ particles and two real numbers $a, b$, where $H_i$ has bounded norm and $b - a \geq 1/\text{poly}(n)$, $r$ is polynomial in $n$ and $k$ is $O(1)$. It is promised that the lowest eigenvalue of $H$ is either smaller than $a$ or larger than $b$. Output “Yes” in the first case and “No” otherwise.

The problem was first shown to be QMA-Complete for 5-local Hamiltonian \cite{18,3}. Recent developments have improved this to Hamiltonians with much simpler structures – the 3-local, 2-local, 2-D, and even 1-D cases – all proved to be complete for QMA \cite{16,15,23,1}.

Non-Identity Check problem was first considered in Ref. \cite{14}. It can be stated as:

**Definition 3** (Non-Identity Check). Given a classical description of a quantum circuit $U$ on $n$ qubits and two real numbers $a, b$ with $b - a \geq 1/\text{poly}(n)$. It is promised that

$$\min_{\varphi} \|U - e^{i\varphi}I\|$$

is either larger than $b$ or smaller than $a$. Output “Yes” in the first case and “No” in the second.

In the definition of the problem, the quantity $\min_{\varphi} \|U - e^{i\varphi}I\|$ is used to evaluate the closeness of $U$ to identity. We can also use phase range $\alpha(U)$ or diamond norm instead. And it’s easy to see that, all the three definitions mentioned above can be used in defining the Non-Identity Check problem without changing anything. The point is that they are quantities related to each other by monotonic trigonometric functions. Moreover, the inverse polynomial gap in one of them implies that in the others. In the next section, we will use phase range to define and analyze the Non-Identity Check problem. It is interesting to note at this point that the hardness of Non-Identity Check implies that of the estimation of the diamond norm of the difference of two unitary quantum circuits to inverse polynomial precision.

### 3 Hardness of Non-Identity Check for Short Circuits

We will prove the hardness of Non-Identity Check problem for short circuits by reducing the 1-D Local Hamiltonian problem to it. The main technical tool is $\alpha, \alpha_{\text{max}}, \alpha_{\text{min}}$ discussed in Section \cite{2} Namely, the following lemmas will be useful in the proof. The first two can be found in the Appendix of Ref. \cite{7} and we won’t prove them here.

**Lemma 1.** For unitary $U_1$ and $U_2$ such that

$$\alpha_{\text{max}}(U_1) + \alpha_{\text{max}}(U_2) < \pi,$$

$$\alpha_{\text{min}}(U_1) + \alpha_{\text{min}}(U_2) > -\pi,$$

we have

$$\alpha_{\text{max}}(U_1U_2) \leq \alpha_{\text{max}}(U_1) + \alpha_{\text{max}}(U_2),$$

$$\alpha_{\text{min}}(U_1U_2) \geq \alpha_{\text{min}}(U_1) + \alpha_{\text{min}}(U_2).$$
Lemma 2. For Hermitian $H$, $K$ and $-\pi < H + K < \pi$,
\[
\alpha_{\text{max}}(e^{iH} e^{iK}) \leq \alpha_{\text{max}}(e^{i(H+K)}),
\]
\[
\alpha_{\text{min}}(e^{iH} e^{iK}) \geq \alpha_{\text{min}}(e^{i(H+K)}).
\]

Lemma 3. $\alpha(U_1, U_2) \leq \alpha(U_1) + \alpha(U_2)$.

Proof. If either $\alpha(U_1)$ or $\alpha(U_2)$ equals $\pi$, the above equation obviously holds. Now if both $\alpha(U_1)$ and $\alpha(U_2)$ is less than $\pi$, we can choose phases $\varphi_1$ and $\varphi_2$ such that
\[
U_1^\dagger = e^{i\varphi_1} V_1, U_2 = e^{i\varphi_2} V_2,
\]
and $V_1$ and $V_2$ have eigenvalues of arguments in $(-\pi/2, \pi/2)$. The condition in Lemma 1 holds for $V_1$ and $V_2$ and it follows that $\alpha(V_1 V_2) \leq \alpha(V_1) + \alpha(V_2)$ which finishes the proof by noticing that $\alpha(U)$ is invariant under the change of a global phase in $U$.

It’s interesting to note that Lemma 3 implies that $\alpha(U_1, U_2)$ is a distance measure on the space of $U(d)/U(1)$. Specifically,
\[
\alpha(U_1, U_3) = \alpha(U_1^2 U_2 U_3) \leq \alpha(U_1^2 U_2) + \alpha(U_2 U_3) = \alpha(U_1, U_2) + \alpha(U_2, U_3).
\]

Lemma 4. For unitary $U$ and $V$, $|\alpha(U) - \alpha(V)| \leq \pi \|U - V\|$. 

Proof. Since $\alpha$ is a distance measure,
\[
|\alpha(U) - \alpha(V)| = |\alpha(U, I) - \alpha(V, I)| \leq \alpha(U^\dagger V).
\]

Using Eq. (5) and $\sin(x) \geq 2x/\pi$ for $x \in [0, \pi/2]$, we have
\[
\|U - V\| \geq \min_\varphi \|U - e^{i\varphi} V\| \geq 2 \sin \frac{\alpha(U^\dagger V)}{4} \geq \frac{1}{\pi} \alpha(U^\dagger V) \geq \frac{1}{\pi} |\alpha(U) - \alpha(V)|.
\]

Lemma 5. For Hermitian $H, K$ and $0 \leq H, K, H + K \leq \pi$, $0 < t < 1$,
\[
|\alpha(e^{iHt} e^{iKt}) - \alpha(e^{i(H+K)t})| \leq ct^2,
\]
where $c$ is a constant independent of $H, K$ and $t$.

Proof. Using the expansion of the matrix exponential function and the condition $0 \leq H, K, H + K \leq \pi$, $0 < t < 1$, it’s easy to show that there exists some constant $c_1$ such that
\[
\|e^{iHt} e^{iKt} - e^{i(H+K)t}\| \leq c_1 t^2.
\]
The inequality follows immediately from Lemma 4.

With these results in hand, we start the proof of the main result, Theorem 1.

Proof of Theorem 1. As Non-Identity Check of short circuit is a special case of the general Non-Identity Check problem, the fact that it is in QMA follows from the previous result in Ref. [14]. It suffices to prove the hardness result only. We will reduce the 1-D Local Hamiltonian problem to it.

Suppose we are given an instance of the 1-D Local Hamiltonian problem which has input $H = \sum_{i=1}^n H_i$ and real numbers $a, b$ with at least inverse polynomial gap. $H$ is a Hamiltonian of an $n$ particle system with local dimension $d$ and each term $H_i$ is an operator on two neighbouring particles which can be described by a $d^2$ by $d^2$ Hermitian matrix. It is a “Yes” instance if there exists some density matrix $\rho$ such that $\text{tr}(H \rho) \leq a$ and a “No” instance if $\text{tr}(H \rho) \geq b$ for all $\rho$. This problem is known to be QMA-Complete for $d \geq 12$. For simplicity, one can always rescale the problem and assume that $H_i$’s are positive semidefinite and $\|H_i\| \leq 1$.

Note that 1-D property of the problem allows us to write $H$ as $H_{\text{odd}} + H_{\text{even}}$ where $H_{\text{odd}}$ and $H_{\text{even}}$ each contain local terms acting on different particles. This is illustrated in Figure 3. $H_{\text{odd}}$ is the sum of $H_1, H_3, H_5, \ldots$ where $H_1$
are no longer the same as they were in the original. Let $\tilde{H}$ be the sum $\sum_i \tilde{H}_i$. It’s obvious that $|d\rangle \otimes^n$ is an eigenstate of $\tilde{H}$ with eigenvalue $r$ while the smallest eigenvalue of $\tilde{H}$ equals that of $H$. The 1-D Hamiltonian problem of $H$ is now reduced to deciding if $\lambda(H)$, the eigenvalue range of $\tilde{H}$, is larger than $r - a$ or smaller than $r - b$. The eigenvalue range problem can be viewed as the Hamiltonian version of the Non-Identity Check problem for circuits. We will show that it’s possible to use circuit Non-Identity Check to solve this eigenvalue range problem of local Hamiltonian.

Before further reducing the problem, we normalize $\tilde{H}$ by dividing $2r/\pi$ so that the conditions of the lemmas we will use are met. Denote the normalized Hamiltonian again with $H$ and its local terms with $H_i$ for simplicity; but they are no longer the same as they were in the original 1-D Local Hamiltonian problem. After that, we have $\|H\| \leq \pi/2$. Let $l$ and $s$ be $(r - a)\pi/2r$ and $(r - b)\pi/2r$ respectively. It’s a “Yes” instance if $\lambda(H) \geq l$ and a “No” instance if $\lambda(H) \leq s$. Notice that $l$ and $s$ have inverse polynomial gap.

We can now construct a Non-Identity problem as follows. The circuit is simply

$$U_H = e^{iH_{\text{local}}}e^{iH_{\text{alt}}}, \quad (8)$$

and the two threshold real numbers $a = st$, $b = lt - ct^2$. Here, $t$ is chosen to be $(l - s)/2c$ where $c$ is the constant in Lemma 5. It’s easy to check that $b - a$ has at least inverse polynomial gap. As the local terms $H_1, H_3, H_5, \ldots$ in $H_{\text{local}}$ are on different particles, $e^{iH_{\text{alt}}}$ equals the tensor product of $e^{iH_{1t}}, e^{iH_{3t}}, e^{iH_{5t}}, \ldots$ and can be implemented in parallel. Similar property holds for $H_{\text{even}}$. Therefore $U_H$ is indeed a constant depth circuit.

Since $\lambda(H)$ is promised either larger than $l$ or smaller than $s$, we can verify that the promise for the above Non-Identity problem also holds. If $\lambda(H)$ is larger than $l$, it follows from Lemma 5 that $\alpha(U_H)$ is at least

$$\alpha(e^{iHt}) - ct^2 = \lambda(Ht) - ct^2 \geq lt - ct^2 = b.$$ 

If $\lambda(H)$ is smaller than $s$, Lemma 2 implies that $\alpha(U_H)$ is at most

$$\alpha(e^{iHt}) \leq st = a.$$ 

It’s also easy to check that the eigenvalue range problem of $H$ is a “Yes” (or “No”) instance if and only if the Non-Identity Check problem of $U_H$ is a “Yes” (or “No”) instance.

It’s worth noting that the main idea in the proof is highly related to quantum simulation using Trotter expansion

$$e^{A+B} = \lim_{n \to \infty} (e^{A/n}e^{B/n})^n.$$ 

Fortunately however, it is enough to simulate the first round of $e^{A/n}e^{B/n}$ and leave the amplification procedure to the verifier.
The circuit we constructed above contains quantum gates such as $e^{iH_1t}$ which need $\Omega(\log n)$ bits to specify. In order to translate the result to the case where only a finite universal set of quantum gates are allowed, we need to expand each gate in the circuit using Solovay-Kitaev theorem. This will give us the result in Corollary 1. The main problem here is to analyze how the imperfections in each gate will affect the phase range $\alpha$ of the circuit. Suppose we want to use unitary gates $U_1$ and $U_2$ but the actual implementations are unitary gates $V_1$ and $V_2$ with $V_1 = U_1 + E_1$ and $V_2 = U_2 + E_2$, then
\[
\|V_1V_2 - U_1U_2\| = \|(U_1 + E_1)(U_2 + E_2) - U_1U_2\|
\]
\[
= \|U_1E_2 + E_1(U_2 + E_2)\|
\]
\[
= \|U_1E_2 + E_1V_2\|
\]
\[
\leq \|E_1\| + \|E_2\|,
\]
and similarly,
\[
\|V_1 \otimes V_2 - U_1 \otimes U_2\| \leq \|E_1\| + \|E_2\|.
\]
These two facts and Lemma 4 imply that for any circuit $C$ and its imperfect implementation $C'$
\[
|\alpha(C) - \alpha(C')| \leq \pi \|C - C'\| \leq \pi \sum_i \|E_i\|,
\]
where $E_i$’s are the errors in all the gates of $C'$. Thus, the total error in $\alpha$ of the circuit is at most $\pi$ times the summation of norms of all errors in each gate. It can be made inverse polynomial small and much smaller than the gap of threshold parameter $a$ and $b$. This validates the claim in Corollary 1.

It’s proved in Ref. [13] that there exists some universal gate set such that only $O(\log(1/\epsilon))$ number of gates are required to achieve an error bound of $\epsilon$. A similar argument as above gives the proof of Corollary 2.

4 Conclusion

In this paper, we conclude that Non-Identity Check for constant depth quantum circuit is QMA-Complete given $\Omega(\log n)$ bit of precision to each gate. However, the depth may vary when using a fixed universal gate set. Employing different versions of Solovay-Kitaev theorem, we are able to prove the hardness for circuits of polylogarithmic or even logarithmic depth.

It is interesting to compare our result with the problem of distinguishing mixed state quantum computation in terms of the diamond norm [2]. Although the main difference is simply whether some output are discarded or not, the problem of distinguishing mixed state quantum computation seems to be much harder. In fact, it was shown to be QIP-Complete [25]. Rosgen [24] further proved that logarithmic depth quantum circuits are as hard to distinguish as polynomial depth quantum circuit and thus distinguishing logarithmic depth mixed state quantum circuits remains QIP-Complete.

We leave the question of the complexity of Non-Identity Check for constant depth quantum circuits with gates from a finite universal gate set as an interesting open problem.

Acknowledgment

The authors would like to thank Daniel Gottesman, Richard Cleve and John Watrous for helpful discussions. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research & Innovation.

References

[1] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The Power of Quantum Systems on a Line. Communications in Mathematical Physics, 287(1):41–65, 2009. See also arXiv:0705.4077.
[2] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In Proc. 30th ACM Symposium on the Theory of Computing, pages 20–30, 1998.
[3] D. Aharonov and T. Naveh. Quantum NP - A Survey, 2002. arXiv:quant-ph/0210077.
[4] S. Beigi and P. W. Shor. On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels. 2007. Available arXiv:0709.2090.
[5] M. Blum, A. K. Chandra, and M. N. Wegman. Equivalence of free boolean graphs can be decided probabilistically in polynomial time. 10(2):80–82, 1980.
[6] A. Broadbent and E. Kashefi. Parallelizing quantum circuits. To appear in Theoretical Computer Science, 2009. See also arXiv:0704.1736.
[7] A. M. Childs, J. Preskill, and J. Renes. Quantum information and precision measurement. Journal of Modern Optics, 47:155–176, 2000. See also arXiv:quant-ph/9904021.
[8] R. Cleve and J. Watrous. Fast parallel circuits for the quantum fourier transform. In Proc. 41st ACM Symposium on the Theory of Computing, pages 526–536, 2000.
[9] S. Cook. The complexity of theorem proving procedures. In Proceedings of the Third Annual ACM Symposium on Theory of Computing, pages 151–158, 1971.
[10] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm, 2005. arXiv:quant-ph/0505030.
[11] R. Duan, Y. Feng, and M. Ying. Entanglement is not necessary for perfect discrimination between unitary operations. Physical Review Letters, 98(10):100503, 2007.
[12] S. Fenner, F. Green, S. Homer, and Y. Zhang. Bounds on the power of constant-depth quantum circuits. In Proc. 15th International Symposium on Fundamentals of Computation Theory, pages 44–55, 2005.
[13] A. Harrow, B. Recht, and I. L. Chuang. Efficient discrete approximations of quantum gates. J. Math. Phys., 43:4445, 2002. See also arXiv:quant-ph/0111031.
[14] D. Janzing, P. Wocjan, and T. Beth. Non-Identity Check is QMA-Complete. International Journal of Quantum Information, 3(3):463–473, 2005. See also arXiv:quant-ph/0305050.
[15] J. Kempe, A. Kitaev, and O. Regev. The Complexity of the Local Hamiltonian Problem. In FSTTCS, pages 372–383, 2004. See also arXiv:quant-ph/0406180.
[16] J. Kempe and O. Regev. 3-Local Hamiltonian is QMA-Complete. Quantum Information and Computation, 3(3):258–264, 2003. See also arXiv:quant-ph/0302079.
[17] A. Y. Kitaev. Quantum computations: algorithms and error correction. Russian Mathematical Surveys, 52(6):1191–1249, 1997.
[18] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. Classical and Quantum Computation. American Mathematical Society, 2002.
[19] L. Levin. Universal search problems. Problems of Information Transmission, 9(3):265–266, 1973.
[20] Y.-K. Liu. Consistency of Local Density Matrices is QMA-complete. In Proc. RANDOM 2006, pages 438–449, 2006.
[21] Y.-K. Liu, M. Christandl, and F. Verstraete. N-representability is QMA-complete. Physical Review Letters, 98, 2007. See also arXiv:quant-ph/0609125.
[22] C. Moore and M. Nilsson. Parallel quantum computation and quantum codes. SIAM Journal on Computing, 31(3):799–815, 2002.
[23] R. Oliveira and B. M. Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. Quantum Information and Computation, 8(10):900–924, 2008. See also arXiv:quant-ph/0504050.
[24] B. Rosgen. Distinguishing short quantum computations. In Proceedings of the 25th International Symposium on Theoretical Aspects of Computer Science, pages 597–608, 2008.
[25] B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In Proc. 20th Conference on Computational Complexity, pages 344–354, 2005.
[26] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM, (4):701–717, 1980.
[27] B. M. Terhal and D. P. DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. Quantum Information and Computation, 4(2), 2004. See also arXiv:quant-ph/0205133.
[28] J. Watrous. Lecture Notes of CS798: Theory of Quantum Information, 2008.
[29] T.-C. Wei, M. Mosca, and A. Nayak. Interacting boson problems are QMA-hard, 2009. arXiv:0905.3413.
[30] A. C.-C. Yao. Quantum circuit complexity. In SFCS ’93: Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, pages 352–361, Washington, DC, USA, 1993. IEEE Computer Society.
[31] R. Zippel. Probabilistic algorithms for sparse polynomials. International Symposium on Symbolic and Algebraic Computation, Lecture Notes in Computer Science, 1979:216–226.