Quantum Information and Computation, Vol. 14, No. 13&14 (2014) 1149–1164

HARDNESS OF CLASSICALLY SIMULATING QUANTUM CIRCUITS WITH UNBOUNDED TOFFOLI AND FAN-OUT GATES

YASUHIRO TAKAHASHI[1], TAKESHI YAMAZAKI[2], and KAZUYUKI TANAKA[2]
[1]*NTT Communication Science Laboratories, NTT Corporation*
Atsugi, Kanagawa 243-0198, Japan
[2]*Mathematical Institute, Tohoku University*
Sendai, Miyagi 980-8578, Japan

Received July 18, 2013
Revised January 29, 2014

We study the classical simulatability of constant-depth polynomial-size quantum circuits followed by only one single-qubit measurement, where the circuits consist of universal gates on at most two qubits and additional gates on an unbounded number of qubits. First, we consider unbounded Toffoli gates as additional gates and deal with the weak simulation, i.e., sampling the output probability distribution. We show that there exists a constant-depth quantum circuit with only one unbounded Toffoli gate that is not weakly simulatable, unless $\mathsf{BQP} \subseteq \mathsf{PostBPP} \cap \mathsf{AM}$. Then, we consider unbounded fan-out gates as additional gates and deal with the strong simulation, i.e., computing the output probability. We show that there exists a constant-depth quantum circuit with only two unbounded fan-out gates that is not strongly simulatable, unless $\mathsf{P} = \mathsf{PP}$. These results are in contrast to the fact that any constant-depth quantum circuit without additional gates on an unbounded number of qubits is strongly and weakly simulatable.

Keywords: constant-depth quantum circuit, classical simulation, unbounded Toffoli gate, unbounded fan-out gate
Communicated by: R Jozsa & B Terhal

1 Introduction

In quantum information processing, it is important to understand the difference between the computational power of a quantum computer and that of a classical computer. For this purpose, it is known to be useful to study the classical simulatability of quantum computation processes. In this context, the above difference can be found even in rather simple computation processes [22, 8, 3, 6, 17], such as constant-depth polynomial-size quantum circuits. There is great interest in studying the classical simulatability of such simple computation processes because this is particularly useful for identifying the source of the computational power of a quantum computer.

In this paper, we study the classical simulatability of constant-depth polynomial-size quantum circuits. In 2004, Terhal et al. provided evidence for the hardness of classically simulating such circuits followed by polynomially many single-qubit measurements, where the circuits consist of universal gates on at most two qubits [22]. Subsequently, other authors provided (or mentioned) further evidence for this [8, 3, 6]. As discussed in [22, 8, 6], an important assumption in these arguments is that the number of measurements is polynomial in the length

of the input. In fact, for example, any constant-depth quantum circuit followed by only one single-qubit measurement is efficiently simulatable classically [22]. Even in this simplest output setting, however, it is not yet known how the use of gates on an unbounded number of qubits affects the classical simulatability of constant-depth quantum circuits.

We focus on quantum circuits in the simplest output setting, where they consist of universal gates on at most two qubits (Hadamard, $\pi/8$, and CNOT gates [18]) and additional gates on an unbounded number of qubits, or more concretely, unbounded Toffoli and fan-out gates. An unbounded Toffoli gate on $n+1$ qubits computes the AND of n inputs. An unbounded fan-out gate on $n+1$ qubits makes n copies of a classical source bit and, when $n=1$, the gate is a CNOT gate. The main reason we adopt these gates as elementary gates is that they are a natural generalization of the classical ones assumed to be elementary gates for studying the computational power of small-depth classical circuits [23]. Moreover, the study of an unbounded fan-out gate in the context of the classical simulatability complements previous studies of the gate, showing that it is very powerful [10, 12, 21].

We deal with the strong and weak simulations [22, 15, 6, 16, 17]. The strong simulation of a quantum circuit means that, when an input to the circuit and its output are specified, the probability of obtaining the output can be efficiently computed classically. The weak simulation means that the output probability distribution of the circuit can be efficiently sampled classically. The strong simulation implies the weak simulation [22, 6, 16]. The error setting in the weak simulation is different from Terhal et al.'s efficient simulation [22] in that the error in the weak simulation is not a multiple of the output probability. Our setting seems more natural than the previous multiplicative one.

First, we consider constant-depth quantum circuits with unbounded Toffoli gates and their weak simulatability. We provide evidence for the hardness of weakly (and thus strongly) simulating a $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit, which is a constant-depth quantum circuit with only one unbounded Toffoli gate:

Theorem 1 *There exists a* $\mathsf{QNC}^0_{\mathrm{t},1}$ *circuit that is not weakly simulatable, unless* $\mathsf{BQP} \subseteq \mathsf{PostBPP} \cap \mathsf{AM}$.

It is considered unlikely that $\mathsf{BQP} \subseteq \mathsf{PostBPP} \cap \mathsf{AM}$ since this (or even a weaker containment, such as $\mathsf{BQP} \subseteq \mathsf{PostBPP}$) would imply that BQP is contained in the polynomial hierarchy, which is considered unlikely [2]. Theorem 1 shows a boundary between classical and quantum computation: any constant-depth quantum circuit without additional gates on an unbounded number of qubits is strongly and weakly simulatable, but such a circuit with only one unbounded Toffoli gate is not strongly or weakly simulatable (under a plausible assumption).

To prove Theorem 1, we first show that, if any $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit is weakly simulatable, then $\mathsf{BQP} \subseteq \mathsf{PostBPP}$. To do this, we parallelize a quantum circuit for $L \in \mathsf{BQP}$ by Fenner et al.'s method [8] and obtain a QNC^0 circuit, which is a constant-depth quantum circuit without gates on an unbounded number of qubits. The circuit has polynomially many postselection qubits that have to be measured to obtain a relationship between the output qubit and membership of the input in L. Using an unbounded Toffoli gate, we regard the postselection qubits and the output qubit as new "one" output qubit in two ways and construct two $\mathsf{QNC}^0_{\mathrm{t},1}$ circuits. Their weak simulations yield a $\mathsf{PostBPP}$ algorithm for L. We then deal with the containment $\mathsf{BQP} \subseteq \mathsf{AM}$ using Terhal et al.'s argument in terms of the efficient simulation [22]. Since the number of measurements in their argument is polynomial and the efficient simulation

is different from the weak simulation as described above, the argument does not work directly. We modify the argument and do an error analysis using one of the two $\mathsf{QNC}^0_{\mathrm{t},1}$ circuits.

As shown in [15], there exists a weakly simulatable polynomial-size quantum circuit that is not strongly simulatable (under a plausible assumption). On the basis of the idea of the proof of Theorem 1, we show the difference between the strong and weak simulatability in a simpler setting:

Theorem 2 *There exists a weakly simulatable* $\mathsf{QNC}^0_{\mathrm{t},1}$ *circuit that is not strongly simulatable, unless* $\mathsf{P} = \mathsf{PP}$.

This contributes to our understanding not only of the classical simulatability of a $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit but also of the notions of the strong and weak simulatability.

Then, we consider constant-depth quantum circuits with unbounded fan-out gates and their strong simulatability. The OR circuit in [21] allows us to replace an unbounded Toffoli gate in Theorem 1 with polynomially many unbounded fan-out gates. Thus, there exists a constant-depth quantum circuit with polynomially many unbounded fan-out gates that is not strongly (or weakly) simulatable (under a plausible assumption). We provide evidence for the hardness of strongly simulating a simpler circuit, or more concretely, a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit, which is a constant-depth quantum circuit with only two unbounded fan-out gates:

Theorem 3 *There exists a* $\mathsf{QNC}^0_{\mathrm{f},2}$ *circuit that is not strongly simulatable, unless* $\mathsf{P} = \mathsf{PP}$.

It is considered unlikely that $\mathsf{P} = \mathsf{PP}$, which would imply the collapse of the polynomial hierarchy. As in Theorem 1, Theorem 3 shows a boundary: any constant-depth quantum circuit without additional gates is strongly simulatable, but such a circuit with only two unbounded fan-out gates is not strongly simulatable (under a plausible assumption).

Our idea in showing Theorem 3 is to use the Hadamard test [17], or more precisely, to parallelize it by two unbounded fan-out gates. For a QNC^0 circuit, the parallelized Hadamard test is a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit and allows us to show that, if any $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit is strongly simulatable, there exists a polynomial-time deterministic classical algorithm for computing a matrix element of a QNC^0 circuit with exponential precision. This algorithm can be transformed into the one for computing a matrix element of a polynomial-size quantum circuit with exponential precision by Fenner et al.'s method [8] of parallelizing quantum circuits. This implies that $\mathsf{P} = \mathsf{PP}$ [17] and thus Theorem 3.

More generally, using the idea, we characterize the relationship $\mathsf{P} = \mathsf{PP}$ using the strong simulatability of the parallelized Hadamard test for a QNC^0 circuit, which is a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit. This contributes to our understanding of the strong simulatability of such a circuit in the sense that the hardness of its strong simulation is exactly evaluated. Moreover, this is interesting in that the simple quantum computation process characterizes the classical relationship.

2 Preliminaries

2.1 Quantum circuits

We use the standard notation for quantum states and the standard diagrams for quantum circuits [18]. A quantum circuit consists of elementary gates. Our elementary gates are Hadamard gates H, $\pi/8$ gates T, CNOT gates, unbounded Toffoli gates, and unbounded fan-out gates, where

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

We denote T^4 and HT^4H as Z and X, respectively. A Toffoli gate on $k+1$ qubits implements the quantum operation defined as

$$\left(\bigotimes_{j=0}^{k-1}|x_j\rangle\right)|y\rangle \mapsto \left(\bigotimes_{j=0}^{k-1}|x_j\rangle\right)|y \oplus \bigwedge_{j=0}^{k-1} x_j\rangle,$$

where $x_j, y \in \{0,1\}$, $k \geq 2$, and $\oplus$ denotes addition modulo 2. The first k input qubits, i.e., the qubits in state $\bigotimes_{j=0}^{k-1}|x_j\rangle$, are called control qubits. A Toffoli gate on three qubits is simply called a Toffoli gate. A fan-out gate on $k+1$ qubits implements the quantum operation defined as

$$|y\rangle\bigotimes_{j=0}^{k-1}|x_j\rangle \mapsto |y\rangle\bigotimes_{j=0}^{k-1}|x_j \oplus y\rangle,$$

where $y, x_j \in \{0,1\}$ and $k \geq 1$. The first input qubit, i.e., the qubit in state $|y\rangle$, is called the control qubit. When $k = 1$, a fan-out gate is a CNOT gate. When a Toffoli gate or a fan-out gate is applied on an unbounded number of qubits, it is called an unbounded Toffoli gate or an unbounded fan-out gate, respectively.

The complexity measures of a quantum circuit are its size and depth. The size of a quantum circuit is defined as the total size of all elementary gates in it, where the size of an elementary gate is defined as the number of qubits affected by the gate. The depth of a quantum circuit is defined as follows. Input qubits are considered to have depth 0. For each gate G, the depth of G is equal to 1 plus the maximum depth of a gate on which G depends. The depth of a quantum circuit is defined as the maximum depth of a gate in it. Intuitively, the depth is the number of layers in the circuit, where a layer consists of gates that can be applied in parallel. A quantum circuit can use ancillary qubits initialized to $|0\rangle$. Resetting the states to $|0\rangle$ at the end of the computation is not required.

We deal with a uniform family of polynomial-size quantum circuits $\{C_n\}_{n\geq 1}$. Each C_n is a quantum circuit with n input qubits and poly(n) ancillary qubits. A symbol denoting a quantum circuit, such as C_n, also denotes its matrix representation. When a classical output is obtained from C_n, the circuit is followed by only one measurement in the computational basis, i.e., a Z-measurement, on a specified qubit called the output qubit. The output qubit in this paper is one of the ancillary qubits. The uniformity means that there exists a polynomial-time deterministic classical algorithm for computing the function $1^n \mapsto \overline{C_n}$, where $\overline{C_n}$ is the encoding of the description of C_n. Any quantum circuit in this paper is understood to be an element of a uniform family of quantum circuits and thus, for simplicity, we frequently deal with C_n in place of $\{C_n\}_{n\geq 1}$. Let C_n be a constant-depth polynomial-size quantum circuit. In general, the number of gates on an unbounded number of qubits in C_n is poly(n). In particular, when the number of such gates in C_n is one and the gate is an unbounded Toffoli gate, we call C_n a $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit. When the number is two and the gates are unbounded fan-out gates, we call C_n a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit. When C_n has no such gates, we call it a QNC^0 circuit.

2.2 Classical simulatability

The classical simulatability of a quantum circuit is defined as follows [15, 6, 16, 17]:

Definition 1 *Let C_n be a polynomial-size quantum circuit with n input qubits and* $\mathrm{poly}(n)$ *ancillary qubits including the output qubit. For any $x \in \{0,1\}^*$ of length n and $y \in \{0,1\}$, let $\Pr[C_n(x) = y]$ be the probability of obtaining y by a Z-measurement on the output qubit of C_n with the input state $|x\rangle$.*

- *C_n is strongly simulatable if, for any polynomial p, there exists a polynomial-time deterministic classical algorithm (i.e., polynomial-time deterministic Turing machine) A such that, for any $x \in \{0,1\}^*$ of length n,*

$$|A(x) - \Pr[C_n(x) = 1]| \leq \frac{1}{2^{p(n)}}.$$

- *C_n is weakly simulatable if, for any polynomial p, there exists a polynomial-time probabilistic classical algorithm (i.e., polynomial-time probabilistic Turing machine) A such that, for any $x \in \{0,1\}^*$ of length n,*

$$|\Pr[A(x) = 1] - \Pr[C_n(x) = 1]| \leq \frac{1}{2^{p(n)}}.$$

In the definition, for simplicity, we use a classical algorithm defined by a Turing machine, but we can regard it as a uniform family of classical circuits (that can have random bits) [6].

As described in Introduction, the objective of our paper is to show the hardness of classically simulating simple quantum circuits. Previous results in this direction are obtained by using the above definitions of the classical simulatability [15, 6, 16, 17]. We adopt the same definitions to fairly compare our results with the previous ones. These definitions deal with quantum circuits in a restricted setting. For example, input states are assumed to be computational basis states and measurements are assumed to be Z-measurements. Moreover, we focus on the effect of using gates on an unbounded number of qubits in the simplest output setting and thus consider two-outcome events (i.e., a Z-measurement on the output qubit) only. Although these restrictions seem artificial from the physical point of view, they allow us to compare quantum circuits with classical ones clearly from the theoretical point of view.

The definitions of the classical simulatability do not tell us how exponentially small errors are negligible or not, where the errors are the right hand values of the above inequalities. In other words, the simulatability and its related concepts in this paper, such as "hardness", are not operationally meaningful. Thus, the paper is about investigating the relationships between quantum circuits and combinatorial structures, but is not about the practical utility.

A strongly simulatable quantum circuit is weakly simulatable [22, 6, 16]. The weak simulation is different from Terhal et al.'s efficient simulation [22] in that the error in the weak simulation is not a multiple of $\Pr[C_n(x) = 1]$. In other words, the error in the weak simulation is an absolute one, but that in the efficient simulation is a one relative to $\Pr[C_n(x) = 1]$. In this sense, the error setting in the weak simulation seems more natural. We note that any QNC^0 circuit followed by only one single-qubit measurement is strongly (and thus weakly) simulatable [22].

2.3 Complexity classes

The complexity classes we deal with in this paper are defined as follows [18, 6, 1, 11, 2]:

Definition 2 *Let $L \subseteq \{0,1\}^*$.*

- $L \in \mathsf{BQP}$ *if there exists a polynomial-size quantum circuit* C_n *with* n *input qubits and* $\mathrm{poly}(n)$ *ancillary qubits including the output qubit such that, for any* $x \in \{0,1\}^*$ *of length* n*,*
  - *if* $x \in L$, $\Pr[C_n(x) = 1] \geq \frac{2}{3}$,
  - *if* $x \notin L$, $\Pr[C_n(x) = 1] \leq \frac{1}{3}$.
- $L \in \mathsf{PostBPP}$ *if there exists a polynomial-time probabilistic classical algorithm* A *that, for any* $x \in \{0,1\}^*$*, outputs* $A(x), \mathrm{post}(x) \in \{0,1\}$ *such that*
  - $\Pr[\mathrm{post}(x) = 1] > 0$,
  - *if* $x \in L$, $\Pr[A(x) = 1 | \mathrm{post}(x) = 1] \geq \frac{2}{3}$,
  - *if* $x \notin L$, $\Pr[A(x) = 1 | \mathrm{post}(x) = 1] \leq \frac{1}{3}$.

We note that $\mathsf{PostBPP}$ is equal to $\mathsf{BPP}_{\mathsf{path}}$ defined in [11]. The constants 2/3 and 1/3 in the definitions can be replaced with $1/2 + \varepsilon$ and $1/2 - \varepsilon$, respectively, for any constant $0 < \varepsilon < 1/2$ [18, 6]. We also deal with the well-known complexity classes P, AM, and PP [4]. Moreover, we deal with the function classes FP and $\#\mathsf{P}$ [4]: FP is the class of functions for which there exists a polynomial-time deterministic classical algorithm and $\#\mathsf{P}$ is the class of functions counting the number of solutions to polynomial-time decidable relations.

2.4 Parallelization of quantum circuits

We frequently use a quantum circuit obtained by Fenner et al.'s method [8]. The existence of the circuit (combined with a constant-depth polynomial-size quantum circuit for permuting qubits [14] and with X gates) can be described as follows:

Lemma 1 *For any polynomial-size quantum circuit* C_n *with* n *input qubits and* a *ancillary qubits, there exists a* QNC^0 *circuit* D_n *with* n *input qubits and* $a+b$ *ancillary qubits such that* b *is even,* $b = O(\mathrm{size}(C_n))$*, and, for any* $x \in \{0,1\}^*$ *of length* n*,*

$$D_n|x\rangle|0\rangle^{\otimes(a+b)} = \frac{1}{\sqrt{2^b}}(C_n|x\rangle|0\rangle^{\otimes a})|1\rangle^{\otimes b} + \sum_{y \in \{0,1\}^b \setminus \{1^b\}} \alpha_y |\psi_y\rangle|y\rangle,$$

where $\mathrm{size}(C_n)$ *is the polynomial representing the size of* C_n*,* $\alpha_y \in \mathbf{C}$*, and* $|\psi_y\rangle$ *is an* $(n+a)$*-qubit state.*

The new b ancillary qubits are called the postselection qubits.

3 Circuit with One Unbounded Toffoli Gate

3.1 Proof of Theorem 1

We divide the proof of Theorem 1 into two lemmas. One is on the containment $\mathsf{BQP} \subseteq \mathsf{PostBPP}$ and the other is on $\mathsf{BQP} \subseteq \mathsf{AM}$. Recall that a Toffoli gate (on three qubits) outputs 1 if and only if the state of the control qubits is $|11\rangle$. Combining the gate with an X gate, we can obtain a circuit that outputs 1 if and only if the state of the control qubits is $|01\rangle$. We call it a (0,1)-Toffoli gate. Using these gates, we first show the following lemma:

Lemma 2 *If every* $\mathsf{QNC}^0_{\mathrm{t},1}$ *circuit is weakly simulatable, then* $\mathsf{BQP} \subseteq \mathsf{PostBPP}$.

Proof: Let $L \in \mathsf{BQP}$. There exists a polynomial-size quantum circuit C_n with n input qubits and a ancillary qubits including the output qubit such that, for any $x \in \{0,1\}^*$ of length n,

- if $x \in L$, $\Pr[C_n(x) = 1] \geq \frac{2}{3}$,
- if $x \notin L$, $\Pr[C_n(x) = 1] \leq \frac{1}{3}$.

By Lemma 1, there exists a QNC^0 circuit D_n with n input qubits and $a + b$ ancillary qubits including the output qubit such that, for any $x \in \{0,1\}^*$ of length n,

- if $x \in L$, $\Pr[D_n(x) = 1 | \mathrm{post}_n(x) = 1^b] \geq \frac{2}{3}$,
- if $x \notin L$, $\Pr[D_n(x) = 1 | \mathrm{post}_n(x) = 1^b] \leq \frac{1}{3}$,

where $b = O(\mathrm{size}(C_n))$, "$\mathrm{post}_n(x) = 1^b$" means that all results of Z-measurements on the postselection qubits are 1, and $\Pr[\mathrm{post}_n(x) = 1^b] = 1/2^b$. This implies that, for any $x \in \{0,1\}^*$ of length n,

- if $x \in L$, $\Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b] \geq \frac{2}{3} \cdot \frac{1}{2^b}$,
- if $x \notin L$, $\Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b] \leq \frac{1}{3} \cdot \frac{1}{2^b}$.

We define a quantum circuit E_n as follows, where it has n input qubits, $a + b$ ancillary qubits for D_n, and new two ancillary qubits including the output qubit for E_n:

1. Apply D_n on the n input qubits and $a + b$ ancillary qubits.
2. Apply an unbounded Toffoli gate on the b postselection qubits and one of the new two ancillary qubits that is not the output qubit for E_n. The output of the gate is written into the new ancillary qubit.
3. Apply a Toffoli gate on the output qubit for D_n, which is one of the a ancillary qubits, and the new two ancillary qubits. The output of the gate is written into the output qubit for E_n.

We also define a quantum circuit F_n similarly to E_n except that the Toffoli gate in Step 3 is replaced with the $(0,1)$-Toffoli gate. The circuits E_n and F_n are depicted in Figs. 1(a) and (b), respectively, where the bottom qubits are the output qubits. A Toffoli gate can be decomposed exactly into a constant-depth constant-size quantum circuit consisting of H, T, and CNOT gates with no ancillary qubits [18]. Since D_n is a QNC^0 circuit, E_n and F_n are $\mathsf{QNC}^0_{\mathrm{t},1}$ circuits.

The unbounded Toffoli gate in Step 2 reduces the b postselection qubits to new one postselection qubit, which is the new ancillary qubit that is not the output qubit for E_n. Moreover, the Toffoli gate in Step 3 outputs 1 if and only if the state of the output qubit for D_n and the new postselection qubit is $|11\rangle$. Thus, for any $x \in \{0,1\}^*$ of length n, $\Pr[E_n(x) = 1] = \Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b]$. Similarly, $\Pr[F_n(x) = 1] = \Pr[D_n(x) = 0 \& \mathrm{post}_n(x) = 1^b]$. Since $\Pr[\mathrm{post}_n(x) = 1^b] = 1/2^b$, $\Pr[E_n(x) = 1] + \Pr[F_n(x) = 1] = 1/2^b$.

As described above, E_n and F_n are $\mathsf{QNC}^0_{\mathrm{t},1}$ circuits. Thus, with the assumption, there exist polynomial-time probabilistic classical algorithms A and B such that, for any $x \in \{0,1\}^*$ of length n,

$$|\Pr[A(x) = 1] - \Pr[E_n(x) = 1]| \leq \frac{1}{2^{b+6}}, \ |\Pr[B(x) = 1] - \Pr[F_n(x) = 1]| \leq \frac{1}{2^{b+6}}.$$

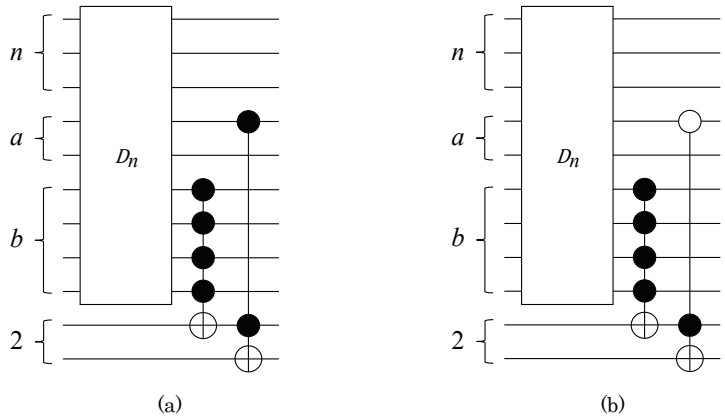


Fig. 1. (a) Circuit E_n. (b) Circuit F_n.

Since $\Pr[E_n(x) = 1] + \Pr[F_n(x) = 1] = 1/2^b$, it holds that

$$\frac{1}{2^b}\left(1 - \frac{1}{32}\right) \leq \Pr[A(x) = 1] + \Pr[B(x) = 1] \leq \frac{1}{2^b}\left(1 + \frac{1}{32}\right).$$

We define a polynomial-time probabilistic classical algorithm G as follows, where the input is $x \in \{0,1\}^*$:

1. Choose $r \in \{0,1\}$ uniformly at random.
2. (a) If $r = 1$, compute $A(x)$.
   - i. If $A(x) = 1$, set $\mathrm{post}(x) = 1$ and $G(x) = 1$.
   - ii. If $A(x) = 0$, set $\mathrm{post}(x) = 0$ and $G(x) = 1$.

   (b) If $r = 0$, compute $B(x)$.
   - i. If $B(x) = 1$, set $\mathrm{post}(x) = 1$ and $G(x) = 0$.
   - ii. If $B(x) = 0$, set $\mathrm{post}(x) = 0$ and $G(x) = 0$.

By the definition of G,

$$\Pr[\mathrm{post}(x) = 1] = \frac{1}{2} \cdot \Pr[A(x) = 1] + \frac{1}{2} \cdot \Pr[B(x) = 1].$$

Since $\Pr[A(x) = 1] + \Pr[B(x) = 1] > 0$, $\Pr[\mathrm{post}(x) = 1] > 0$. Moreover,

$$\Pr[G(x) = 1 \& \mathrm{post}(x) = 1] = \frac{1}{2} \cdot \Pr[A(x) = 1].$$

Thus, for any $x \in \{0,1\}^*$ of length n,

$$\Pr[G(x) = 1 | \mathrm{post}(x) = 1] = \frac{\Pr[G(x) = 1 \& \mathrm{post}(x) = 1]}{\Pr[\mathrm{post}(x) = 1]} = \frac{\Pr[A(x) = 1]}{\Pr[A(x) = 1] + \Pr[B(x) = 1]}.$$

If $x \in L$,

$$\Pr[G(x) = 1 | \mathrm{post}(x) = 1] \geq \frac{\Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b] - \frac{1}{2^{b+6}}}{\frac{1}{2^b}\left(1 + \frac{1}{32}\right)} \geq \frac{\frac{2}{3} \cdot \frac{1}{2^b} - \frac{1}{2^{b+6}}}{\frac{1}{2^b}\left(1 + \frac{1}{32}\right)} \geq \frac{3}{5}.$$

If $x \notin L$,

$$\Pr[G(x)=1|\mathrm{post}(x)=1] \leq \frac{\Pr[D_n(x)=1\&\mathrm{post}_n(x)=1^b]+\frac{1}{2^{b+6}}}{\frac{1}{2^b}\left(1-\frac{1}{32}\right)} \leq \frac{\frac{1}{3}\cdot\frac{1}{2^b}+\frac{1}{2^{b+6}}}{\frac{1}{2^b}\left(1-\frac{1}{32}\right)} \leq \frac{2}{5}.$$

Thus, $L \in \mathsf{PostBPP}$. □

Then, we deal with the containment $\mathsf{BQP} \subseteq \mathsf{AM}$ using Terhal et al.'s argument [22]. The argument uses a set of results of internal coin tosses in the classical simulation of (a parallelized version of) a quantum circuit for $L \in \mathsf{BQP}$, where the number of elements of the set on input x is large when $x \in L$ and the number is small when $x \notin L$. Even if the difference in the numbers is somewhat small, the Goldwasser-Sipser set lower bound protocol can decide whether the number is large or small [9, 22, 4], which implies that $L \in \mathsf{AM}$. More precisely, the key part of the argument is to show that, under an assumption about the classical simulatability of a QNC^0 circuit, any $L \in \mathsf{BQP}$ has the following property, which we call the property $\mathcal{P}$: there exist a constant $0 < \varepsilon < 1/3$, polynomials m, q $(m \geq q)$, and a family of sets $\{S_x\}_{x\in\{0,1\}^*}$ such that, for any $x \in \{0,1\}^*$ of length n,

- $S_x \subseteq \{0,1\}^{m(n)}$,
- if $x \in L$, $|S_x| \geq (1-\varepsilon)\cdot\frac{2}{3}\cdot 2^{q(n)}$,
- if $x \notin L$, $|S_x| \leq (1+\varepsilon)\cdot\frac{1}{3}\cdot 2^{q(n)}$,

where the problem of deciding whether a bit string of length $m(n)$ is in S_x has a polynomial-time deterministic classical algorithm. If L has the property $\mathcal{P}$, in order to decide whether $x \in L$ or not, it suffices to decide whether $|S_x| \geq (1-\varepsilon)\cdot\frac{2}{3}\cdot 2^{q(n)}$ or $|S_x| \leq (1+\varepsilon)\cdot\frac{1}{3}\cdot 2^{q(n)}$. This can be done by using the Goldwasser-Sipser protocol as described in [22], which implies that $L \in \mathsf{AM}$. Thus, to show Theorem 1, it suffices to show the following lemma:

Lemma 3 *If every $\mathsf{QNC}^0_{t,1}$ circuit is weakly simulatable, then any $L \in \mathsf{BQP}$ has the property $\mathcal{P}$.*

Proof: Let $L \in \mathsf{BQP}$. As in the proof of Lemma 2, there exists a QNC^0 circuit D_n such that, for any $x \in \{0,1\}^*$ of length n,

- if $x \in L$, $\Pr[D_n(x)=1\&\mathrm{post}_n(x)=1^b] \geq \frac{2}{3}\cdot\frac{1}{2^b}$,
- if $x \notin L$, $\Pr[D_n(x)=1\&\mathrm{post}_n(x)=1^b] \leq \frac{1}{3}\cdot\frac{1}{2^b}$.

We define a quantum circuit E_n as in the proof of Lemma 2. It holds that, for any $x \in \{0,1\}^*$ of length n, $\Pr[E_n(x)=1] = \Pr[D_n(x)=1\&\mathrm{post}_n(x)=1^b]$.

We fix a polynomial p satisfying $(3\cdot 2^b)/2^p < 1/10$. Since E_n is a $\mathsf{QNC}^0_{t,1}$ circuit, with the assumption, there exists a polynomial-time probabilistic classical algorithm A such that, for any $x \in \{0,1\}^*$ of length n,

$$|\Pr[A(x)=1] - \Pr[E_n(x)=1]| \leq \frac{1}{2^{p(n)}}.$$

More concretely, there exist such an algorithm A and a polynomial m such that, for any $x \in \{0,1\}^*$ of length n, the above inequality holds, where

$$\Pr[A(x)=1] = \frac{|\{r \in \{0,1\}^{m(n)} | A_r(x)=1\}|}{2^{m(n)}}$$

and A_r is A with the result of its internal coin tosses r. We note that A with a fixed r can be regarded as a polynomial-time deterministic classical algorithm. We can choose m satisfying $m \geq b$.

Let $\varepsilon = 1/4$, $q = m - b$, and $S_x = \{r \in \{0,1\}^{m(n)} | A_r(x) = 1\}$ for any $x \in \{0,1\}^*$ of length n. If $x \in L$,

$$\begin{aligned} |S_x| &= 2^{m(n)} \cdot \Pr[A(x) = 1] \geq 2^{m(n)} \cdot \left(\Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b] - \frac{1}{2^{p(n)}} \right) \\ &\geq 2^{m(n)} \cdot \left(\frac{2}{3} \cdot \frac{1}{2^{b(n)}} - \frac{1}{2^{p(n)}} \right) = \left(1 - \frac{3}{2} \cdot \frac{2^{b(n)}}{2^{p(n)}} \right) \cdot \frac{2}{3} \cdot \frac{2^{m(n)}}{2^{b(n)}} \geq (1-\varepsilon) \cdot \frac{2}{3} \cdot 2^{q(n)}. \end{aligned}$$

If $x \notin L$,

$$\begin{aligned} |S_x| &= 2^{m(n)} \cdot \Pr[A(x) = 1] \leq 2^{m(n)} \cdot \left(\Pr[D_n(x) = 1 \& \mathrm{post}_n(x) = 1^b] + \frac{1}{2^{p(n)}} \right) \\ &\leq 2^{m(n)} \cdot \left(\frac{1}{3} \cdot \frac{1}{2^{b(n)}} + \frac{1}{2^{p(n)}} \right) = \left(1 + 3 \cdot \frac{2^{b(n)}}{2^{p(n)}} \right) \cdot \frac{1}{3} \cdot \frac{2^{m(n)}}{2^{b(n)}} \leq (1+\varepsilon) \cdot \frac{1}{3} \cdot 2^{q(n)}. \end{aligned}$$

Thus, L has the property $\mathcal{P}$. □

3.2 Proof of Theorem 2

We consider a polynomial-time computable function $f = \{f_n\}_{n \geq 1}$, where $f_n : \{0,1\}^n \to \{0,1\}$. That is, there exists a uniform family of polynomial-size classical circuits such that it computes f. For simplicity, we denote $\{f_n\}_{n \geq 1}$ as f_n. For any f_n, there exists a polynomial-size quantum (in fact, classical reversible) circuit C_n^f with n input qubits and $a \geq 1$ ancillary qubits including the output qubit such that C_n^f consists only of Toffoli and X gates and implements the quantum operation $|y\rangle|0\rangle^{\otimes a} \mapsto |y\rangle|f_n(y)\rangle|0\rangle^{\otimes(a-1)}$, where $y \in \{0,1\}^n$. The Hadamard-Toffoli circuit for f_n, which we call HT_n^f, is defined as follows [15], where it has n input qubits and a ancillary qubits including the output qubit: apply H gates on the input qubits, then apply C_n^f on the $n+a$ qubits by using the n input qubits as the input qubits for C_n^f. It can be shown that, for any f_n, HT_n^f is weakly simulatable and that, unless $\mathsf{FP} = \#\mathsf{P}$, that is, unless $\mathsf{P} = \mathsf{PP}$ [4], there exists an f_n such that HT_n^f is not strongly simulatable [15].

By Lemma 1, for any HT_n^f with n input qubits and a ancillary qubits, there exists a QNC^0 circuit D_n^f with n input qubits and $a + b$ ancillary qubits. As in the proof of Lemma 2, we consider a $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit E_n^f, which is defined similarly to E_n except that D_n in E_n is replaced with D_n^f. We can show the following lemma:

Lemma 4 *The following statements hold:*

(1). For any polynomial-time computable function f_n, E_n^f is weakly simulatable.

(2). If, for any polynomial-time computable function f_n, E_n^f is strongly simulatable, then $\mathsf{P} = \mathsf{PP}$.

Proof: Let f_n be a polynomial-time computable function. For any $x \in \{0,1\}^n$, when the input state is $|x\rangle$, the output state of HT_n^f is

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle |f_n(y)\rangle |0\rangle^{\otimes(a-1)},$$

where $x \cdot y$ represents the inner product of x and y modulo 2. By the construction of E_n^f and Lemma 1,

$$\Pr[E_n^f(x) = 1] = \Pr[D_n^f(x) = 1 \& \mathrm{post}_n(x) = 1^b] = \frac{\#_n^f(1)}{2^{n+b}},$$

where $\#_n^f(c) = |\{y \in \{0,1\}^n | f_n(y) = c\}|$ for any $c \in \{0,1\}$. We define a polynomial-time probabilistic classical algorithm A as follows, where the input is $x \in \{0,1\}^*$ of length n:

1. Choose $y \in \{0,1\}^n$ and $r \in \{0,1\}^{b(n)}$ uniformly at random.
2. Set $A(x) = f_n(y)$ if $r = 1^b$ and $A(x) = 0$ otherwise.

By the definition of A, $\Pr[A(x) = 1] = \frac{\#_n^f(1)}{2^{n+b}}$. Thus, (1) holds.

We assume that E_n^f is strongly simulatable. By the definition, there exists a polynomial-time deterministic classical algorithm A such that, for any $x \in \{0,1\}^*$ of length n,

$$|A(x) - \Pr[E_n^f(x) = 1]| = \left| A(x) - \frac{\#_n^f(1)}{2^{n+b}} \right| \leq \frac{1}{2^{n+b+2}}.$$

This implies that $|2^{n+b} \cdot A(x) - \#_n^f(1)| \leq 1/2^2$. This yields a polynomial-time deterministic classical algorithm for computing $\#_n^f(1)$ and $\#_n^f(0) = 2^n - \#_n^f(1)$, which implies $\mathsf{FP} = \#\mathsf{P}$ and thus $\mathsf{P} = \mathsf{PP}$ [4]. Thus, (2) holds. □

Lemma 4 immediately implies Theorem 2.

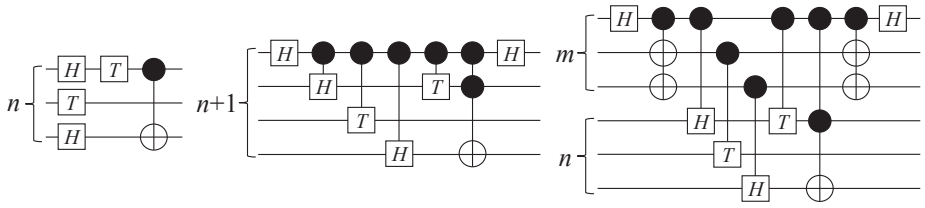
4 Circuit with Two Unbounded Fan-Out Gates

4.1 Parallelized Hadamard test

Let C_n be a polynomial-size quantum circuit with n input qubits and a ancillary qubits. The Hadamard test for C_n is the well-known quantum circuit that relates its output probability to the real or imaginary part of the matrix element $\langle 0|^{\otimes(n+a)} C_n |0\rangle^{\otimes(n+a)}$ [17]. It has n input qubits and $a+1$ ancillary qubits including the output qubit. The circuit is defined as follows: apply an H gate on the output qubit, then apply the controlled version of C_n on the $n+a+1$ qubits by using the output qubit as the control qubit, and then apply an H gate on the output qubit. For example, let C_3 be the quantum circuit depicted in Fig. 2(a). In this case, $a = 0$ and the Hadamard test for the circuit is depicted in Fig. 2(b), where the top qubit is the output qubit.

A key circuit for showing Theorem 3 is a parallelized version of the Hadamard test. It relates its output probability to the matrix element as the standard Hadamard test. Moreover, the depth of the parallelized version of the Hadamard test for a QNC^0 circuit is constant, in contrast to the fact that, in general, the depth of the standard Hadamard test for a QNC^0 circuit is polynomial in the length of the input. Let C_n be a polynomial-size quantum circuit with n input qubits and a ancillary qubits, U_1 be a single-qubit unitary gate, and m be the maximum number of gates included in a layer in C_n. We define a quantum circuit, which we call the parallelized Hadamard test for C_n and U_1, as follows, where it has n input qubits, a ancillary qubits for C_n, and new m ancillary qubits including the output qubit:

1. Apply an H gate on the output qubit.



(a) (b) (c)

Fig. 2. (a) A quantum circuit C_3 with $a = 0$. (b) The Hadamard test for C_3 in (a). (c) The parallelized Hadamard test for C_3 in (a) and $U_1 = I$. In this case, $m = 3$. The gate next to H is an unbounded fan-out gate, where the top qubit is the control qubit.

2. Apply an unbounded fan-out gate on the new m ancillary qubits, where the output qubit is used as the control qubit.

3. Apply the controlled version of C_n, where the new m ancillary qubits are used as the control qubits. The gates of the controlled version of C_n are arranged so that, if the original gates in C_n are in a layer, their controlled versions are also in a layer in this new circuit.

4. This step is the same as Step 2.

5. This step is the same as Step 1.

6. Apply the U_1 gate on the output qubit.

The parallelized Hadamard test for the circuit in Fig. 2(a) and $U_1 = I$ is depicted in Fig. 2(c), where the top qubit is the output qubit and $m = 3$.

The parallelized Hadamard test is described by the gates that are not our elementary gates. Fortunately, we can decompose such gates exactly into constant-depth constant-size quantum circuits using our elementary gates as shown in [5]. Moreover, the output probabilities of the parallelized Hadamard test for C_n are related to the real and imaginary parts of $\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}$ as follows, where $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ are the real and imaginary parts of z, respectively, for any $z \in \mathbf{C}$:

Lemma 5 *For any* QNC^0 *circuit* C_n *(with* n *input qubits and* a *ancillary qubits) and single-qubit unitary gate* U_1 *generated by a constant number of* H *and* T *gates, there exists a* $\mathsf{QNC}^0_{\mathrm{f},2}$ *circuit* D_n *that implements the same operation exactly as the parallelized Hadamard test for* C_n *and* U_1*. Moreover, for any* $x \in \{0,1\}^*$ *of length* n*, when the input state is* $|x\rangle$ *and* $U_1 = I$*, it holds that*

$$\Pr[D_n(x) = 0] = \frac{1 + \mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})}{2}.$$

Similarly, when $U_1 = HT^2$*, it holds that*

$$\Pr[D_n(x) = 0] = \frac{1 + \mathrm{Im}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})}{2}.$$

Proof: Let C_n be a QNC^0 circuit and U_1 be a single-qubit unitary gate generated by a constant number of H and T gates. The non-elementary gates in the parallelized Hadamard

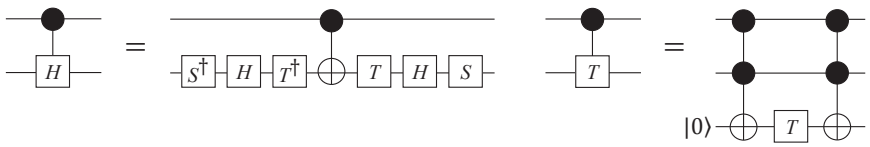


Fig. 3. Decompositions of the controlled-H and controlled-T gates [5], where $T^\dagger = T^7$, $S = T^2$, and $S^\dagger = T^6$.

test for C_n and U_1 are a controlled-H gate, a controlled-T gate, and a controlled-CNOT gate. The controlled-CNOT gate is a Toffoli gate, which can be decomposed exactly into a constant-depth constant-size quantum circuit consisting of H, T, and CNOT gates with no ancillary qubits [18]. Moreover, as shown in [5], the controlled-H and controlled-T gates can be decomposed as depicted in Fig. 3. In particular, the decomposition of the controlled-T gate requires one ancillary qubit (initialized to $|0\rangle$), which is reset to $|0\rangle$ at the end of the computation. Thus, by adding at most $t = \mathrm{poly}(n)$ ancillary qubits, we can obtain $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit D_n that implements the same operation exactly as the parallelized Hadamard test for C_n and U_1, where t is the number of controlled-T gates in the parallelized Hadamard test.

We assume that U_1 maps $|0\rangle$ and $|1\rangle$ to $\alpha|0\rangle + \beta|1\rangle$ and $\gamma|0\rangle + \delta|1\rangle$, respectively, and that the input state is $|x\rangle$. A direct calculation shows that the output state of D_n is

$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle^{\otimes(m-1)}\left(\alpha\frac{|x\rangle|0\rangle^{\otimes a}+C_n|x\rangle|0\rangle^{\otimes a}}{\sqrt{2}}+\gamma\frac{|x\rangle|0\rangle^{\otimes a}-C_n|x\rangle|0\rangle^{\otimes a}}{\sqrt{2}}\right)|0\rangle^{\otimes t}$$
$$+\frac{1}{\sqrt{2}}|1\rangle|0\rangle^{\otimes(m-1)}\left(\beta\frac{|x\rangle|0\rangle^{\otimes a}+C_n|x\rangle|0\rangle^{\otimes a}}{\sqrt{2}}+\delta\frac{|x\rangle|0\rangle^{\otimes a}-C_n|x\rangle|0\rangle^{\otimes a}}{\sqrt{2}}\right)|0\rangle^{\otimes t},$$

where the first qubit is the output qubit. This implies that

$$\Pr[D_n(x)=0]=\frac{1}{2}+\frac{|\alpha|^2-|\gamma|^2}{2}\cdot\mathrm{Re}(\langle x|\langle 0|^{\otimes a}C_n|x\rangle|0\rangle^{\otimes a})-\mathrm{Im}(\alpha\gamma^*)\cdot\mathrm{Im}(\langle x|\langle 0|^{\otimes a}C_n|x\rangle|0\rangle^{\otimes a}).$$

When $U_1 = I$, $\alpha = 1$ and $\gamma = 0$. Thus, it holds that

$$\Pr[D_n(x)=0]=\frac{1+\mathrm{Re}(\langle x|\langle 0|^{\otimes a}C_n|x\rangle|0\rangle^{\otimes a})}{2}.$$

When $U_1 = HT^2$, $\alpha = 1/\sqrt{2}$ and $\gamma = i/\sqrt{2}$. Thus, it holds that

$$\Pr[D_n(x)=0]=\frac{1+\mathrm{Im}(\langle x|\langle 0|^{\otimes a}C_n|x\rangle|0\rangle^{\otimes a})}{2}.$$

Thus, the desired relationships hold. □

In the following, the parallelized Hadamard test represents the $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit consisting only of our elementary gates. Lemma 5 implies the following relationship between the strong simulatability of the parallelized Hadamard test and the problem of computing a matrix element:

Lemma 6 *The following statements are equivalent:*

(1). For any QNC^0 *circuit* C_n *and single-qubit unitary gate* $U_1 \in \{I, HT^2\}$*, the parallelized Hadamard test for* C_n *and* U_1 *is strongly simulatable.*

(2). For any QNC^0 *circuit* C_n*, there exists a polynomial-time deterministic classical algorithm for computing* $\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}$ *with exponential precision. More precisely, for any polynomial* p*, there exists a polynomial-time deterministic classical algorithm* A *such that, for any* $x \in \{0,1\}^*$ *of length* n*,*

$$|A(x) - \mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})| \leq \frac{1}{2^{p(n)}}.$$

Moreover, such an algorithm exists also for computing the imaginary part.

Proof: We assume that (1) holds. Let C_n be a QNC^0 circuit and p be a polynomial. We consider the parallelized Hadamard test D_n for C_n and $U_1 = I$. With the assumption, there exists a polynomial-time deterministic classical algorithm A such that, for any $x \in \{0,1\}^*$ of length n,

$$|(1 - A(x)) - \Pr[D_n(x) = 0]| \leq \frac{1}{2^{p(n)+1}}.$$

Lemma 5 implies that

$$|(1 - 2 \cdot A(x)) - \mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})| \leq \frac{1}{2^{p(n)}}.$$

This implies that there exists a polynomial-time deterministic classical algorithm for computing $\mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})$ with exponential precision. A similar argument with the parallelized Hadamard test for C_n and $U_1 = HT^2$ yields such an algorithm for computing the imaginary part. Thus, (2) holds. Similarly, we can show that (2) implies (1). □

4.2 Proof of Theorem 3

To show Theorem 3, we need the following lemma, which is a simple consequence of Lemma 1 and the results in [7, 17]:

Lemma 7 *The following statements are equivalent:*

(1). For any QNC^0 *circuit* C_n*, there exists a polynomial-time deterministic classical algorithm for computing* $\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}$ *with exponential precision.*

(2). For any polynomial-size quantum circuit C_n*, there exists a polynomial-time deterministic classical algorithm for computing* $\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}$ *with exponential precision.*

(3). $\mathsf{P} = \mathsf{PP}$.

Proof: It is obvious that (2) implies (1). We assume that (1) holds. Let C_n be a polynomial-size quantum circuit (with n input qubits and a ancillary qubits) and p be a polynomial. By Lemma 1, there exists a QNC^0 circuit D_n with n input qubits and $a+b$ ancillary qubits such that b is even, $b = O(\mathrm{size}(C_n))$, and, for any $x \in \{0,1\}^*$ of length n,

$$\langle x|\langle 0|^{\otimes (a+b)} D_n |x\rangle |0\rangle^{\otimes (a+b)} = \frac{1}{\sqrt{2^b}} \langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}.$$

More precisely, D_n is the circuit in Lemma 1 combined with X gates on the postselection qubits. With the assumption, there exists a polynomial-time deterministic classical algorithm A such that, for any $x \in \{0,1\}^*$ of length n,

$$|A(x) - \mathrm{Re}(\langle x|\langle 0|^{\otimes (a+b)} D_n |x\rangle |0\rangle^{\otimes (a+b)})| \leq \frac{1}{2^{p(n)+b}}.$$

The above equation implies that

$$|\sqrt{2^b} \cdot A(x) - \mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})| \leq \frac{\sqrt{2^b}}{2^{p(n)+b}} \leq \frac{1}{2^{p(n)}}.$$

This implies that there exists a polynomial-time deterministic classical algorithm for computing $\mathrm{Re}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})$ with exponential precision. Similarly, a polynomial-time deterministic classical algorithm for computing $\mathrm{Im}(\langle x|\langle 0|^{\otimes (a+b)} D_n |x\rangle |0\rangle^{\otimes (a+b)})$ yields such an algorithm for computing $\mathrm{Im}(\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a})$. Thus, (2) holds.

It is known that $\mathsf{P} = \mathsf{PP}$ if and only if $\mathsf{FP} = \#\mathsf{P}$ [4]. As shown in [17], for any polynomial-time computable function $f_n : \{0,1\}^n \to \{0,1\}$, which corresponds to a polynomial-time decidable relation, the problem of computing $|\{x \in \{0,1\}^n | f_n(x) = 0\}|$ can be reduced to that of computing $\langle 0|^{\otimes (n+a)} C_n |0\rangle^{\otimes (n+a)}$ with exponential precision for some polynomial-size quantum circuit C_n. Thus, (2) implies (3). On the other hand, the problem of computing $\langle x|\langle 0|^{\otimes a} C_n |x\rangle |0\rangle^{\otimes a}$ with exponential precision for any polynomial-size quantum circuit C_n can be reduced to that of computing $\#\mathsf{P}$ functions [7]. Thus, (3) implies (2). □

Lemmas 6 and 7 immediately imply the characterization of the relationship $\mathsf{P} = \mathsf{PP}$. That is, $\mathsf{P} = \mathsf{PP}$ if and only if, for any QNC^0 circuit C_n and single-qubit unitary gate $U_1 \in \{I, HT^2\}$, the parallelized Hadamard test for C_n and U_1 is strongly simulatable. As shown in Lemma 5, the parallelized Hadamard test for any QNC^0 circuit C_n and $U_1 \in \{I, HT^2\}$ is a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit. Thus, this characterization implies Theorem 3.

5 Conclusions and Future Work

We considered the classical simulatability of constant-depth polynomial-size quantum circuits followed by only one single-qubit measurement. First, we provided evidence for the hardness of weakly simulating a $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit. Then, we characterized the relationship $\mathsf{P} = \mathsf{PP}$ using the strong simulatability of a $\mathsf{QNC}^0_{\mathrm{f},2}$ circuit and provided evidence for the hardness of strongly simulating such a circuit. These results are in contrast to the fact that any QNC^0 circuit followed by only one single-qubit measurement is strongly and weakly simulatable.

Interesting challenges would be to further study the classical simulatability of constant-depth polynomial-size quantum circuits. For example, can we show that, if any $\mathsf{QNC}^0_{\mathrm{t},1}$ circuit (followed by only one single-qubit measurement) is weakly simulatable, then $\mathsf{P} = \mathsf{PP}$? Moreover, can we provide evidence for the hardness as in Theorems 1 and 3 when we consider the error $1/\mathrm{poly}(n)$ in place of $1/2^{p(n)}$ in the classical simulations? As one of the referees suggests, on the basis of the results in [13, 19, 20], it would be possible to show that there exists a $\mathsf{QNC}^0_{\mathrm{f},1}$ circuit (i.e., constant-depth quantum circuit with only one unbounded fan-out gate) that is not strongly simulatable, unless $\mathsf{P} = \mathsf{PP}$.

Acknowledgments

The authors thank the anonymous referees for their valuable comments.

References

1. Aaronson, S.: Quantum computing, postselection, and probabilistic polynomial-time. Proceedings of the Royal Society A 461, 3473–3482 (2005)

2. Aaronson, S.: BQP and the polynomial hierarchy. In: Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC). pp. 141–150 (2010)
3. Aaronson, S., Arkhipov, A.: The computational complexity of linear optics. In: Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC). pp. 333–342 (2011)
4. Arora, S., Barak, M.: Computational Complexity: A Modern Approach. Cambridge University Press (2009)
5. Bera, D., Fenner, S., Green, F., Homer, S.: Efficient universal quantum circuits. Quantum Information and Computation 10(1&2), 16–27 (2010)
6. Bremner, M.J., Jozsa, R., Shepherd, D.J.: Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proceedings of the Royal Society A 467, 459–472 (2011)
7. Dawson, C.M., Hines, A.P., Mortimer, D., Haselgrove, H.L., Nielsen, M.A., Osborne, T.J.: Quantum computing and polynomial equations over the finite field $\mathbf{Z_2}$. Quantum Information and Computation 5(2), 102–112 (2005)
8. Fenner, S., Green, F., Homer, S., Zhang, Y.: Bounds on the power of constant-depth quantum circuits. In: Proceedings of Fundamentals of Computation Theory (FCT). Lecture Notes in Computer Science, vol. 3623, pp. 44–55 (2005)
9. Goldwasser, S., Sipser, M.: Private coins versus public coins in interactive proof systems. In: Proceedings of the 18th ACM Symposium on Theory of Computing (STOC). pp. 59–68 (1986)
10. Green, F., Homer, S., Moore, C., Pollett, C.: Counting, fanout, and the complexity of quantum ACC. Quantum Information and Computation 2(1), 35–65 (2002)
11. Han, Y., Hemaspaandra, L.A., Thierauf, T.: Threshold computation and cryptographic security. SIAM Journal on Computing 26(1), 59–78 (1997)
12. Høyer, P., Špalek, R.: Quantum fan-out is powerful. Theory of Computing 1(5), 81–103 (2005)
13. Jaeger, F., Vertigan, D.L., Welsh, D.J.A.: On the computational complexity of the Jones and Tutte polynomials. Mathematical Proceedings of the Cambridge Philosophical Society 108(1), 35–53 (1990)
14. Moore, C., Nilsson, M.: Parallel quantum computation and quantum codes. SIAM Journal on Computing 31(3), 799–815 (2001)
15. van den Nest, M.: Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. Quantum Information and Computation 10(3&4), 258–271 (2010)
16. van den Nest, M.: Simulating quantum computers with probabilistic methods. Quantum Information and Computation 11(9&10), 784–812 (2011)
17. Ni, X., van den Nest, M.: Commuting quantum circuits: efficient classical simulations versus hardness results. Quantum Information and Computation 13(1&2), 54–72 (2013)
18. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
19. Shepherd, D.: Binary matroids and quantum probability distributions (2010), arXiv:quant-ph/1005.1744
20. Shepherd, D., Bremner, M.J.: Temporally unstructured quantum computation. Proceedings of the Royal Society A 465, 1413–1439 (2009)
21. Takahashi, Y., Tani, S.: Collapse of the hierarchy of constant-depth exact quantum circuits. In: Proceedings of the 28th IEEE Conference on Computational Complexity (CCC). pp. 168–178 (2013)
22. Terhal, B.M., DiVincenzo, D.P.: Adaptive quantum computation, constant-depth quantum circuits and Arthur-Merlin games. Quantum Information and Computation 4(2), 134–145 (2004)
23. Vollmer, H.: Introduction to Circuit Complexity. Springer (1999)