Quantum Information and Computation, Vol. 16, No. 3&4 (2016) 0251–0270

COMMUTING QUANTUM CIRCUITS WITH FEW OUTPUTS ARE UNLIKELY TO BE CLASSICALLY SIMULATABLE

YASUHIRO TAKAHASHI, SEIICHIRO TANI
NTT Communication Science Laboratories, NTT Corporation
Atsugi, Kanagawa 243-0198, Japan

TAKESHI YAMAZAKI, KAZUYUKI TANAKA
Mathematical Institute, Tohoku University
Sendai, Miyagi 980-8578, Japan

Received June 27, 2015
Revised December 5, 2015

We study the classical simulatability of commuting quantum circuits with n input qubits and $O(\log n)$ output qubits, where a quantum circuit is classically simulatable if its output probability distribution can be sampled up to an exponentially small additive error in classical polynomial time. Our main result is that there exists a commuting quantum circuit that is not classically simulatable unless the polynomial hierarchy collapses to the third level. This is the first formal evidence that a commuting quantum circuit is not classically simulatable even when the number of output qubits is $O(\log n)$. Then, we consider a generalized version of the circuit and clarify the condition under which it is classically simulatable. Lastly, using a proof similar to that of the main result, we provide an evidence that a slightly extended Clifford circuit is not classically simulatable.

Keywords: classical simulation, commuting quantum circuit, Clifford circuit
Communicated by: R Jozsa & B Terhal

1 Introduction and Summary of Results

One of the most important challenges in quantum information processing is to understand the difference between quantum and classical computation. An approach to meeting this challenge is to study the classical simulatability of quantum computation. Previous studies have shown that restricted models of quantum computation, such as commuting quantum circuits, contribute to this purpose [20, 6, 18, 17, 3, 2, 14, 10, 19, 7]. Because of the simplicity of such restricted models, they also contribute to identifying the source of the computational power of quantum computers. It is thus of interest to study their classical simulatability.

We study the classical simulatability of commuting quantum circuits with n input qubits and $O(\mathrm{poly}(n))$ ancillary qubits initialized to $|0\rangle$, where a commuting quantum circuit is a quantum circuit consisting of pairwise commuting gates, each of which acts on a constant number of qubits. When every gate in a commuting quantum circuit acts on at most c qubits, the circuit is said to be c-local. A commuting quantum circuit is a restricted model of quantum computation in the sense that all the gates in the circuit can be applied in an arbitrary order without affecting output states. Moreover, there exists a basis in which all the gates are diagonal and thus, under some conditions, they can be implemented simultaneously [9]. In

spite of these severe restrictions, as mentioned below, there are evidences that commuting quantum circuits are not classically simulatable in various settings [3, 14]. This remarkable feature makes such circuits particularly interesting for study.

For considering the classical simulatability, we adopt strong and weak simulations. The strong simulation of a quantum circuit is to compute its output probabilities in classical polynomial time and the weak one is to sample its output probability distribution likewise. Any strongly simulatable quantum circuit is weakly simulatable [20, 3]. Our main focus is on the hardness of classically simulating quantum circuits and thus we mainly consider weak simulatability, which yields a stronger result. Previous hardness results on the weak simulatability are usually obtained with respect to multiplicative errors or exponentially small additive errors [20, 3, 10, 19, 7]. Although most of them are obtained with respect to only one of the error settings, they can usually be turned into hardness results with respect to the other error setting. In general, it is difficult to exactly determine the relative strength of these error settings and, in this paper, we deal with exponentially small additive errors. We note that our hardness results can be turned into hardness results with respect to multiplicative errors.

In 2011, Bremner et al. [3] showed that there exists a 2-local IQP circuit with $O(\mathrm{poly}(n))$ output qubits such that it is not weakly simulatable (under a plausible assumption), where an IQP circuit is a commuting quantum circuit such that each commuting gate is diagonal in the X-basis $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$. Roughly speaking, this result means that, when the number of output qubits is sufficiently large, even a simple commuting quantum circuit is powerful. On the other hand, in 2013, Ni et al. [14] showed that any 2-local commuting quantum circuit with $O(\log n)$ output qubits is strongly simulatable, whereas there exists a 3-local commuting quantum circuit with only one output qubit such that it is not strongly simulatable (under a plausible assumption). Thus, when the number of output qubits is $O(\log n)$, the classical simulatability of commuting quantum circuits depends on the number of qubits affected by each gate. A natural question is whether there exists a commuting quantum circuit with $O(\log n)$ output qubits such that it is not weakly simulatable.

We provide the first formal evidence for answering the question affirmatively:

Theorem 1 *There exists a 5-local commuting quantum circuit with $O(\log n)$ output qubits such that it is not weakly simulatable unless the polynomial hierarchy* PH *collapses to the third level, i.e., unless* $\mathsf{PH} = \Delta_3^p$.

It is widely believed that PH does not collapse to any level [16]. Thus, the circuit in Theorem 1 is a desired evidence. To prove Theorem 1, we first show that there exists a depth-3 quantum circuit A_n with $O(\mathrm{poly}(n))$ output qubits such that it is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$. Our idea for constructing the circuit in Theorem 1 is to decrease the number of the output qubits by combining A_n with an OR reduction quantum circuit [9], which reduces the computation of the OR function on k bits to that on $O(\log k)$ bits. The resulting circuit has only $O(\log n)$ output qubits and is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$, but it is not a commuting quantum circuit. An important observation is that the OR reduction circuit can be transformed into a 2-local commuting quantum circuit. We regard a quantum circuit consisting of A_n, g, and $A_n^\dagger$ as a single gate $A_n^\dagger g A_n$ for any gate g that is either a ΛX gate or a commuting gate in the commuting OR reduction circuit, where $A_n^\dagger$ is the circuit obtained from A_n by reversing the order of the gates and replacing each gate with its inverse. A rigorous analysis of a quantum circuit consisting of the gates $A_n^\dagger g A_n$ implies Theorem 1.

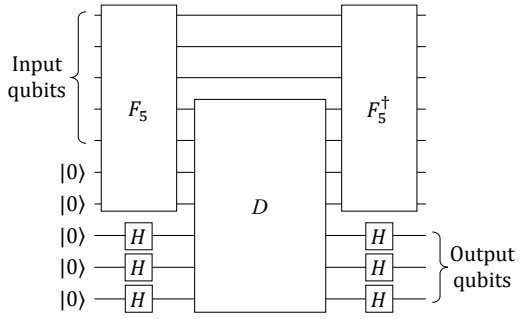


Fig. 1. Circuit $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$, where $n = 5$, $s = 2$, $t = 4$, and $l = 3$.

Then, we study the weak simulatability of a generalized version of the circuit in Theorem 1. We assume that we are given two quantum circuits F_n and D: F_n has n input qubits, $s = O(\mathrm{poly}(n))$ ancillary qubits, and t output qubits, and D is a commuting quantum circuit on $t + l$ qubits such that each commuting gate is diagonal in the Z-basis $\{|0\rangle, |1\rangle\}$, where $l = O(\log n)$. We consider the circuit of the form depicted in Fig. 1, which we denote as $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$, although its precise definition is provided in Section 3.2. The input qubits and output qubits of the circuit are the input qubits of F_n and the l qubits on which H gates are applied, respectively. In particular, when F_n is A_n and D consists only of controlled phase-shift gates, a commuting version of the whole circuit is the circuit in Theorem 1. We show that the weak simulatability of F_n implies that of the whole circuit:

Theorem 2 *If F_n is weakly simulatable, then $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$ with $l = O(\log n)$ output qubits is also weakly simulatable.*

This is a generalization of the previous result that any IQP circuit with $O(\log n)$ output qubits is weakly simulatable [3], which corresponds to the case when F_n is a layer of H gates. We show Theorem 2 by generalizing the proof of that previous result. Theorem 2 implies a suggestion on how to improve Theorem 1 in terms of locality as follows. Choosing a depth-3 quantum circuit as F_n yields the 5-local commuting quantum circuit in Theorem 1 and a possible way to construct a 3- or 4-local one that is not weakly simulatable would be to somehow choose a depth-2 quantum circuit as F_n. By Theorem 2, such a construction is impossible. This is because, since any depth-2 quantum circuit is strongly (and thus weakly) simulatable [20, 11], choosing a depth-2 quantum circuit as F_n yields only a weakly simulatable quantum circuit.

Lastly, we consider Clifford circuits with n input qubits and $O(\mathrm{poly}(n))$ ancillary qubits, where the ancillary qubits are allowed to be in a general product state (not restricted to a tensor product of $|0\rangle$). In 2008, Clark et al. [4] showed that, when the number of output qubits is only one, such a Clifford circuit is strongly simulatable. A simple extension of the proof of this result implies that, even when the number of output qubits is $O(\log n)$, such a Clifford circuit is strongly simulatable. In contrast to this, we provide an evidence that a slightly extended Clifford circuit with $O(\log n)$ output qubits is not weakly simulatable:

Theorem 3 *There exists a Clifford circuit augmented by a depth-1 non-Clifford layer of elementary gates (see Section 2.1 for definition) with $O(\mathrm{poly}(n))$ ancillary qubits in a particular product state and with $O(\log n)$ output qubits such that it is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$.*

Just like Theorems 1 and 2, Theorem 3 contributes to understanding a subtle difference between quantum and classical computation. The proof of Theorem 3 is very similar to that of Theorem 1 except that the proof uses a constant-depth OR reduction circuit [9].

2 Preliminaries

2.1 Quantum Circuits

We use the standard notation for quantum states and the standard diagrams for quantum circuits [15]. Let $\mathbf{N}$ and $\mathbf{C}$ be the set of natural numbers and the set of complex numbers, respectively. The elementary gates in this paper are a Hadamard gate H, a phase-shift gate $R(\theta)$ with angle $\theta = \pm 2\pi/2^k$ for any $k \in \mathbf{N}$, and a controlled-Z gate ΛZ, where

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ R(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix},\ \Lambda Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

We denote $R(\pi)$, $R(\pi/2)$, and $HR(\pi)H$ as Z, P, and X, respectively, where Z and X (with $Y = iXZ$ and identity I) are called Pauli gates. We also denote $H\Lambda ZH$ as ΛX, which is a CNOT gate, where H acts on the target qubit. A quantum circuit consists of the elementary gates. A Clifford circuit is a quantum circuit consisting only of H, P, and ΛZ. A commuting quantum circuit is a quantum circuit consisting of pairwise commuting gates, where we do not require that each commuting gate be one of the elementary gates. In other words, when we think of a quantum circuit as a commuting quantum circuit, we are allowed to regard a group of elementary gates in the circuit as a single gate and we require that such gates be pairwise commuting.

The complexity measures of a quantum circuit are its size and depth. The size of a quantum circuit is the number of elementary gates in it. To define the depth, we consider the circuit as a set of layers $1, \ldots, d$ consisting of one-qubit or two-qubit gates, where gates in the same layer act on pairwise disjoint sets of qubits and any gate in layer j is applied before any gate in layer $j+1$. The depth of the circuit is the smallest possible value of d [6]. It might be natural to require that each gate in a layer be one of the elementary gates, but for simplicity, when we count the depth, we allow any one-qubit or two-qubit gates that can be obtained as a sequence of elementary gates in the circuit. This does not essentially affect our results, since, regardless of whether we adopt the requirement or not, the depth of the circuit we are interested in is a constant. A quantum circuit can use ancillary qubits initialized to $|0\rangle$.

We deal with a uniform family of polynomial-size quantum circuits $\{C_n\}_{n\geq 1}$, where each C_n has n input qubits and $O(\mathrm{poly}(n))$ ancillary qubits, and angles θ of phase-shift gates in C_n are restricted to $\pm 2\pi/2^k$ with $k = O(\mathrm{poly}(n))$. Some of the input and ancillary qubits are called output qubits. At the end of the computation, Z-measurements, i.e., measurements in the Z-basis, are performed on the output 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 classical description of C_n. A symbol denoting a quantum circuit, such as C_n, also denotes its matrix representation in some fixed basis. Any quantum circuit in this paper is understood to be an element of a uniform family of quantum circuits and thus, for simplicity, we deal with a quantum circuit C_n in place of a family $\{C_n\}_{n\geq 1}$. We require that

each commuting gate in a commuting quantum circuit act on a constant number of qubits. When every commuting gate acts on at most c qubits, the circuit is said to be c-local [14].

2.2 Classical Simulatability

We deal with a uniform family of polynomial-size classical circuits to model a polynomial-time deterministic classical algorithm. Similarly, to model its probabilistic version, we deal with a uniform family of polynomial-size randomized classical circuits, each of which has a register initialized with random bits for each run of the computation [3]. As in the case of quantum circuits, for simplicity, we consider a classical circuit in place of a family of classical circuits.

Let C_n be a polynomial-size quantum circuit with n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits, and m output qubits. For any $x \in \{0,1\}^n$, there exists an output probability distribution $\{(y, \Pr[C_n(x) = y])\}_{y\in\{0,1\}^m}$, where $\Pr[C_n(x) = y]$ is the probability of obtaining $y \in \{0,1\}^m$ by Z-measurements on the output qubits of C_n with the input state $|x\rangle$. The classical simulatability of C_n is defined as follows [20, 12, 3, 13, 14, 10, 19]:

Definition 1

- *C_n is strongly simulatable if $\Pr[C_n(x) = y]$ and its marginal output probabilities can be computed up to an exponentially small additive error in classical $O(\mathrm{poly}(n))$ time. More precisely, for any m' qubits $(0 < m' \le m)$ chosen from the m output qubits of C_n, and polynomial p, there exists a polynomial-size classical circuit D_n such that, for any $x \in \{0,1\}^n$ and $y' \in \{0,1\}^{m'}$,*

$$|D_n(x, y') - \Pr[C_n(x)|_{m'} = y']| \le \frac{1}{2^{p(n)}}.$$

- *C_n is weakly simulatable if $\{(y, \Pr[C_n(x) = y])\}_{y\in\{0,1\}^m}$ can be sampled up to an exponentially small additive error in classical $O(\mathrm{poly}(n))$ time. More precisely, for any polynomial p, there exists a polynomial-size randomized classical circuit R_n such that, for any $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$,*

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

Any strongly simulatable quantum circuit is weakly simulatable [20, 3].

2.3 Complexity Classes

The following two complexity classes are important for our discussion [1, 3, 8]:

Definition 2 *Let L be a language, i.e., $L \subseteq \{0,1\}^*$.*

- *$L \in \mathsf{PostBQP}$ if there exists a polynomial-size quantum circuit C_n with n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits, one output qubit, and one particular qubit (other than the output qubit) called the postselection qubit such that, for any $x \in \{0,1\}^n$,*
  - $\Pr[\mathrm{post}_n(x) = 0] > 0$,
  - *if $x \in L$,* $\Pr[C_n(x) = 1|\mathrm{post}_n(x) = 0] \ge 2/3$,
  - *if $x \notin L$,* $\Pr[C_n(x) = 1|\mathrm{post}_n(x) = 0] \le 1/3$,

  where the event "$\mathrm{post}_n(x) = 0$" means that the classical outcome of the Z-measurement on the postselection qubit is 0.

- $L \in \mathsf{PostBPP}$ *if there exists a polynomial-size randomized classical circuit* R_n *with* n *input bits that, for any* $x \in \{0,1\}^n$*, outputs* $R_n(x), \mathrm{post}_n(x) \in \{0,1\}$ *such that*
  - $\Pr[\mathrm{post}_n(x) = 0] > 0$,
  - *if* $x \in L$, $\Pr[R_n(x) = 1 | \mathrm{post}_n(x) = 0] \geq 2/3$,
  - *if* $x \notin L$, $\Pr[R_n(x) = 1 | \mathrm{post}_n(x) = 0] \leq 1/3$.

We use the notation $\mathrm{post}_n(x) = 0$ both in the quantum and classical settings, but the meaning will be clear from the context.

Another important class is the polynomial hierarchy $\mathsf{PH} = \bigcup_{j \geq 1} \Delta_j^p$. Here, $\Delta_1^p = \mathsf{P}$ and $\Delta_{j+1}^p = \mathsf{P}^{\mathsf{N}\Delta_j^p}$ for any $j \geq 1$, where P is the class of languages decided by polynomial-size classical circuits and $\mathsf{N}\Delta_j^p$ is the non-deterministic class associated to Δ_j^p [16, 3]. It is widely believed that $\mathsf{PH} \neq \Delta_j^p$ for any $j \geq 1$ [16]. As shown in Ref. [3], if $\mathsf{PostBQP} \subseteq \mathsf{PostBPP}$, then $\mathsf{PH} = \Delta_3^p$. It can be shown that, in our setting of elementary gates and quantum circuits, this relationship also holds when the condition $\Pr[\mathrm{post}_n(x) = 0] > 0$ in the definition of $\mathsf{PostBQP}$ is replaced with the condition that, for some polynomial q (depending only on C_n), $\Pr[\mathrm{post}_n(x) = 0] \geq 1/2^{q(n)}$. In the following, we adopt the latter condition.

3 Commuting Quantum Circuits

3.1 Hardness of the Weak Simulation

The key components of the circuit in Theorem 1 are the following two circuits:

- A depth-3 polynomial-size quantum circuit A_n with n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits, and $O(\mathrm{poly}(n))$ output qubits such that it is not weakly simulatable (with respect to exponentially small additive error) unless $\mathsf{PH} = \Delta_3^p$.
- The commuting version of an OR reduction quantum circuit [9], which reduces the computation of the OR function on k bits to that on $O(\log k)$ bits.

In fact, as depicted in Fig. 3(b), the circuit in Theorem 1 is of the form

$$(A_n^\dagger g_t A_n) \cdots (A_n^\dagger g_2 A_n)(A_n^\dagger g_1 A_n)(A_n^\dagger \Lambda X A_n),$$

where each g_j is a commuting gate in the commuting OR reduction circuit, t is the number of such commuting gates, and $A_n^\dagger$ is the circuit obtained from A_n by reversing the order of the gates and replacing each gate with its inverse.

The circuit described in Ref. [6], here called A_n, has depth 3, polynomial size, n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits, and $O(\mathrm{poly}(n))$ output qubits. It is not weakly simulatable with respect to *multiplicative error* unless $\mathsf{PH} = \Delta_3^p$ [3]. We show that it is not weakly simulatable in the additive-error setting, either:

Lemma 1 *The circuit* A_n *is not weakly simulatable (with respect to exponentially small additive error as in Def. 1) unless* $\mathsf{PH} = \Delta_3^p$.

We relegate the proof to Appendix A.1. By the proof of Lemma 1, we can assume that A_n has $a + b$ ancillary qubits, particular $b + 1$ qubits called the postselection qubits, and $b + 2$ output qubits, where $a = O(\mathrm{poly}(n))$, $b = O(\mathrm{poly}(n))$, and the postselection qubits are the first $b + 1$ output qubits.

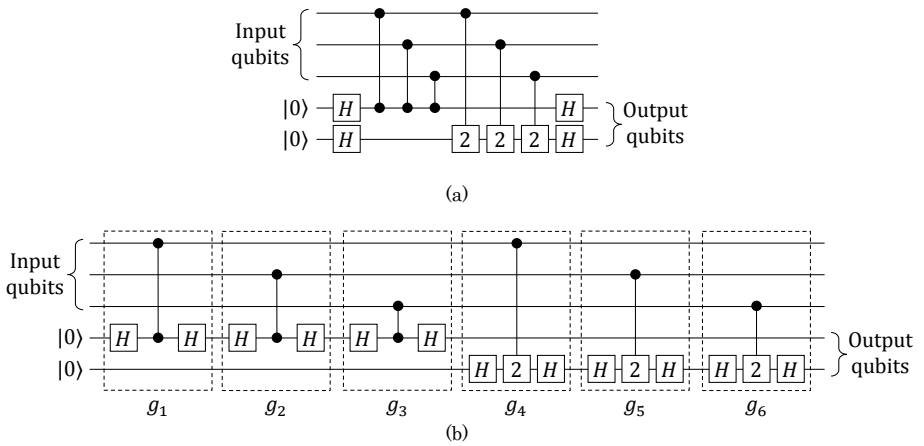


Fig. 2. (a): The non-commuting OR reduction circuit with three input qubits, where the gate represented by two black circles connected by a vertical line is a ΛZ gate, i.e., a controlled-$R(2\pi/2^1)$ gate, and the gate "2" is an $R(2\pi/2^2)$ gate. (b): The commuting OR reduction circuit with three input qubits.

We decrease the number of the first $b+1$ output qubits using an OR reduction circuit with $b+1$ input qubits [9]. The OR reduction circuit has $m = \lceil \log(b+2) \rceil$ ancillary qubits, which are also output qubits. For any input state $|x\rangle|0^m\rangle$ with $x \in \{0,1\}^{b+1}$, the circuit outputs $|x\rangle|\eta\rangle$, where $|\eta\rangle = |0^m\rangle$ if $x = 0^{b+1}$ and $\langle 0^m|\eta\rangle = 0$ otherwise. The first part consists of H gates on the ancillary qubits. The middle part consists of $b+1$ controlled-$R(2\pi/2^k)$ gates over all $1 \le k \le m$, where each gate uses an input qubit as the control qubit and an ancillary qubit as the target qubit. The last part is the same as the first one. We call the circuit the *non-commuting* OR reduction circuit. It is depicted in Fig. 2(a), where $b = 2$.

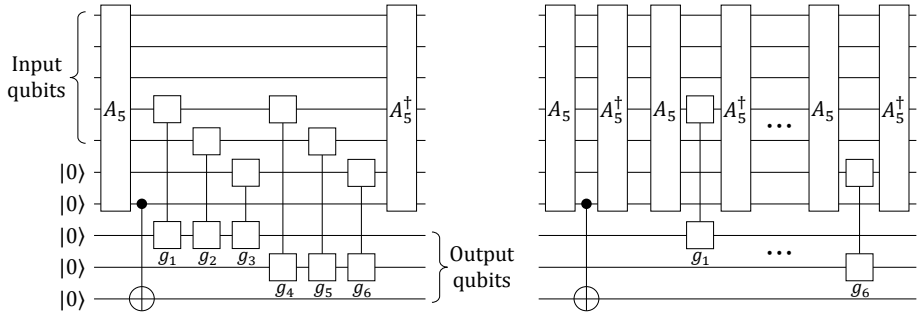
An important observation is that the non-commuting OR reduction circuit with $b+1$ input qubits can be transformed into a 2-local commuting quantum circuit with $b+1$ input qubits. This is shown by considering a quantum circuit consisting of gates g_j on two qubits, where g_j is a controlled-$R(2\pi/2^k)$ gate (in the non-commuting OR reduction circuit) sandwiched between H gates on the target qubit. Since controlled-$R(2\pi/2^k)$ gates are pairwise commuting gates on two qubits and $H^2 = I$, the gates g_j are also pairwise commuting gates on two qubits and the operation implemented by the circuit is the same as that implemented by the non-commuting OR reduction circuit. We call the circuit the *commuting* OR reduction circuit. It is depicted in Fig. 2(b), where $b = 2$.

Using A_n and the commuting OR reduction circuit, we construct a quantum circuit E_n with n input qubits, $a+b+m+1$ ancillary qubits, and $m+1$ output qubits as follows. As an example, E_n is depicted in Fig. 3(a), where $n = 5$, $a = 0$, and $b = 2$ (and thus $m = 2$).

1. Apply A_n on n input qubits and $a+b$ ancillary qubits, where the input qubits of E_n are those of A_n.

2. Apply a ΛX gate on the last output qubit of A_n and on an ancillary qubit (other than the ancillary qubits in Step 1), where the output qubit is the control qubit.

3. Apply a commuting OR reduction circuit on the $b+1$ postselection qubits of A_n and



(a) (b)

Fig. 3. (a): Circuit E_n, where $n = 5$, $a = 0$, and $b = 2$ (and thus $m = 2$). The gate represented by a black circle and $\oplus$ connected by a vertical line is a ΛX gate. The gates g_j are the ones in Fig. 2(b). (b): The commuting quantum circuit based on E_n in (a).

m ancillary qubits (other than the ancillary qubits in Steps 1 and 2), where the $b+1$ postselection qubits are the input qubits of the OR reduction circuit.

4. Apply $A_n^\dagger$ as in Step 1.

The output qubits of E_n are the $m+1$ ancillary qubits used in Steps 2 and 3. Step 4 does not affect the output probability distribution of E_n, but it allows us to construct the commuting quantum circuit described below.

We construct a commuting quantum circuit based on E_n as follows. We regard a quantum circuit consisting of A_n, g, and $A_n^\dagger$ (in this order) as a single gate $A_n^\dagger g A_n$ for any gate g that is either a ΛX gate in Step 2 of E_n or g_j in the commuting OR reduction circuit. We consider a quantum circuit consisting of the gates $A_n^\dagger g A_n$. The input qubits and output qubits of E_n are naturally considered as the input qubits and output qubits of the new circuit, respectively. The circuit based on E_n in Fig. 3(a) is depicted in Fig. 3(b). Since the gates g in E_n are pairwise commuting, so are the gates $A_n^\dagger g A_n$. Moreover, since the depth of A_n is three and g acts on two qubits, $A_n^\dagger g A_n$ acts on a constant number of qubits. Thus, the circuit is a commuting quantum circuit with $m+1 = O(\log n)$ output qubits. The following lemma holds:

Lemma 2 *The commuting quantum circuit based on E_n is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$.*

Proof: We assume that $\mathsf{PH} \neq \Delta_3^p$. By Lemma 1, A_n is not weakly simulatable. It is easy to show that the proof that A_n is not weakly simulatable depends only on $\Pr[A_n(x) = 0^{b+1}1]$ and $\Pr[A_n(x) = 0^{b+1}0]$ for any $x \in \{0,1\}^n$. By the construction of E_n, for any $x \in \{0,1\}^n$,

$$\Pr[A_n(x) = 0^{b+1}1] = \Pr[E_n(x) = 0^m 1],\ \Pr[A_n(x) = 0^{b+1}0] = \Pr[E_n(x) = 0^m 0].$$

This implies that E_n is not weakly simulatable. The proof is the same as that of Lemma 1 except that the number of output qubits we need to consider is only $m+1$. By the construction of the commuting quantum circuit based on E_n, its output probability distribution is the same as that of E_n. Thus, the commuting quantum circuit is not weakly simulatable. □

If we can show that the commuting quantum circuit based on E_n is 5-local, Lemma 2 immediately implies Theorem 1. To show that the circuit is 5-local, we give the details of

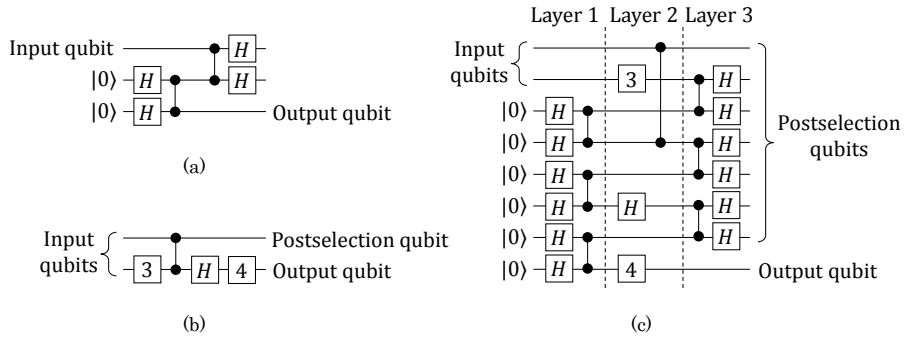


Fig. 4. (a): The teleportation circuit. (b): An example of C_n, where $n = 2$ and $a = 0$. The gate represented by $k \in \mathbf{N}$ is an $R(2\pi/2^k)$ gate. (c): Depth-3 circuit A_n constructed from C_n in (b) by the method in Ref. [6], where $b = 6$ and thus the total number of postselection qubits is seven.

the circuit obtained by applying Fenner et al.'s method for parallelizing quantum circuits [6]. This is because, as described in the proof of Lemma 1, A_n is obtained by applying the method to some PostBQP circuit C_n with n input qubits, a ancillary qubits, one output qubit, and one postselection qubit (corresponding to one of the postselection qubits of A_n). The circuit obtained by the method is based on a one-qubit teleportation circuit. We adopt the teleportation circuit depicted in Fig. 4(a), which is obtained from the standard one by decomposing it into the elementary gates. If the classical outcomes of Z-measurements on the two qubits other than the output qubit are 0, the output state is the same as the input state. We call the first measured qubit, which is the input qubit, "the first teleportation qubit", and the second one "the second teleportation qubit".

For example, we consider the circuit depicted in Fig. 4(b) as C_n, where $n = 2$ and $a = 0$. The depth-3 circuit A_n constructed from C_n by the method in Ref. [6] is depicted in Fig. 4(c), where $b = 6$ and thus the total number of postselection qubits is seven. The first layer consists of the first halves of the teleportation circuits and the third layer consists of the last halves. The second layer consists of the gates in C_n. The teleportation qubits are the postselection qubits. If all classical outcomes of Z-measurements on the teleportation qubits are 0, all teleportation circuits teleport their input states successfully and thus the output state is the same as that of C_n. We show that the commuting quantum circuit based on E_n is 5-local:

Lemma 3 *For any gate $A_n^\dagger g A_n$ in the commuting quantum circuit based on E_n, there exists a quantum circuit on at most five qubits that implements the gate.*

Proof: We simplify $A_n^\dagger g A_n$ to obtain the desired circuit on at most five qubits. We first analyze the case when $g = g_j$ in the commuting OR reduction circuit. This case is divided into the following three cases, where we represent A_n as $L_3 L_2 L_1$, each of which is a layer of A_n, and assume that g is applied on a postselection qubit q_1 and an output qubit q_2 of E_n:

- Case 1: q_1 is the first teleportation qubit (of a teleportation circuit).

  As an example, $A_n^\dagger g A_n$ is depicted in Fig. 5(a), where A_n is the circuit in Fig. 4(c), g is a controlled-$R(2\pi/2^k)$ gate sandwiched between H gates, and q_1 is the fourth qubit of A_n from the top, which is the first teleportation qubit. We note that g acts on the set of qubits $\{q_1, q_2\}$ and that there is no gate on q_2 in each layer. All ΛZ gates in layer 3 other than the one on q_1 and qubit q_3 are cancelled out in $L_3^\dagger g L_3$. Only the ΛZ gate, which is

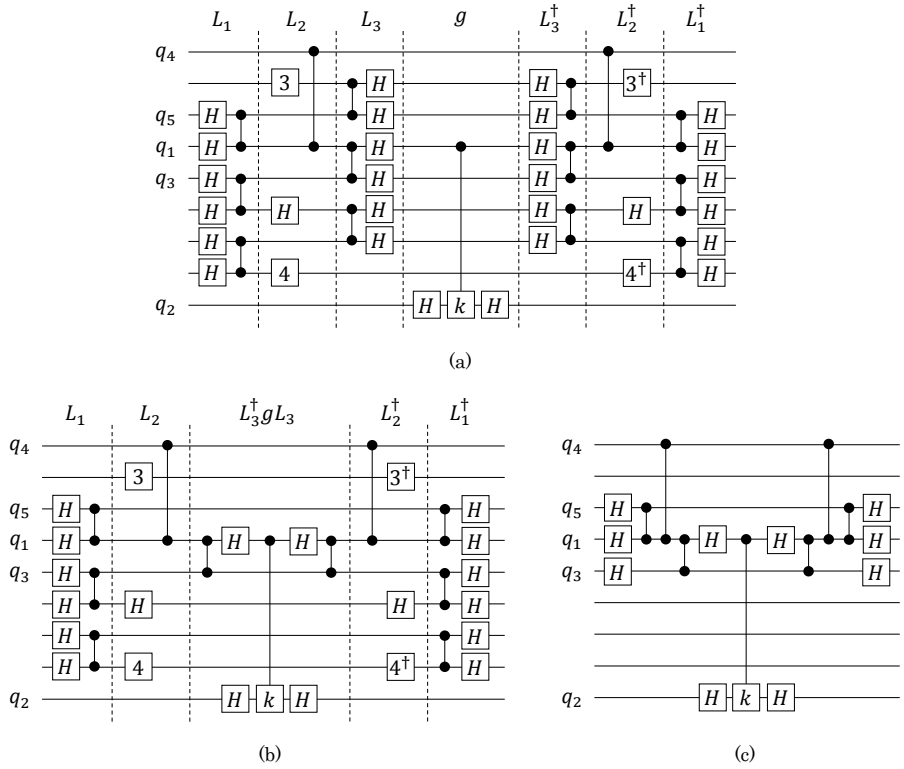


Fig. 5. (a): Gate $A_n^\dagger g A_n$, where A_n is the circuit in Fig. 4(c), g is a controlled-$R(2\pi/2^k)$ gate sandwiched between H gates, and q_1 is the fourth qubit of A_n from the top. (b): The circuit obtained from (a) by simplifying $L_3^\dagger g L_3$. (c): The circuit on five qubits obtained from (b).

not cancelled out, increases the number of qubits involved with $\{q_1, q_2\}$ by one. Thus, $L_3^\dagger g L_3$ acts on $\{q_1, q_2, q_3\}$. The circuit obtained from $A_n^\dagger g A_n$ in Fig. 5(a) by simplifying $L_3^\dagger g L_3$ is depicted in Fig. 5(b). By the construction of the teleportation circuit, there is no gate on q_3 in layer 2. Only one ΛZ gate on q_1 and qubit q_4 in layer 2 increases the number of qubits involved with $\{q_1, q_2, q_3\}$ by one. Thus, $L_2^\dagger L_3^\dagger g L_3 L_2$ acts on at most four qubits. If a ΛZ gate acts on q_3 or q_4 and on another qubit, it is cancelled out in $L_1^\dagger L_2^\dagger L_3^\dagger g L_3 L_2 L_1$. Only one ΛZ gate on q_1 and qubit q_5 in layer 1 increases the number of qubits involved with $\{q_1, q_2, q_3, q_4\}$ by one. Thus, $L_1^\dagger L_2^\dagger L_3^\dagger g L_3 L_2 L_1$ acts on at most five qubits. The circuit obtained from $A_n^\dagger g A_n$ in Fig. 5(b) is depicted in Fig. 5(c).

- Case 2: q_1 is the second teleportation qubit (of a teleportation circuit).

  As an example, $A_n^\dagger g A_n$ is depicted in Fig. 6(a), where A_n is the circuit in Fig. 4(c), g is a controlled-$R(2\pi/2^k)$ gate sandwiched between H gates, and q_1 is the second qubit of A_n from the bottom, which is the second teleportation qubit. As in Case 1, there is no gate on q_2 in each layer and $L_3^\dagger g L_3$ acts on $\{q_1, q_2, q_3\}$. The circuit obtained from $A_n^\dagger g A_n$ in Fig. 6(a) by simplifying $L_3^\dagger g L_3$ is depicted in Fig. 6(b). By the construction of the teleportation circuit, there is no gate on q_1 in layer 2. If a ΛZ gate acts on q_3 and a qubit in layer 2, it is cancelled out in $L_2^\dagger L_3^\dagger g L_3 L_2$. Thus, gates in layer 2 do not

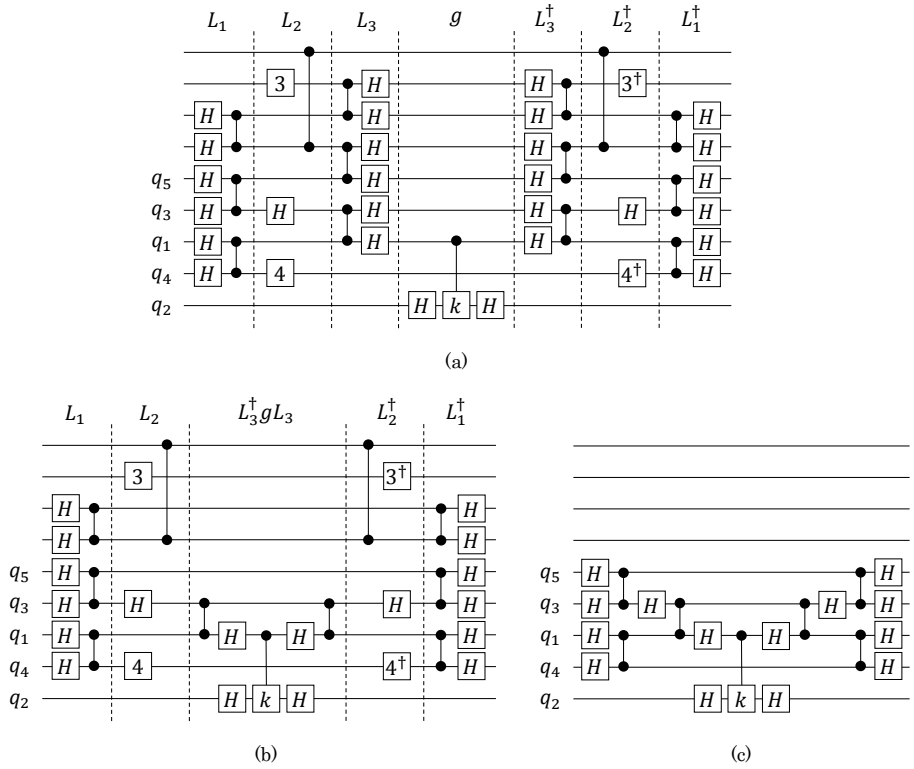


Fig. 6. (a): Gate $A_n^\dagger g A_n$, where A_n is the circuit in Fig. 4(c), g is a controlled-$R(2\pi/2^k)$ gate sandwiched between H gates, and q_1 is the second qubit of A_n from the bottom. (b): The circuit obtained from (a) by simplifying $L_3^\dagger g L_3$. (c): The circuit on five qubits obtained from (b).

increase the number of qubits involved with $\{q_1, q_2, q_3\}$. In layer 1, a ΛZ gate on q_1 and qubit q_4 increases the number of qubits involved with $\{q_1, q_2, q_3\}$ by one, and so does a ΛZ gate on q_3 and qubit q_5. In particular, the latter happens only when an H gate acts on q_3 in layer 2. This is because, when any other gate (i.e., ΛZ or $R(\pm 2\pi/2^k)$) acts on q_3 in layer 2, it is cancelled out in $L_2^\dagger L_3^\dagger g L_3 L_2$ and thus a ΛZ gate on q_3 and qubit q_5 is also cancelled out in $L_1^\dagger L_2^\dagger L_3^\dagger g L_3 L_2 L_1$. Thus, $L_1^\dagger L_2^\dagger L_3^\dagger g L_3 L_2 L_1$ acts on at most five qubits. The circuit obtained from $A_n^\dagger g A_n$ in Fig. 6(b) is depicted in Fig. 6(c).

- Case 3: q_1 is the postselection qubit corresponding to the one of C_n.

  As in the above cases, there is no gate on q_2 in each layer. By the construction of A_n, there is no gate on q_1 in layer 3. Thus, it suffices to consider only $L_2 L_1$. Since g acts on two qubits and the number of qubits on which both g and $L_2 L_1$ are applied is one, $L_1^\dagger L_2^\dagger g L_2 L_1$ acts on at most $2^2 + 1 = 5$ qubits.

The analysis for Case 3 works for the remaining case when $g = \Lambda X$ in Step 2 of E_n. □

As described above, Lemma 2 combined with Lemma 3 immediately implies Theorem 1. In the argument used to show Theorem 1, the values of the input do not play an important role. Thus, the theorem still holds when all input qubits have to be $|0\rangle$, or even some (separable)

non-computational basis state such as $|+\rangle = H|0\rangle$, along with the definition of the uniform family of circuits provided in Ref. [3].

The gate set in the above proof of Theorem 1 is $\{H, \Lambda Z\} \cup \{R(\pm 2\pi/2^k) | k \in \mathbf{N}\}$. We discuss whether Theorem 1 holds when we adopt the finite universal gate set $\mathcal{G} = \{H, R(\pi/4), \Lambda Z\}$. The circuit in Theorem 1 consists of A_n, $A_n^\dagger$, a $\Lambda X (= H\Lambda ZH)$ gate, and the commuting OR reduction circuit, where A_n is obtained from some PostBQP circuit C_n and uses only gates in C_n, H gates, and ΛZ gates. We can assume that all gates in C_n are drawn from $\mathcal{G}$ [1]. Moreover, the inverse of each gate in $\mathcal{G}$ is exactly implemented by the gates in $\mathcal{G}$. Thus, A_n and $A_n^\dagger$ consist of the gates in $\mathcal{G}$, and the proof of Theorem 1 works if we have a commuting OR reduction circuit using gates drawn from $\mathcal{G}$. Since it is difficult to construct such a circuit exactly [9], we construct an approximate one. To do this, each gate g_j in the original commuting OR reduction circuit is approximated up to a precision exponential in n by using the Solovay-Kitaev algorithm [5]. The proof of Theorem 1 with the approximate circuit works, but the only problem is that the resulting circuit is not a commuting quantum circuit. This is because, in general, approximate gates $\widetilde{g}_j$ are not pairwise commuting, although they are approximately pairwise commuting in the sense that $\widetilde{g}_i\widetilde{g}_j$ and $\widetilde{g}_j\widetilde{g}_i$ are exponentially close. Thus, if we define a commuting quantum circuit as a quantum circuit consisting of approximately pairwise commuting gates, Theorem 1 holds when we adopt $\mathcal{G}$.

3.2 Weak Simulatability of a Generalized Version

As in Fig. 2(a), a non-commuting OR reduction circuit with $b+1$ input qubits can be represented as three parts: the first part consists of H gates on $m = \lceil \log(b+2) \rceil$ qubits, the middle part a quantum circuit D', and the last part H gates on m qubits, where D' consists only of controlled-$R(2\pi/2^k)$ gates. Since ΛX in Step 2 of E_n is $H\Lambda ZH$, the circuit in Theorem 1 can be represented similarly: the first part consists of A_n and H gates on $m+1$ qubits, the middle part D'', and the last part $A_n^\dagger$ and H gates on $m+1$ qubits, where D'' consists of D' and ΛZ, and A_n has $a+b$ ancillary qubits and $b+2$ output qubits. The output qubits of the whole circuit are the $m+1$ qubits on which H gates are applied.

We consider a generalized version of the circuit in Theorem 1. We assume that we are given two quantum circuits F_n and D: F_n has n input qubits, $s = O(\mathrm{poly}(n))$ ancillary qubits, and t output qubits, and D is a commuting quantum circuit on $t+l$ qubits such that each commuting gate is diagonal in the Z-basis, where $l = O(\log n)$. We construct a quantum circuit with n input qubits, $s+l$ ancillary qubits, and l output qubits as follows, where we denote this circuit as $(F_n^\dagger \otimes H^{\otimes l}) D (F_n \otimes H^{\otimes l})$. As an example, the circuit is depicted in Fig. 1, where $n = 5$, $s = 2$, $t = 4$, and $l = 3$.

1. Apply F_n on n input qubits and s ancillary qubits, where the input qubits of the whole circuit are those of F_n.

2. Apply H gates on l ancillary qubits (other than the ancillary qubits in Step 1).

3. Apply D on $t+l$ qubits, which are the output qubits of F_n and the ancillary qubits in Step 2.

4. Apply H gates as in Step 2 and then $F_n^\dagger$ as in Step 1.

The output qubits of the whole circuit are the l qubits on which H gates are applied. The circuit in Theorem 1 corresponds to the case when $F_n = A_n$, $D = D''$, $s = a + b$, $t = b + 2$, and $l = m + 1$.

When F_n is a layer of H gates with arbitrary s and t, $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$ is weakly simulatable [3]. A simple generalization of the proof of that previous result implies Theorem 2. In fact, roughly speaking, the classical algorithm for weakly simulating $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$ can be described as follows: fix the state of the qubits other than the $O(\log n)$ output qubits on the basis of the assumption in Theorem 2 and then follow the change of the states of the output qubits. We describe this algorithm precisely. Let $p(n)$ be an arbitrary polynomial. By the assumption that F_n is weakly simulatable, there exists a polynomial-size randomized classical circuit R_n such that, for any $x \in \{0,1\}^n$ and $z \in \{0,1\}^t$,

$$|\Pr[R_n(x) = z] - \Pr[F_n(x) = z]| \leq \frac{1}{2^{p(n)+t}}.$$

Since D consists only of gates that are diagonal in the Z-basis, for any $z \in \{0,1\}^t$ and $w \in \{0,1\}^l$, there exists some value $f(z,w)$ computed from the diagonal elements of D such that $D|z\rangle|w\rangle = e^{if(z,w)}|z\rangle|w\rangle$. We consider a polynomial-size randomized classical circuit T_n that implements the following classical algorithm, where the input is $x \in \{0,1\}^n$:

1. Compute $z_0 = R_n(x) \in \{0,1\}^t$.
2. Compute the probability of obtaining y by Z-measurements on the state

$$\frac{1}{\sqrt{2^l}} \sum_{w \in \{0,1\}^l} e^{if(z_0,w)} H^{\otimes l}|w\rangle$$

   for every $y \in \{0,1\}^l$.
3. Output $y \in \{0,1\}^l$ according to the probability distribution computed in Step 2.

The probability in Step 2 is represented as

$$\frac{1}{2^l} \sum_{w,w' \in \{0,1\}^l} e^{-if(z_0,w')+if(z_0,w)} \langle w'|H^{\otimes l}|y\rangle\langle y|H^{\otimes l}|w\rangle.$$

We can compute $f(z_0, w)$ using a polynomial-size classical circuit. This is because D has only polynomially many gates and, for each gate g, it is easy to classically compute $\gamma_g \in \mathbf{C}$ such that $g|z_0\rangle|w\rangle = \gamma_g|z_0\rangle|w\rangle$ by using the classical description of D, which includes information about the complex numbers defining g and the qubit numbers on which g is applied. Moreover, since the state in Step 2 is only on $l = O(\log n)$ qubits, we can compute the probability in Step 2 up to an exponentially small additive error using a polynomial-size classical circuit. We can show that the above algorithm generates the output probability distribution of $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$. We relegate the proof to Appendix A.2.

4 Clifford Circuits

The construction of the circuit in Theorem 3 is similar to that of the circuit in Theorem 1. The key components are the following two circuits:

- A Clifford circuit Q_n with n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits in a particular product state, and $O(\mathrm{poly}(n))$ output qubits such that it is not weakly simulatable (with respect to exponentially small additive error) unless $\mathsf{PH} = \Delta_3^p$.
- A constant-depth OR reduction circuit with unbounded fan-out gates [9], where an unbounded fan-out gate is a gate that is obtained by regarding a sequence of ΛX gates with the same control qubit as a single gate.

The circuit in Theorem 3 is a modification of the combination of these circuits.

The Clifford circuit described in Ref. [10], here called Q_n, has n input qubits, $O(\mathrm{poly}(n))$ ancillary qubits in a particular product state, and $O(\mathrm{poly}(n))$ output qubits. It is not weakly simulatable with respect to *multiplicative error* unless $\mathsf{PH} = \Delta_3^p$ [10]. We show that Q_n is not weakly simulatable in the additive-error setting, either:

Lemma 4 *The circuit Q_n is not weakly simulatable (with respect to exponentially small additive error as in Def. 1) unless $\mathsf{PH} = \Delta_3^p$.*

We relegate the proof to Appendix A.3. By the proof of Lemma 4, we can assume that Q_n has $a = O(\mathrm{poly}(n))$ ancillary qubits initialized to $|0\rangle$, $b = O(\mathrm{poly}(n))$ ancillary qubits in a product state $|\varphi\rangle^{\otimes b}$, particular $b+1$ qubits called the postselection qubits, and $b+2$ output qubits, where $|\varphi\rangle = R(\pi/4)H|0\rangle = (|0\rangle + e^{i\pi/4}|1\rangle)/\sqrt{2}$ and the postselection qubits are the first $b+1$ output qubits.

We decrease the number of the first $b+1$ output qubits of Q_n as in E_n. To do this, we construct a quantum circuit E'_n with n input qubits and $a+b+m+1$ ancillary qubits as follows, where $m = \lceil \log(b+2) \rceil$. As an example, E'_n is depicted in Fig. 7(a), where $n = 5$, $a = 0$, and $b = 2$.

1. Apply Q_n on n input qubits, a ancillary qubits initialized to $|0\rangle$, and b ancillary qubits initialized to $|\varphi\rangle$, where the input qubits of E'_n are those of Q_n.
2. Apply a ΛX gate on the last output qubit of Q_n and on an ancillary qubit (other than the ancillary qubits in Step 1), where the output qubit is the control qubit.
3. Apply a *non-commuting* OR reduction circuit on the $b+1$ postselection qubits of Q_n and m ancillary qubits (other than the ancillary qubits in Steps 1 and 2), where the $b+1$ postselection qubits are the input qubits of the OR reduction circuit.

The output qubits of E'_n are the $m+1$ ancillary qubits used in Steps 2 and 3. The circuit E'_n is a Clifford circuit combined with an OR reduction circuit with $O(\mathrm{poly}(n))$ ancillary qubits in a particular product state and with $O(\log n)$ output qubits. Using Lemma 4 and a proof similar to that of Lemma 2, we show the following lemma:

Lemma 5 *The circuit E'_n is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$.*

Proof: We assume that $\mathsf{PH} \neq \Delta_3^p$. By Lemma 4, Q_n is not weakly simulatable. It is easy to show that the proof that Q_n is not weakly simulatable depends only on $\Pr[Q_n(x) = 0^{b+1}1]$ and $\Pr[Q_n(x) = 0^{b+1}0]$ for any $x \in \{0,1\}^n$. By the construction of E'_n, for any $x \in \{0,1\}^n$,

$$\Pr[Q_n(x) = 0^{b+1}1] = \Pr[E'_n(x) = 0^m 1],\ \Pr[Q_n(x) = 0^{b+1}0] = \Pr[E'_n(x) = 0^m 0].$$

This implies that E'_n is not weakly simulatable. The proof is the same as that of Lemma 4 except that the number of output qubits we need to consider is only $m+1$. □

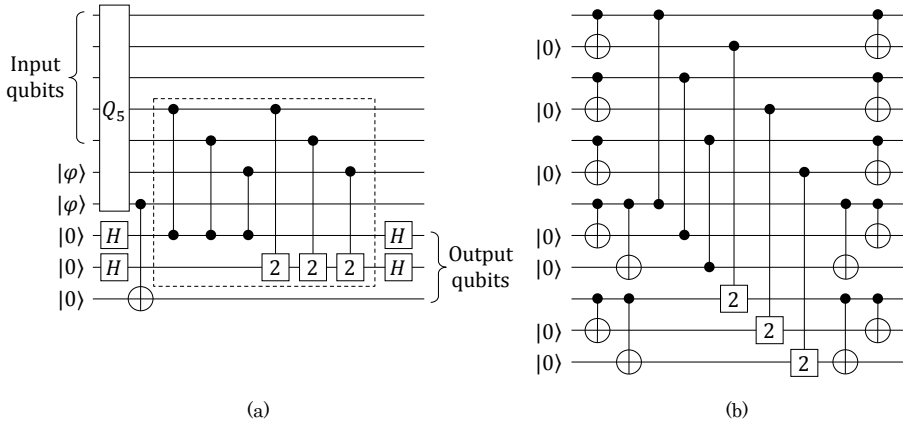


Fig. 7. (a): Circuit E'_n, where $n = 5$, $a = 0$, and $b = 2$. The dashed box represents the middle part of the non-commuting OR reduction circuit. (b): The circuit obtained from the middle part in (a). The qubits in state $|0\rangle$ are new ancillary qubits, which are not depicted in (a).

Using Lemma 5 and a modified version of E'_n, we show Theorem 3:

Proof of Theorem 3: We assume that $\mathsf{PH} \neq \Delta_3^p$. By Lemma 5, E'_n is not weakly simulatable. We modify E'_n as follows. First, we replace the non-commuting OR reduction circuit in Step 3 with a constant-depth OR reduction circuit with unbounded fan-out gates [9], where an unbounded fan-out gate can be considered as a sequence of ΛX gates with the same control qubit. Then, we decompose the unbounded fan-out gates into ΛX gates in the constant-depth OR reduction circuit. We call the resulting circuit E''_n. By the construction of E''_n, its output probability distribution is the same as that of E'_n. Thus, E''_n is not weakly simulatable. The procedure for obtaining E''_n transforms the middle part of the non-commuting OR reduction circuit in Step 3 of E'_n, which is the only part in E'_n that includes non-Clifford gates, into a quantum circuit that has ΛX gates and a depth-1 layer consisting of all the gates in the middle part. The circuit obtained in this way from the middle part in Fig. 7(a) is depicted in Fig. 7(b). Thus, E''_n is a Clifford circuit augmented by a depth-1 non-Clifford layer, which consists only of controlled phase-shift gates, and this completes the proof. □

5 Conclusions and Future Work

We showed that there exists a 5-local commuting quantum circuit with $O(\log n)$ output qubits such that it is not weakly simulatable unless $\mathsf{PH} = \Delta_3^p$. This is the first formal evidence that a commuting quantum circuit is not weakly simulatable even when the number of output qubits is $O(\log n)$. Then, we clarified the condition under which a generalized version of the circuit is weakly simulatable. Lastly, we provided an evidence that a slightly extended Clifford circuit is not weakly simulatable.

We present two open problems related to commuting quantum circuits:

- Does there exist a 3- or 4-local commuting quantum circuit with $O(\log n)$ output qubits such that it is not weakly simulatable (under a plausible assumption)?
- Do the theorems in this paper hold when exponentially small error $1/2^{p(n)}$ is replaced with polynomially small error $1/p(n)$ in the definitions of the classical simulatability?

As described in Section 1, Theorem 2 suggests that our construction method of commuting quantum circuits does not work for solving the first problem affirmatively. It might be useful for solving it to find depth-3 quantum circuits that are simpler than A_n and are not weakly simulatable. Moreover, our construction method is based on the parallelization method in Ref. [6], which yields a depth-3 quantum circuit that can be related to the original circuit in the event with an exponentially small probability. To solve the second problem affirmatively, it would be necessary to avoid dealing with such exponentially small probabilities.

Finally, we mention another open problem suggested by one of the referees of this paper. In contrast to our setting where all ancillary qubits are initialized to $|0\rangle$, it would be interesting to investigate the case when the ancillary qubits are initialized in the totally depolarized state.

Acknowledgments

We thank Harumichi Nishimura and Tomoyuki Morimae for valuable suggestions on the previous version of the paper. We also thank the anonymous referees for improving the presentation. S.T. is deeply grateful to the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the MEXT in Japan) for encouraging the research presented in this paper.

References

1. Aaronson, S.: Quantum computing, postselection, and probabilistic polynomial-time. Proceedings of the Royal Society A 461, 3473–3482 (2005)
2. Aaronson, S., Arkhipov, A.: The computational complexity of linear optics. Theory of Computing 9(4), 143–252 (2013)
3. 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)
4. Clark, S., Jozsa, R., Linden, N.: Generalized Clifford groups and simulation of associated quantum circuits. Quantum Information and Computation 8(1&2), 106–126 (2008)
5. Dawson, C.M., Nielsen, M.A.: The Solovay-Kitaev algorithm. Quantum Information and Computation 6(1), 81–95 (2006)
6. 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)
7. Fujii, K., Kobayashi, H., Morimae, T., Nishimura, H., Tamate, S., Tani, S.: Impossibility of classically simulating one-clean-qubit computation (2015), arXiv:1409.6777v2
8. Han, Y., Hemaspaandra, L.A., Thierauf, T.: Threshold computation and cryptographic security. SIAM Journal on Computing 26(1), 59–78 (1997)
9. Høyer, P., Špalek, R.: Quantum fan-out is powerful. Theory of Computing 1(5), 81–103 (2005)
10. Jozsa, R., Van den Nest, M.: Classical simulation complexity of extended Clifford circuits. Quantum Information and Computation 14(7&8), 633–648 (2014)
11. Markov, I.L., Shi, Y.: Simulating quantum computation by contracting tensor networks. SIAM Journal on Computing 38(3), 963–981 (2008)
12. 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)
13. Van den Nest, M.: Simulating quantum computers with probabilistic methods. Quantum Information and Computation 11(9&10), 784–812 (2011)
14. 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)

15. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
16. Papadimitriou, C.H.: Computational Complexity. Addison Wesley (1994)
17. Shepherd, D.: Binary matroids and quantum probability distributions (2010), arXiv:1005.1744
18. Shepherd, D., Bremner, M.J.: Temporally unstructured quantum computation. Proceedings of the Royal Society A 465, 1413–1439 (2009)
19. Takahashi, Y., Yamazaki, T., Tanaka, K.: Hardness of classically simulating quantum circuits with unbounded Toffoli and fan-out gates. Quantum Information and Computation 14(13&14), 1149–1164 (2014)
20. 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)

Appendix A

A.1 Proof of Lemma 1

We first describe A_n associated with $L \in \mathsf{PostBQP}$ [6]. For any $L \in \mathsf{PostBQP}$, there exists a polynomial-size quantum circuit C_n with n input qubits, $a = O(\mathrm{poly}(n))$ ancillary qubits, one output qubit, and one postselection qubit such that, for any $x \in \{0,1\}^n$,

- $\Pr[\mathrm{post}_n(x) = 0] \geq 1/2^{q(n)}$,
- if $x \in L$, $\Pr[C_n(x) = 1 | \mathrm{post}_n(x) = 0] \geq 2/3$,
- if $x \notin L$, $\Pr[C_n(x) = 1 | \mathrm{post}_n(x) = 0] \leq 1/3$,

where q is some polynomial depending only on C_n. As shown in Ref. [6], there exists a depth-3 polynomial-size quantum circuit A_n with n input qubits, $a + b$ ancillary qubits, and one output qubit such that, for any $x \in \{0,1\}^n$,

- if $x \in L$, $\Pr[A_n(x) = 1 | \mathrm{qpost}_n(x) = 0^{b+1}] \geq 2/3$,
- if $x \notin L$, $\Pr[A_n(x) = 1 | \mathrm{qpost}_n(x) = 0^{b+1}] \leq 1/3$,

where $b = O(\mathrm{poly}(n))$, the event "$\mathrm{qpost}_n(x) = 0^{b+1}$" means that all classical outcomes of Z-measurements on the qubit corresponding to the postselection qubit of C_n and particular b qubits (other than the output qubit) are 0. We call these $b+1$ qubits the postselection qubits of A_n. Since the probability of obtaining 0^b by Z-measurements on the b qubits is $1/2^b$ [6], $\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] \geq 1/2^{b+q}$. We regard A_n as a new circuit A'_n with $b+2$ output qubits, where one of the output qubits is the original output qubit q_{out} of A_n and the others are the $b+1$ postselection qubits of A_n. Without loss of generality, we assume that the last output qubit of A'_n is q_{out}. It holds that, for any $x \in \{0,1\}^n$, $\Pr[A'_n(x) = 0^{b+1}1] = \Pr[A_n(x) = 1 \& \mathrm{qpost}_n(x) = 0^{b+1}]$ and $\Pr[A'_n(x) = 0^{b+1}0] = \Pr[A_n(x) = 0 \& \mathrm{qpost}_n(x) = 0^{b+1}]$. For simplicity, we denote A'_n hereafter as A_n, which is the desired circuit. By the construction of A_n, for any $x \in \{0,1\}^n$,

- if $x \in L$, $\Pr[A_n(x) = 0^{b+1}1] \geq 2 \cdot \Pr[\mathrm{qpost}_n(x) = 0^{b+1}]/3$,
- if $x \notin L$, $\Pr[A_n(x) = 0^{b+1}1] \leq \Pr[\mathrm{qpost}_n(x) = 0^{b+1}]/3$.

We assume that $\mathsf{PH} \neq \Delta_3^p$. This implies the existence of $L \in \mathsf{PostBQP} \setminus \mathsf{PostBPP}$ as described in Section 2. We can construct A_n associated with this L as described above. We show that, if A_n is weakly simulatable, then $L \in \mathsf{PostBPP}$. This completes the proof since $L \notin \mathsf{PostBPP}$. The assumption that A_n is weakly simulatable implies that there exists a polynomial-size randomized classical circuit R_n such that, for any $x \in \{0,1\}^n$ and $y \in \{0,1\}^{b+2}$, $|\Pr[R_n(x) = y] - \Pr[A_n(x) = y]| \leq 1/2^{b+q+10}$. In particular, $\Pr[A_n(x) = 0^{b+1}1]$ and $\Pr[A_n(x) = 0^{b+1}0]$ can be approximated by $\Pr[R_n(x) = 0^{b+1}1]$ and $\Pr[R_n(x) = 0^{b+1}0]$, respectively, up to an additive error of $1/2^{b+q+10}$. Thus, $\Pr[\mathrm{qpost}_n(x) = 0^{b+1}]$, which is equal to $\Pr[A_n(x) = 0^{b+1}1] + \Pr[A_n(x) = 0^{b+1}0]$, can be approximated by $\Pr[R_n(x) = 0^{b+1}1] + \Pr[R_n(x) = 0^{b+1}0]$ up to an additive error of $1/2^{b+q+9}$.

We construct a polynomial-size randomized classical circuit S_n that implements the following classical algorithm with input $x \in \{0,1\}^n$:

1. Compute $R_n(x)$.

2. (a) If $R_n(x) = 0^{b+1}1$, set $\mathrm{post}_n(x) = 0$ and $S_n(x) = 1$.
   (b) If $R_n(x) = 0^{b+1}0$, set $\mathrm{post}_n(x) = 0$ and $S_n(x) = 0$.
   (c) Otherwise, set $\mathrm{post}_n(x) = 1$ and $S_n(x) = 1$.

By the definition of S_n, $\Pr[\mathrm{post}_n(x) = 0] = \Pr[R_n(x) = 0^{b+1}1] + \Pr[R_n(x) = 0^{b+1}0]$, which can be approximated by $\Pr[\mathrm{qpost}_n(x) = 0^{b+1}]$ up to an additive error of $1/2^{b+q+9}$. Since $\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] \geq 1/2^{b+q}$, $\Pr[\mathrm{post}_n(x) = 0] > 0$. Moreover, by the definition of S_n,

$$\Pr[S_n(x) = 1 | \mathrm{post}_n(x) = 0] = \frac{\Pr[R_n(x) = 0^{b+1}1]}{\Pr[R_n(x) = 0^{b+1}1] + \Pr[R_n(x) = 0^{b+1}0]}.$$

If $x \in L$, $\Pr[S_n(x) = 1 | \mathrm{post}_n(x) = 0]$ is lower bounded by

$$\begin{aligned}\frac{\Pr[A_n(x) = 0^{b+1}1] - \frac{1}{2^{b+q+10}}}{\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] + \frac{1}{2^{b+q+9}}} &\geq \frac{\frac{2}{3} \cdot \Pr[\mathrm{qpost}_n(x) = 0^{b+1}] - \frac{1}{2^{b+q+10}}}{\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] + \frac{1}{2^{b+q+9}}} \\ &= \frac{2}{3} - \frac{7\varepsilon}{3(1+2\varepsilon)} > \frac{2}{3} - \frac{7}{3}\varepsilon > \frac{3}{5},\end{aligned}$$

where $\varepsilon = 1/(2^{b+q+10} \cdot \Pr[\mathrm{qpost}_n(x) = 0^{b+1}])$ and it holds that

$$0 < \varepsilon \leq \frac{1}{2^{b+q+10} \cdot \frac{1}{2^{b+q}}} = \frac{1}{2^{10}}.$$

If $x \notin L$, $\Pr[S_n(x) = 1 | \mathrm{post}_n(x) = 0]$ is upper bounded by

$$\frac{\Pr[A_n(x) = 0^{b+1}1] + \frac{1}{2^{b+q+10}}}{\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] - \frac{1}{2^{b+q+9}}} \leq \frac{\frac{1}{3} \cdot \Pr[\mathrm{qpost}_n(x) = 0^{b+1}] + \frac{1}{2^{b+q+10}}}{\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] - \frac{1}{2^{b+q+9}}} = \frac{1}{3} + \frac{5\varepsilon}{3(1-2\varepsilon)} < \frac{2}{5}.$$

The constants $2/3$ and $1/3$ in the definition of $\mathsf{PostBPP}$ can be replaced with $1/2 + \delta$ and $1/2 - \delta$, respectively, for any constant $0 < \delta < 1/2$ [3]. Thus, $L \in \mathsf{PostBPP}$. □

A.2 Proof of Theorem 2

Let $|x\rangle$ be an n-qubit input state, where $x \in \{0,1\}^n$. Moreover, let

$$F_n|x\rangle|0^s\rangle = \sum_{z\in\{0,1\}^t} \alpha_{x,z}|\psi_{x,z}\rangle|z\rangle,$$

where $\alpha_{x,z} \in \mathbf{C}$ and $|\psi_{x,z}\rangle$ is an $(n+s-t)$-qubit state. Then,

$$\begin{aligned}(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})|x\rangle|0^{s+l}\rangle &= \frac{1}{\sqrt{2^l}}(F_n^\dagger \otimes H^{\otimes l}) \sum_{z\in\{0,1\}^t, w\in\{0,1\}^l} \alpha_{x,z}|\psi_{x,z}\rangle \otimes (D|z\rangle|w\rangle) \\ &= \frac{1}{\sqrt{2^l}}(F_n^\dagger \otimes H^{\otimes l}) \sum_{z\in\{0,1\}^t, w\in\{0,1\}^l} \alpha_{x,z}e^{if(z,w)}|\psi_{x,z}\rangle|z\rangle|w\rangle.\end{aligned}$$

Thus, for any $y \in \{0,1\}^l$, $\Pr[(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})(x) = y]$ is computed as

$$\sum_{z\in\{0,1\}^t} |\alpha_{x,z}|^2 \cdot \frac{1}{2^l} \sum_{w,w'\in\{0,1\}^l} e^{-if(z,w')+if(z,w)}\langle w'|H^{\otimes l}|y\rangle\langle y|H^{\otimes l}|w\rangle.$$

As described in Section 3.2, the probability in Step 2 of our classical algorithm is

$$\frac{1}{2^l} \sum_{w,w'\in\{0,1\}^l} e^{-if(z_0,w')+if(z_0,w)}\langle w'|H^{\otimes l}|y\rangle\langle y|H^{\otimes l}|w\rangle$$

and we can compute the probability up to an exponentially small additive error using a polynomial-size classical circuit. In the following, for simplicity, we assume that we can compute the probability exactly. Then, for any $y \in \{0,1\}^l$, $\Pr[T_n(x) = y]$ is

$$\sum_{z_0\in\{0,1\}^t} \Pr[R_n(x) = z_0] \cdot \frac{1}{2^l} \sum_{w,w'\in\{0,1\}^l} e^{-if(z_0,w')+if(z_0,w)}\langle w'|H^{\otimes l}|y\rangle\langle y|H^{\otimes l}|w\rangle.$$

This implies that, for any $x \in \{0,1\}^n$ and $y \in \{0,1\}^l$,

$$\begin{aligned}|\Pr[T_n(x) = y] - \Pr[(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})(x) = y]| &\le \sum_{z_0\in\{0,1\}^t} |\Pr[R_n(x) = z_0] - |\alpha_{x,z_0}|^2| \\ = \sum_{z_0\in\{0,1\}^t} |\Pr[R_n(x) = z_0] - \Pr[F_n(x) = z_0]| &\le \frac{2^t}{2^{p(n)+t}} = \frac{1}{2^{p(n)}}.\end{aligned}$$

A similar argument works when we compute the probability in Step 2 up to an exponentially small additive error. Thus, $(F_n^\dagger \otimes H^{\otimes l})D(F_n \otimes H^{\otimes l})$ is weakly simulatable. □

A.3 Proof of Lemma 4

We describe Q_n associated with $L \in \mathsf{PostBQP}$ [10]. For any $L \in \mathsf{PostBQP}$, as in the proof of Lemma 1, there exists a polynomial-size quantum circuit C_n with n input qubits, $a = O(\mathrm{poly}(n))$ ancillary qubits (initialized to $|0\rangle$), one output qubit, and one postselection qubit. As shown in Ref. [10], there exists a Clifford circuit Q_n with n input qubits, a ancillary qubits (initialized to $|0\rangle$), $b = O(\mathrm{poly}(n))$ ancillary qubits in a product state $|\varphi\rangle^{\otimes b}$, and one output qubit such that, for any $x \in \{0,1\}^n$,

- if $x \in L$, $\Pr[Q_n(x) = 1 | \mathrm{qpost}_n(x) = 0^{b+1}] \geq 2/3$,
- if $x \notin L$, $\Pr[Q_n(x) = 1 | \mathrm{qpost}_n(x) = 0^{b+1}] \leq 1/3$,

where $|\varphi\rangle = R(\pi/4)H|0\rangle = (|0\rangle + e^{i\pi/4}|1\rangle)/\sqrt{2}$. The event "$\mathrm{qpost}_n(x) = 0^{b+1}$" means that all classical outcomes of Z-measurements on the qubit corresponding to the postselection qubit of C_n and particular b qubits (other than the output qubit) are 0. We call these $b+1$ qubits the postselection qubits of Q_n. Since we can show that the probability of obtaining 0^b by Z-measurements on the b qubits is $1/2^b$, it holds that $\Pr[\mathrm{qpost}_n(x) = 0^{b+1}] \geq 1/2^{b+q}$. We regard Q_n as a new circuit Q'_n with $b+2$ output qubits, where one of the output qubits is the original output qubit q_{out} of Q_n and the others are the $b+1$ postselection qubits of Q_n. Without loss of generality, we assume that the last output qubit of Q'_n is q_{out}. For simplicity, we denote Q'_n as Q_n, which is the desired circuit. We assume that $\mathsf{PH} \neq \Delta_3^p$. This yields $L \in \mathsf{PostBQP} \setminus \mathsf{PostBPP}$ and thus Q_n. As in the proof of Lemma 1, we can show that, if Q_n is weakly simulatable, then $L \in \mathsf{PostBPP}$. This completes the proof since $L \notin \mathsf{PostBPP}$. □