Space-Bounded Unitary Quantum Computation with Postselection

Seiichiro Tani
NTT Communication Science Laboratories, NTT Corporation, Japan
International Research Frontiers Initiative (IRFI), Tokyo Institute of Technology, Japan

Abstract

Space-bounded computation has been a central topic in classical and quantum complexity theory. In the quantum case, every elementary gate must be unitary. This restriction makes it unclear whether the power of space-bounded computation changes by allowing intermediate measurement. In the bounded error case, Fefferman and Remscrim [STOC 2021, pp.1343–1356] and Girish, Raz and Zhan [ICALP 2021, pp.73:1–73:20] recently provided the break-through results that the power does not change. This paper shows that a similar result holds for space-bounded quantum computation with *postselection*. Namely, it is proved possible to eliminate intermediate postselections and measurements in the space-bounded quantum computation in the bounded-error setting. Our result strengthens the recent result by Le Gall, Nishimura and Yakaryilmaz [TQC 2021, pp.10:1–10:17] that logarithmic-space bounded-error quantum computation with *intermediate* postselections and measurements is equivalent in computational power to logarithmic-space unbounded-error probabilistic computation. As an application, it is shown that bounded-error space-bounded one-clean qubit computation (DQC1) with postselection is equivalent in computational power to unbounded-error space-bounded probabilistic computation, and the computational supremacy of the bounded-error space-bounded DQC1 is interpreted in complexity-theoretic terms.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases quantum complexity theory, space-bounded computation, postselection

Digital Object Identifier 10.4230/LIPIcs.MFCS.2022.81

Related Version *Full Version*: `https://arxiv.org/abs/2206.15122`

Funding This work was partially supported by JSPS KAKENHI Grant Number JP20H05966 and JP22H00522.

Acknowledgements I am grateful to anonymous referees of MFCS 2022 for their valuable comments.

1 Introduction

1.1 Background

Space-bounded computation is one of the most fundamental topics in complexity theory that have been studied in the classical and quantum settings, since it reflects common practical situations where available memory space is much less than input size. Watrous [25, 26] initiated the study of space-bounded quantum computation based on quantum Turing machines and proved that, in the unbounded-error setting, space-bounded quantum computation is equivalent in computational power to space-bounded probabilistic computation: $\mathsf{PrQSPACE}(s) = \mathsf{PrSPACE}(s)$ for any space-constructible s with $s(n) \in \Omega(\log n)$. This and the classical results [5, 13] imply that unbounded-error space-bounded quantum computation can be simulated by deterministic computation with the squared amount of the space used by the former model.

There are some subtleties (see [16] for the details) in considering space-bounded quantum computation. The most relevant one is whether we allow intermediate measurements, that is, the measurements made during computation, which are allowed in, e.g., [25, 26, 24]. In

47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022).
Editors: Stefan Szeider, Robert Ganian, and Alexandra Silva; Article No. 81; pp. 81:1–81:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the case of polynomial-time quantum computation, it is well-known that all intermediate measurements can be deferred to the end of computation by coherently copying the state of the qubits to be measured to ancilla qubits, and keeping their contents unchanged through the computation. This may require a polynomial number of ancilla qubits to store the copies, since there may exist a polynomial number of intermediate measurements in the original computation. This is acceptable in the polynomial-time quantum computation. However, this method is not applicable in general in the case of space-bounded quantum computation. For instance, if we consider a logarithmic-space quantum computation that runs in polynomial time, the above transformation may require a polynomial number of ancilla qubits, much more than the available space. Thus, it is a fundamental question in space-bounded quantum computation whether it is possible to space-efficiently eliminate intermediate measurements. Recently, Fefferman and Remscrim [7] and Girish, Raz and Zhan [12] independently provided the breakthrough results that it is possible in the bounded error setting.

Postselection is a fictitious function that projects a quantum state on a single qubit to the prespecified state (say, $|1\rangle$) with certainty, as far as the former state has a non-zero overlap with the latter. Since Aaronson [1] introduced postselection to the quantum complexity theory field, it has turned out to be very effective concept in the field although it is unrealistic. In particular, Aaronson succeeded in characterizing a classical complexity class in a quantum way by introducing postselection: $\mathsf{PP} = \mathsf{PostBQP}$ [1]. This characterization gives one-line proofs of the classical results [4, 8], for which only involved classical proofs had been known, and has been a foundation for establishing the quantum computational supremacy of subuniversal quantum computation models (e.g., [6, 2, 17]) under complexity-theoretic assumptions. Another example of characterizing classical complexity classes with postselection is that PSPACE is equal to $\mathsf{PostQMA}$ [19], the class of languages that can be recognized by quantum Merlin-Arthur proof systems with polynomial-time quantum verifier with the ability of postselection. Along this line of work, Le Gall et al. [11] recently considered logarithmic-space quantum computation with postselection in the bounded-error setting and proved that its associated complexity class $\mathsf{PostBQL}$ is equivalent to PL, the class of languages that can be recognized with unbounded error by logarithmic-space probabilistic computation. This beautiful result can be regarded as the equivalent of $\mathsf{PP} = \mathsf{PostBQP}$ in the logarithmic-space quantum computation. Their model allows intermediate postselections as well as intermediate measurements, which play a key role for space-efficiency since the qubits on which intermediate postselections or measurements are made can be reused as initialized ancilla qubits for subsequent computation. Thus, a straightforward question is whether it is possible to space-efficiently eliminate intermediate postselections and measurements. Our main result answers this question affirmatively.

1.2 Our Contribution

We consider the space-bounded quantum computation that allows postselections and measurements only at the end of computation, which we call space-bounded *unitary* quantum computation with postselection. Our result informally says that such quantum computation is equivalent in computational power to the space-bounded quantum computation that allows intermediate postselections and measurements. More concretely, for a space-constructible function s with $s(n) \in \Omega(\log n)$, let $\mathsf{PostBQSPACE}(s)$ be the class of languages that can be recognized with bounded-error by quantum computation with (intermediate) postselections and measurements that uses $O(s)$ qubits and runs in $2^{O(s)}$ time, and let $\mathsf{PostBQuSPACE}(s)$ be the unitary version of $\mathsf{PostBQSPACE}(s)$. By the definition, it holds $\mathsf{PostBQuSPACE}(s) \subseteq \mathsf{PostBQSPACE}(s)$. We show the converse is also true.

▶ **Theorem 1.** *For any space-constructible function s with $s(n) \in \Omega(\log n)$, it holds that*

$$\mathsf{PostBQuSPACE}(s) = \mathsf{PostBQSPACE}(s) = \mathsf{PrSPACE}(s).$$

This strengthens the result of $\mathsf{PostBQSPACE}(s) = \mathsf{PrSPACE}(s)$, which can be derived straightforwardly from the proof of $\mathsf{PostBQL} = \mathsf{PL}$ in [11, 21]. A special case of Theorem 1 with $s = \log n$ is the following corollary, where we define $\mathsf{PostBQL} \equiv \mathsf{PostBQSPACE}(\log)$ and $\mathsf{PostBQuL} \equiv \mathsf{PostBQuSPACE}(\log)$.

▶ **Corollary 2.** $\mathsf{PostBQuL} = \mathsf{PostBQL} = \mathsf{PL}$.

Theorem 1 holds even when the completeness and soundness errors are $2^{-2^{O(s)}}$ (see Theorem 10 for a more precise statement). This justifies defining the bounded-error class $\mathsf{PostBQuSPACE}$ (note that it is non-trivial to reduce errors in the space-bounded unitary computation).

As an application, we characterize the power of space-bounded computation with postselection on a quantum model that is inherently unitary. The deterministic quantum computation with one quantum bit (DQC1)[15], often mentioned as the one-clean-qubit model, is one of well-studied quantum computation models with limited computational resources (e.g., [3, 23, 17, 9, 18, 10]). This model was originally motivated by nuclear magnetic resonance (NMR) quantum information processing, where it is difficult to initialize qubits to a pure state. In the DQC1 model, the initial state is thus the completely mixed state except for a single qubit, i.e., $|0\rangle\langle 0| \otimes (\mathrm{I}/2)^{\otimes m}$, if the total number of qubits is $m+1$. This model is inherently unitary, since if intermediate measurements or postselections were allowed, the completely mixed state could be projected to the all-zero state $|0^m\rangle$ and thus the DQC1 model would become the ordinary quantum computation model, which is supplied with the all-zero state as the initial state.

Although DQC1 is considered very weak, a polynomial-size DQC1 circuit followed by postselection is surprisingly powerful: The corresponding bounded-error class $\mathsf{PostBQ_{[1]}P}$ is equal to $\mathsf{PostBQP}$ ($= \mathsf{PP}$) [17, 10]. Although this class is unrealistic, it plays an essential role in giving a strong evidence of computational supremacy of the DQC1 computation over classical computation: If any polynomial-size DQC1 circuit is classically simulatable in polynomial time, then the polynomial hierarchy (PH) collapses [17, 10].

Let us consider the space-bounded version of $\mathsf{PostBQ_{[1]}P}$. For a space-constructible function s with $s(n) \in \Omega(\log n)$, let $\mathsf{PostBQ_{[1]}SPACE}(s)$ be the class of languages that can be recognized with bounded-error by DQC1 computation with postselection that uses $O(s)$ qubits and runs in $2^{O(s)}$ time, where all postselections and measurements are made at the the end of computation.

▶ **Theorem 3.** *For any space-constructible function s with $s(n) \in \Omega(\log n)$, it holds that*

$$\mathsf{PostBQ_{[1]}SPACE}(s) = \mathsf{PostBQuSPACE}(s) = \mathsf{PrSPACE}(s).$$

In particular, $\mathsf{PostBQ_{[1]}L} = \mathsf{PostBQuL} = \mathsf{PL}$.

This result relates quantum computational supremacy of space-bounded DQC1 computation with complexity theory as in the time-bounded case. Namely, if any s-space DQC1 computation can be classically simulated with space bound s, then it must hold that $\mathsf{PrSPACE}(s) \subseteq \mathsf{PostBSPACE}(s)$ by Theorem 3, where $\mathsf{PostBSPACE}(s)$ is the classical counterpart of $\mathsf{PostBQuSPACE}(s)$. This relation is the space-bounded equivalent of $\mathsf{PP} \subseteq \mathsf{PostBPP}$. Note that $\mathsf{PP} \subseteq \mathsf{PostBPP}$ leads to the collapse of PH [6], since $\mathsf{PostBPP}$ is in the third level of PH. However, it is open whether $\mathsf{PrSPACE}(s) \subseteq \mathsf{PostBSPACE}(s)$ implies implausible consequences.

1.3 Technical Outline

Since space-bounded quantum computation with postselection can trivially simulate the unitary counterpart by the definition, our main technical contribution is to show that the unitary counterpart can simulate unbounded-error probabilistic computation. Our starting point is the simulation of unbounded-error probabilistic computation by the space-bounded quantum computation with postselection [11]. The simulation [11] consists of two components: the first one, Q_x, simulates the unbounded-error probabilistic computation with acceptance probability p_a on input x to output the state (up to a normalizing factor) $|\Psi_\delta\rangle = (1/2 + p_a)|0\rangle + \delta(1/2 - p_a)|1\rangle$ for a given positive parameter δ; the second one decides whether $p_a > 1/2$ or $p_a < 1/2$ with bounded error by repeatedly running Q_x to prepare the states $|\Psi_\delta\rangle$ for various values of δ and measuring them in the basis $\{|+\rangle, |-\rangle\}$ (based on a modification of the idea [1]). We eliminate the intermediate postselection in Q_x space-efficiently by, every time postselection is made in Q_x, incrementing a counter coherently if the postselection qubit is in the non-postselecting state. It is not difficult to see that this works since Q_x includes only intermediate postselections (and does not include intermediate measurements). This gives a unitary version V_x of Q_x. However, the second component includes both intermediate postselections and measurements, and needs run Q_x sequentially (because running Q_x in parallel is not space-efficient). We then construct two subroutines U_+ and U_-, which accumulate the amplitudes of $|+\rangle$ and $|-\rangle$, respectively, in the states obtained by repeatedly running V_x for various values of δ, as the amplitude of the all-zero state. Finally, we run U_+ and U_- in orthogonal spaces, respectively, followed by postselecting the all-zero state on the qubits that U_+ and U_- act on. The resulting state is significantly supported by one of the spaces, which determines whether $p_a > 1/2$ or $p_a < 1/2$ with high probability.

1.4 Organization

Sec. 2 introduces definitions, basic claims and known theorems. Sec. 3 provides the formal statement of our main result and proves it by using a lemma, which is proved in Sec. 4. Sec. 5 provides an application of the result.

2 Prelimiaries

Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ be the sets of natural numbers, integers, and real numbers, respectively. For $m \in \mathbb{N}$, let $[m]$ be the set of $\{1, \ldots, m\}$. Assume that Σ is the set $\{0, 1\}$. A *promise problem* $L = (L_Y, L_N)$ is a pair of disjoint subsets of Σ^*. In the special case of promise problems such that $L_Y \cup L_N = \Sigma^*$, we say that L_Y is a *language*.

Classical Space-Bounded Computation

We say that a function $s : \mathbb{N} \to \mathbb{N}$ is *space-constructible* if there exists a deterministic Turing machine (DTM) that compute $s(|x|)$ in space $O(s(|x|))$ on input x. Suppose that s is a space constructible function. Then, we say that a function $f : \mathbb{N} \to \mathbb{R}$ is *s-space computable* if there exists a DTM that computes $f(|x|)$ in space $O(s(|x|))$ on input x. For $s \in \Omega(\log n)$, $\mathsf{PrSPACE}(s)$ is the class of promise problems L such that there exists a probabilistic Turing machine (PTM) M running with space $O(s)$ that satisfies the following: For every input $x \in L_Y$, the probability that M accepts x is greater than 1/2, and for every input $x \in L_N$, the probability that M accepts x is at most 1/2. We can replace the condition in the case of $x \in L_N$ with "the probability that M accepts x is *less* than 1/2" without changing the class $\mathsf{PrSPACE}\,(s)$. In this paper, we adopt the latter definition. It is known that the class $\mathsf{PrSPACE}(s)$ does not change even if we impose the time bound $2^{O(s)}$ on the corresponding PTM with space bound s [13] (see also [22]). We define $\mathsf{PL} \equiv \mathsf{PrSPACE}\,(\log)$.

Quantum Circuits

We below introduce just notations and terminologies relevant to this paper. For the basics of quantum computing, see standard textbooks (e.g., [20, 14]). Let $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

A *quantum gate* implements a unitary operator. We say that a quantum gate is *elementary* if it acts on a constant number of qubits. We may use a quantum gate and its unitary operator that the gate implements interchangeably. Examples of elementary gates are $\mathrm{H} \equiv |+\rangle\langle 0|+|-\rangle\langle 1|$, $\mathrm{X} \equiv |0\rangle\langle 1|+|1\rangle\langle 0|$, $\mathrm{T} \equiv |0\rangle\langle 0|+e^{i\pi/4}|1\rangle\langle 1|$, and $\mathrm{CNOT} \equiv |0\rangle\langle 0|\otimes \mathrm{I}+|1\rangle\langle 1|\otimes \mathrm{X}$. For unitary gate g, $\wedge_k(g)$ denotes the unitary gate acting on $k+1$ qubits such that it applies g to the last qubit if the contents of the first k qubits are all 1, and it applies the identity otherwise. We may simply say that $\wedge_k(g)$ is a *k-qubit-controlled* g. In the case of $k=1$, we may use $\wedge(g)$ to denote $\wedge_1(g)$. For instance, $\wedge_2(\mathrm{X})$ is the Toffoli gate and $\wedge(\mathrm{X})$ is the CNOT gate. We also define $\vee_k(g)$ as the unitary gate acting on $k+1$ qubits such that it applies g to the last qubit if the contents of the first k qubits are not all-zero, and it applies the identity otherwise. Gate set G is defined as $G_1 \cup G_2 \cup G_3$ for $G_1 \equiv \{\mathrm{H}, \mathrm{T}, \mathrm{CNOT}\}$, the set G_2 of a constant number of additional elementary gates used for block encoding in [11], and the set G_3 of $\wedge(g)$ for all $g \in G_1 \cup G_2$. This choice of gates is not essential for our results when completeness and soundness errors are allowed to be $2^{-O(s)}$ for space bound s, because of space-efficient version of Solovay-Kitaev theorem (see [16, Theorem 4.3]), which says that it is possible to ϵ-approximate every unitary gate with a sequence of gates in any fixed gate set that is finite and universal in $O(\mathrm{polylog}\,(1/\epsilon))$ deterministic time and $O(\log\,(1/\epsilon))$ deterministic space.

For simple descriptions, we will also use k-qubit-controlled gates $\wedge_k\,(g)$ for $g \in G_1 \cup G_2$ and $k \geq 2$ in the following section, since $\wedge_k\,(g)$ can be implemented with gate set G together with $O(1)$ reusable ancilla qubits with negligible gate overhead:

▷ Claim 4. For every gate g, $\wedge_k(g)$ can be implemented with $\wedge(g)$, and $O(k)$ CNOT and T gates together with $O(1)$ ancilla qubits initialized to $|0\rangle$. Similarly, $\vee_k(g)$ can be implemented with $\wedge(g)$, and $O(k)$ CNOT, T and X gates together with $O(1)$ ancilla qubits initialized to $|0\rangle$. Moreover, the states of the ancilla qubits return to $|0\rangle$ after applying $\wedge_k(g)$ $(\vee_k(g))$.

Since the overhead of $O(k)$ gates can be ignored in our setting of $O(s)$ space and $2^{O(s)}$ time computation, we can effectively use $\wedge_k(g)$ freely. The proofs of Claim 4 and the following Claim 5 are provided in the full version.

Next, we define a special gate that will be used many time in this paper. Let INC_{2^n} be the unitary gate acting on n qubits that transforms $\mathrm{INC}_{2^n} : |j\rangle \mapsto |(j+1) \mod 2^n\rangle$ for all $j \in \{0, \ldots, 2^n - 1\}$. Intuitively, INC_{2^n} increments a counter over $\mathbb{Z}_{2^n}$.

▷ Claim 5. $\wedge_k(\mathrm{INC}_{2^n})$ can be implemented with $O(k+n^2)$ CNOT and T gates with the help of $O(1)$ ancilla qubits initialized to $|0\rangle$. Similarly, $\vee_k(\mathrm{INC}_{2^n})$ can be implemented with $O(k+n^2)$ CNOT, T, and X gates with the help of $O(1)$ ancilla qubits initialized to $|0\rangle$. The states of the ancilla qubits return to $|0\rangle$ after applying $\wedge_k(\mathrm{INC}_{2^n})$ $(\vee_k(\mathrm{INC}_{2^n}))$.

Since the overhead of $O(k+n^2)$ gates with $n, k \in O(s)$ can be ignored in our setting of $O(s)$ space and $2^{O(s)}$ time computation, we can effectively use $\wedge_k(\mathrm{INC}_{2^n})$ freely.

A *quantum circuit* consists of quantum gates in a fixed universal set of a constant number of unitary gates, and (intermediate) measurements. A *quantum circuit with postselection* is a quantum circuit with the ability of postselection even at intermediate points in the circuit. Here, the *postselection* [1] is a fictitious function that projects a quantum state on a single qubit to the state $|1\rangle$ with certainty, as far as there exists a non-zero overlap between the state and $|1\rangle$. For instance, if we make postselection on the first qubit of quantum state $\alpha|0\rangle|\psi_0\rangle + \beta|1\rangle|\psi_1\rangle$ with $\beta \neq 0$, resulting state is $|1\rangle|\psi_1\rangle$. Since the qubit on which postselection has been made is in the state $|1\rangle$ by the definition, we can reuse them as initialized qubits for subsequent computation. This can greatly save the space (i.e., the number of ancilla qubits) as in the case of intermediate measurements. We say that $|1\rangle$ is the postselecting state, and the state orthogonal to the postselecting state, $|0\rangle$, is the non-postselecting state. To simplify descriptions, we may say "postselect $|\phi\rangle$" to mean that we first apply a single-qubit unitary U such that $|1\rangle = U|\phi\rangle$ and then postselect $|1\rangle$. We may also say "postselect $|\phi_1\rangle \otimes \cdots \otimes |\phi_m\rangle$," where $|\phi_i\rangle$ is a single-qubit pure state for every i, to mean postselecting $|\phi_i\rangle$ on the ith qubit for each $i = 1, \ldots, m$. For instance, we may say "postselecting the all-zero state" (i.e., postselecting $|0^m\rangle$). A *unitary quantum circuit* consists of only (unitary) quantum gates and does not include any measurement or postselection. To perform computational tasks, a unitary quantum circuit will be followed by measurements (and postselections).

We say that, for a promise problem L, a family of quantum circuits $\{Q_x : x \in L\}$ with postselections (a family of unitary quantum circuits $\{U_x : x \in L\}$) is *s-space uniform* if there exists a DTM that, on input $x \in L$, outputs a description of Q_x (U_x, respectively) with the use of space $O(s(|x|))$ (and hence in $2^{O(s(|x|))}$ time).

Let $s\colon \mathbb{N} \to \mathbb{N}$ be a space-constructible function with $s(n) = \Omega(\log n)$. Assume that functions $c, d\colon \mathbb{N} \to [0,1]$ are s-space computable, and $c(n) > d(n)$ for sufficiently large $n \in \mathbb{N}$.

▶ **Definition 6** (PostQSPACE). *Let* PostQSPACE$(s)[c,d]$ *be the class of promise problems* $L = (L_Y, L_N)$ *for which there exists an s-space uniform family of quantum circuits with postselection,* $\{Q_x : x \in L\}$*, that act on* $m = O(s(|x|))$ *qubits and consist of* $2^{O(s(|x|))}$ *elementary gates such that, when applying* Q_x *to* $|0\rangle^{\otimes m}$*, (1) the probability* p_{post} *of measuring* $|1\rangle$ *on every postselection qubit is strictly positive; (2) for* $x \in L_Y$*, conditioned on all the postselection qubits being* $|1\rangle$*, the probability that* Q_x *accepts is at least* $c(|x|)$*; (3) for* $x \in L_N$*, conditioned on all the postselection qubits being* $|1\rangle$*, the probability that* Q_x *accepts is at most* $d(|x|)$*.*

▶ **Definition 7** (PostQuSPACE). *Let* PostQuSPACE$(s)[c.d]$ *be the class of promise problems* $L = (L_Y, L_N)$ *for which there exists an s-space uniform family of unitary quantum circuits,* $\{U_x\colon x \in L\}$*, that act on* $m \in O(s(|x|))$ *qubits and consist of* $2^{O(s(|x|))}$ *elementary gates, followed by postselection on the first qubit and measurement on the output qubit (say, the second qubit) in the computational basis, such that, when applying* U_x *to* $|0\rangle^{\otimes m}$*, (1) the probability* p_{post} *of measuring* $|1\rangle$ *on the first qubits is strictly positive; (2) for* $x \in L_Y$*, conditioned on the first qubit being* $|1\rangle$*, the probability that* U_x *accepts is at least* $c(|x|)$*; (3) for* $x \in L_N$*, conditioned on the first qubit being* $|1\rangle$*, the probability that* U_x *accepts is at most* $d(|x|)$*.*

Definition 7 assumes that postselection is made only on a single qubit. This is general enough since, if there are k postselection qubits, then we can aggregate them into a single postselection qubit by using $\wedge_k(\mathrm{X})$ and $O(1)$ ancilla qubits. Obviously, this aggregation does not change p_{post} and the acceptance probability.

Define $\mathsf{PostBQSPACE}(s) \equiv \mathsf{PostQSPACE}(s)[2/3, 1/3]$ and $\mathsf{PostBQL} \equiv \mathsf{PostBQSPACE}(\log)$. Similarly, define $\mathsf{PostBQuSPACE}(s) \equiv \mathsf{PostQuSPACE}(s)[2/3, 1/3]$ and $\mathsf{PostBQuL} \equiv \mathsf{PostBQuSPACE}(\log)$. Le Gall, Nishimura and Yakaryilmaz [11] proved the following.

▶ **Theorem 8** ([11])**.** $\mathsf{PostBQL} = \mathsf{PL}$.

Moreover, it is straightforward to extend the result to the general space bound.

▶ **Theorem 9** ([11])**.** *For any space-constructible function $s\colon \mathbb{N} \to \mathbb{N}$ with $s(n) \in \Omega(\log n)$, it holds that* $\mathsf{PrSPACE}(s) = \mathsf{PostQSPACE}(s)[1 - 2^{-2^{O(s)}}, 2^{-2^{O(s)}}] = \mathsf{PostBQSPACE}(s)$.

In [11], PostBQL is defined based on the space-bounded quantum Turing machine (QTM), following the definition provided in [26]. It is not difficult to see that their proof works for the circuit-based definition. Consequently, the QTM-based definition and the circuit-based definition are equivalent in computational power.

3 Main Results

Theorem 10 provides a formal statement of our main result, which shows that the class of promise problems that can be solved with an s-space uniform family of *unitary* quantum circuits with postselection by using $O(s)$ space and $2^{O(s)}$ time in the *bounded-error* setting is equal to the class of promise problems by *unbounded-error* probabilistic computation with space bound s.

▶ **Theorem 10.** *For any space-constructible function $s : \mathbb{N} \to \mathbb{N}$ with $s(n) = \Omega(\log n)$,*

$$\mathsf{PrSPACE}(s) = \mathsf{PostQuSPACE}(s)\left[1 - 2^{-2^{O(s)}}, 2^{-2^{O(s)}}\right] = \mathsf{PostBQuSPACE}(s).$$

In particular, $\mathsf{PostBQuL} = \mathsf{PL}$.

Theorems 9 and 10 imply that intermediate postselections and measurements add no extra computational power, as stated formally in the following corollary.

▶ **Corollary 11** (Restatement of Theorem 1)**.** *For any space-constructible function $s : \mathbb{N} \to \mathbb{N}$ with $s(n) = \Omega(\log n)$,*

$$\mathsf{PostBQuSPACE}(s) = \mathsf{PostBQSPACE}(s) = \mathsf{PrSPACE}(s).$$

In particular, $\mathsf{PostBQL} = \mathsf{PostBQuL}$.

Proof of Theorem 10. By the definition, we have $\mathsf{PostQuSPACE}(s)\left[1 - 2^{-2^{O(s)}}, 2^{-2^{O(s)}}\right] \subseteq \mathsf{PostBQuSPACE}(s)$. Then, the theorem follows from Lemmas 12 and 13, stated as follows. ◀

▶ **Lemma 12.** *For any space-constructible function $s : \mathbb{N} \to \mathbb{N}$ with $s(n) = \Omega(\log n)$,*

$$\mathsf{PostBQuSPACE}(s) \subseteq \mathsf{PrSPACE}(s).$$

Proof. By the definition, we have $\mathsf{PostBQuSPACE}(s) \subseteq \mathsf{PostBQSPACE}(s)$. Since $\mathsf{PostBQSPACE}(s) = \mathsf{PrSPACE}(s)$ by Theorem 9, the lemma follows. ◀

▶ **Lemma 13.** *For any space-constructible function $s : \mathbb{N} \to \mathbb{N}$ with $s(n) = \Omega(\log n)$,*

$$\mathsf{PrSPACE}(s) \subseteq \mathsf{PostQuSPACE}(s)\left[1 - 2^{-2^{O(s)}}, 2^{-2^{O(s)}}\right].$$

The proof is provided in the following section.

4 Proof of Lemma 13

To prove Lemma 13, we use the fact proved in [11].

▶ **Lemma 14** ([11]). *Suppose that, for any input x, a PTM with space bound $s = s(|x|)$ accepts with probability $p_a = p_a(x)$ and rejects with probability $1 - p_a$ after running in a prespecified time $T(|x|) \in 2^{O(s)}$. There exists an s-space uniform family of quantum circuits Q_x on $m + \lceil \log_2 (T+1) \rceil$ qubits for $m \in O(s)$ that consist of $2^{O(s)}$ elementary gates in the gate set G and intermediate postselections such that, for every $k \in \{0, \ldots, T\}$, it holds that*

$$Q_x|0^m\rangle|k\rangle = \frac{|\Psi_k\rangle|0^{m-1}\rangle|k\rangle}{\||\Psi_k\rangle|0^{m-1}\rangle|k\rangle\|},$$

where $|\Psi_k\rangle \equiv (1/2 + p_a)|0\rangle + 2^{T-k}(1/2 - p_a)|1\rangle$.

Let L be a promise problem in $\mathsf{PrSPACE}(s)$. Then, there exists a PTM M that recognizes L with unbounded error in space $O(s(|x|))$ on input x. By the result by Jung [13] (see also [22]), we assume without loss of generality that M runs in time $T(|x|) \in 2^{O(s(|x|))}$. Since the computation path is split into two paths in each step with equal probability, the accepting probability p_a is of the form $a/2^T$ for some integer $a \in \{0, \cdots, 2^T\} \setminus 2^{T-1}$ (assuming $p_a \neq 1/2$ without loss of generality). There exist an s-space uniform family of quantum circuits Q_x defined in Lemma 14. Note that Q_x makes intermediate postselections and thus Q_x is not unitary. Since we have assumed $p_a \neq 1/2$, we can decide whether p_a is larger or smaller than $1/2$ with unbounded error by measuring $|\Psi_T\rangle$ in the basis $\{|+\rangle, |-\rangle\}$. To distinguish the two cases with bounded error, we need to reduce error probability. For this, Le Gall et al. [11] uses essentially the same idea as is used in [1], repeating the following operations for every k: prepare $|\Psi_k\rangle$ and measure it in the basis $\{|+\rangle, |-\rangle\}$. Since the qubits on which measurements or postselections have been made can be reused by initializing them using block encoding with postselection, the space requirement is bounded by $O(s)$. Thus, intermediate postselections and measurements play a key role in space efficiency.

4.1 Base Unitary Circuit V_x

Our goal is to move every postselection and measurement down to the end of computation while increasing the space requirement by at most a constant factor.

This is not difficult for the Q_x part. The following modification can make Q_x unitary: We prepare an $N \in O(s)$ bit counter C initialized to the all-zero state $|0^N\rangle$ in a quantum register C. Here, we take a sufficiently large integer in $O(s)$ as N. Then, every time postselection is made in Q_x, we instead increment the counter C coherently if the postselection qubit is in the non-postselecting state, and perform the other operations (i.e., unitary gates) in the same way as in the original circuit Q_x. If we assume without loss of generality that non-postselecting state is $|0\rangle$, then the counter C is incremented by applying the X gate to the postselection qubit, applying $\wedge(\mathrm{INC}_{2^N})$ gate controlled by that qubit, and then applying the X gate to that qubit, namely, $(\mathrm{X} \otimes \mathrm{I})(\wedge(\mathrm{INC}_{2^N}))(\mathrm{X} \otimes \mathrm{I})$. Let V_x denote the modified circuit.

By the above construction and the standard analysis (e.g., [25]), if we measure the counter C and postselect the all-zero state after applying V_x to $|0^m\rangle|k\rangle$, the output state is $|\Psi_k\rangle|0^{m-1}\rangle|k\rangle$ up to a normalizing factor. More concretely, every time postselection is made in Q_x, the modified circuit V_x moves the non-postselecting state into the space associated with the counter value being non-zero, that is, the space orthogonal to the space where the postselecting state lies. By setting N so that the maximum counter value $2^N - 1$ is larger than the number of postselections in Q_x, it holds that, once the counter C is incremented, the counter value never returns to zero. Thus, the quantum interference between the states associated with the counter-values being zero and non-zero never occurs. This implies that, if the content of counter register C is zero, the state must be projected to the postselecting state in *every* postselection points in Q_x, and thus the entire register except C is in the state that is equal to $Q_x|0^m\rangle|k\rangle$. Thus, for certain normalized states $|bad_k(j)\rangle$ and $\ell = m + O(1) \in O(s)$, we can write

$$V_x|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|k\rangle_{\mathsf{K}} = \left[\gamma_k|\Psi_k\rangle_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0^N\rangle_{\mathsf{C}} + \sqrt{1-\|\gamma_k|\Psi_k\rangle\|^2}\sum_{j\geq 1}|bad_k(j)\rangle_{\mathsf{R}}|j\rangle_{\mathsf{C}}\right]|k\rangle_{\mathsf{K}}, \tag{1}$$

where $0 < \gamma_k < 1$, and

$$|\Psi_k\rangle \equiv (1/2 + p_a)\,|0\rangle + 2^{T-k}\,(1/2 - p_a)\,|1\rangle = \alpha_k|+\rangle + \beta_k|-\rangle, \tag{2}$$

for $\alpha_k = \langle+|\Psi_k\rangle$ and $\beta_k = \langle-|\Psi_k\rangle$. Here, register K consists of $\lceil\log_2(T+1)\rceil$ qubits and stores the argument $k \in \{0,\ldots,T\}$. The first register $\mathsf{R} \equiv (\mathsf{R}_1,\mathsf{R}_2)$ is the working register except registers C and K, where R_1 is the subregister of R corresponding to the first qubit and R_2 consists of the remaining qubits. Note that V_x uses the register C in addition to registers (R,K) of $O(s)$ qubits, and applies $\wedge(\mathrm{INC}_{2^N})$ instead of every intermediate postselection made in Q_x. Since Q_x consists of $2^{O(s)}$ unitary gates and intermediate postselections on $O(s)$ qubits, and since Claim 5 implies that $\wedge(\mathrm{INC}_{2^N})$ is implementable with $O(N^2)$ $(= O(s))$ CNOT and T gates with $O(1)$ ancilla qubits, which are reusable for other $\wedge(\mathrm{INC}_{2^N})$, it holds that V_x consists of $2^{O(s)}$ gates in G and acts on $O(s)$ qubits.

4.2 Subroutine Unitary Circuits U_+ and U_-

In the following subsections, we will describe the entire algorithm, which includes the error-reduction step. For this, we first provide two unitary subroutines U_+ and U_- in Figure 1. They use V_x and act on registers $(\mathsf{R},\mathsf{C},\mathsf{D},\mathsf{K})$, where D is an $O(s)$-qubit quantum register used as another $O(s)$-bit counter D. We assume without loss of generality that the two registers C and D consist of N qubits for sufficiently large $N \in O(s)$. The following lemmas tell us about the actions of U_+ and U_-.

▶ **Lemma 15.** *For every $k \in \{0,\ldots,T\}$, let α_k and γ_k be the coefficients appearing in Eqs. (1) and (2). Then, U_+ given in Figure 1 acts on $O(s)$ qubits, consists of $2^{O(s)}$ gates in the gate set G, and satisfies*

$$U_+|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\gamma|\alpha_T|^2\cdots|\alpha_0|^2|0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1}|\phi_T(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}}\right]|0\rangle_{\mathsf{K}}$$

for certain unnormalized quantum states $|\phi_T(j)\rangle$ on registers (R,C) for each $j \geq 1$, where $\gamma = |\gamma_T|^2\cdots|\gamma_0|^2$. Moreover, for every $r \in \mathbb{N}\cap 2^{O(s)}$, $(U_+)^r$ acts on $O(s)$ qubits, consists of $2^{O(s)}$ gates in the gate set G, and satisfies

$$(U_+)^r|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\left(\gamma|\alpha_T|^2\cdots|\alpha_0|^2\right)^r|0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1}|\phi_T^{(r)}(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}}\right]|0\rangle_{\mathsf{K}},$$

where $|\phi_T^{(r)}(j)\rangle$ is a certain unnormalized quantum state on registers (R,C) for each $j \geq 1$.

Subroutine U_+ associated with V_x

Repeat the following steps $T+1$ times.

1. Perform V_x on $(\mathsf{R},\mathsf{C},\mathsf{K})$.
2. If the content of C is non-zero or the first qubit in R is in state $|-\rangle$, then apply INC_{2^N} to register D to increment the counter D.
3. If the content of D is zero, then invert the Step1 on $(\mathsf{R},\mathsf{C},\mathsf{K})$, i.e, apply $V_x^\dagger$.
4. If the content of (R,C) is not all-zero, then apply INC_{2^N} to register D to increment the counter D.
5. Apply INC_{T+1} to register K to increment the content in register K.

Apply $\mathrm{INC}_{T+1}^\dagger$ $T+1$ times to initialize register K to the all-zero state.

Subroutine U_- associated with V_x

Same as U_+ except that Step 2 is replaced with the following operation.

2. If the content of C is non-zero or the first qubit in R is in state $|+\rangle$, then apply INC_{2^N} to register D to increment the counter D.

Figure 1 Subroutines U_+ and U_- associated with V_x.

Proof. We first give the analysis of the first repetition on registers $(\mathsf{R},\mathsf{C},\mathsf{D},\mathsf{K})$ initialized to the all-zero state. Step 1 applies V_x to $|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|k\rangle_{\mathsf{K}}$ with $k=0$. By Eq (1), the resulting state in (R,C) is

$$\gamma_k(\alpha_k|+\rangle+\beta_k|-\rangle)_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0\rangle_{\mathsf{C}}+\sqrt{1-\||\gamma_k|\Psi_k\rangle\|^2}\sum_{j\geq 1}|bad_k(j)\rangle_{\mathsf{R}}|j\rangle_{\mathsf{C}},$$

where we omit the register K for simplicity. Then, Step 2 appends register D and increments the counter D if the content of the register C is not zero or the register R_1 is in the state $|-\rangle$. Thus, the resulting state is

$$\begin{aligned}&\mapsto \gamma_k\alpha_k|+\rangle_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}\\ &\quad+\left(\gamma_k\beta_k|-\rangle_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0\rangle_{\mathsf{C}}+\sqrt{1-\||\gamma_k|\Psi_k\rangle\|^2}\sum_{j\geq 1}|bad_k(j)\rangle_{\mathsf{R}}|j\rangle_{\mathsf{C}}\right)|1\rangle_{\mathsf{D}}\\ &\qquad\qquad=\gamma_k\alpha_k|+\rangle_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}+|\phi\rangle_{\mathsf{R,C}}|1\rangle_{\mathsf{D}},\end{aligned}$$

where $|\phi\rangle_{\mathsf{R,C}}=\gamma_k\beta_k|-\rangle_{\mathsf{R1}}|0^{\ell-1}\rangle_{\mathsf{R2}}|0\rangle_{\mathsf{C}}+\sqrt{1-\||\gamma_k|\Psi_k\rangle\|^2}\sum_{j\geq 1}|bad_k(j)\rangle_{\mathsf{R}}|j\rangle_{\mathsf{C}}$. Step 3 then inverts the Step1 on $(\mathsf{R},\mathsf{C},\mathsf{K})$, i.e, applies $V_x^\dagger$, if the content of D is zero. Since $\langle +|_{\mathsf{R1}}\langle 0^{\ell-1}|_{\mathsf{R2}}\langle 0|_{\mathsf{C}}\langle k|_{\mathsf{K}}V_x|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|k\rangle_{\mathsf{K}}=\gamma_k\alpha_k$, the resulting state is

$$\mapsto \gamma_k\alpha_k\left((\gamma_k\alpha_k)^*|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}+\sqrt{1-|\gamma_k\alpha_k|^2}|0^\perp\rangle_{\mathsf{R,C}}\right)|0\rangle_{\mathsf{D}}+|\phi\rangle_{\mathsf{R,C}}|1\rangle_{\mathsf{D}},$$

where $|0^\perp\rangle$ is a certain state orthogonal to the all-zero state. Step 4 then increments the counter D if the content of (R,C) is not all-zero; we have

$$\mapsto |\gamma_k\alpha_k|^2|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}+\sum_{j=1}^{2}|\phi_k(j)\rangle_{\mathsf{R,C}}|j\rangle_{\mathsf{D}},$$

for certain states $|\phi_k(j)\rangle$ for $j = 1, 2$. Step 5 increments the content in register K to get the state on $(\mathsf{R}, \mathsf{C}, \mathsf{D}, \mathsf{K})$:

$$\left[|\gamma_k \alpha_k|^2 |0\rangle_{\mathsf{R}} |0\rangle_{\mathsf{C}} |0\rangle_{\mathsf{D}} + \sum_{j=1}^{2} |\phi_k(j)\rangle_{\mathsf{R},\mathsf{C}} |j\rangle_{\mathsf{D}} \right] |k+1\rangle_{\mathsf{K}} .$$

Then, we repeat the same procedure. A simple induction on k shows that the final state after applying U_+ to $|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|0^N\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}}$ is

$$U_+|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|0^N\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\gamma|\alpha_T|^2 \cdots |\alpha_0|^2 |0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1} |\phi_T(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}} \right] |0\rangle_{\mathsf{K}},$$

where $\gamma = |\gamma_T|^2 \cdots |\gamma_0|^2$. Thus, if we repeat U_+ r times, the resulting state is

$$(U_+)^r|0^\ell\rangle_{\mathsf{R}}|0^N\rangle_{\mathsf{C}}|0^N\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\left(\gamma|\alpha_T|^2 \cdots |\alpha_0|^2\right)^r |0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1} |\phi_T^{(r)}(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}} \right] |0\rangle_{\mathsf{K}},$$

for some unnormalized states $|\phi_T^{(r)}(j)\rangle$.

Next, we consider the space and gate complexities of U_+ (see the full version for a rigorous analysis). Recall that V_x can be implemented with $2^{O(s)}$ gates in G by using $O(1)$ reusable ancilla qubits. One can show by using Claims 4 and 5 that every other step in U_+ can also be implemented with $2^{O(s)}$ gates in G by using $O(1)$ reusable ancilla qubits. Consequently, U_+ can be implemented with $2^{O(s)}$ gates in G and requires $O(1)$ ancilla qubits in addition to $(\mathsf{R}, \mathsf{C}, \mathsf{D}, \mathsf{K})$, which is $O(s)$ qubits in total. Since the ancilla qubits are reusable, $(U_+)^r$ is also implementable with $r \cdot 2^{O(s)} = 2^{O(s)}$ gates in G and acts on $O(s)$ qubits. ◀

We can prove the following lemma for U_- in almost the same way.

▶ **Lemma 16.** *For every $k \in \{0, \ldots, T\}$, let β_k and γ_k be the coefficients appearing in Eqs. (1) and (2). Then, U_- given in Figure 1 acts on $O(s)$ qubits, consists of $2^{O(s)}$ gates in the gate set G, and satisfies*

$$U_-|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\gamma|\beta_T|^2 \cdots |\beta_0|^2 |0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1} |\psi_T(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}} \right] |0\rangle_{\mathsf{K}}$$

for certain unnormalized quantum states $|\psi_T(j)\rangle$ on registers (R, C) for each $j \geq 1$, where $\gamma = |\gamma_T|^2 \cdots |\gamma_0|^2$. Moreover, for every $r \in \mathbb{N} \cap 2^{O(s)}$, $(U_-)^r$ acts on $O(s)$ qubits, consists of $2^{O(s)}$ gates in the gate set G, and satisfies

$$(U_-)^r|0\rangle_{\mathsf{R}}|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{D}}|0\rangle_{\mathsf{K}} = \left[\left(\gamma|\beta_T|^2 \cdots |\beta_0|^2\right)^r |0\rangle_{\mathsf{R},\mathsf{C}}|0\rangle_{\mathsf{D}} + \sum_{j\geq 1} |\psi_T^{(r)}(j)\rangle_{\mathsf{R},\mathsf{C}}|j\rangle_{\mathsf{D}} \right] |0\rangle_{\mathsf{K}},$$

where $|\psi_T^{(r)}(j)\rangle$ is a certain unnormalized quantum state on registers (R, C) for each $j \geq 1$.

4.3 Final Unitary Circuit

Figure 2 shows a unitary quantum circuit with postselection acting on five registers $(\mathsf{W}, \mathsf{R}, \mathsf{C}, \mathsf{D}, \mathsf{K})$, where W is a single-qubit register. Now, we finalize the proof of Lemma 13 with this circuit.

UNITARY QUANTUM CIRCUIT WITH POSTSELECTION FOR PrSPACE(s) PROBLEMS

Initialize registers (W, R, C, D, K) to the all-zero state.
1. Apply the Hadamard gate H to register W.
2. If the content of W is 0, then apply $(U^{+})^{r}$ to registers (R, C, D, K); otherwise, apply $(U^{-})^{r}$ to registers (R, C, D, K).
3. Postselect the all-zero state on register D.
4. Measure register W in the basis $\{|0\rangle, |1\rangle\}$. If the outcome 0, then accept ($p_a > 1/2$); otherwise reject (i.e., $p_a < 1/2$).

Figure 2 Unitary Quantum Circuit with Postselection for PrSPACE(s) problems.

For simplicity, we first assume that $r = 1$. It is straightforward to extend the proof to the general r. It follows from Lemmas 15 and 16 that after Step 2, the state in the register (W, R, C, D, K)) is

$$\frac{1}{\sqrt{2}}|0\rangle_{\mathsf{W}}\left[\gamma|\alpha_T|^2\cdots|\alpha_0|^2|0\rangle_{\mathsf{R,C}}|0\rangle_{\mathsf{D}}+\sum_{j\geq 1}|\phi_T(j)\rangle_{\mathsf{R,C}}|j\rangle_{\mathsf{D}}\right]|0\rangle_{\mathsf{K}}$$
$$+\frac{1}{\sqrt{2}}|1\rangle_{\mathsf{W}}\left[\gamma|\beta_T|^2\cdots|\beta_0|^2|0\rangle_{\mathsf{R,C}}|0\rangle_{\mathsf{D}}+\sum_{j\geq 1}|\psi_T(j)\rangle_{\mathsf{R,C}}|j\rangle_{\mathsf{D}}\right]|0\rangle_{\mathsf{K}}. \quad (3)$$

Step 3 postselects the all-zero state in register D. Thus, the resulting state in the register (W, R, C) is

$$\gamma'\left(|\alpha_T|^2\cdots|\alpha_0|^2|0\rangle_{\mathsf{W}}+|\beta_T|^2\cdots|\beta_0|^2|1\rangle_{\mathsf{W}}\right)|0\rangle_{\mathsf{R,C}} \quad (4)$$

where γ' is the normalizing factor. Here, the probability of measuring postselecting state is

$$p_{post}=\frac{1}{2}\left(\left(\gamma|\alpha_T|^2\cdots|\alpha_0|^2\right)^2+\left(\gamma|\beta_T|^2\cdots|\beta_0|^2\right)^2\right).$$

Recall that $\alpha_k = \langle +|\Psi_k\rangle$ and $\beta_k = \langle -|\Psi_k\rangle$, where $|\Psi_k\rangle$ is defined as Eq. (2). If $p_a > 1/2$, then $\beta_k > 0$ for all k. If $p_a < 1/2$, then $\alpha_k > 0$ for all k. Since $\gamma \neq 0$, p_{post} is strictly positive in both cases.

If $p_a < 1/2$, then $|\alpha_k|^2 > |\beta_k|^2 \geq 0$ for all k, and $|\alpha_k|^2 > (1+\delta)|\beta_k|^2$ for some k and some constant δ, say, 16/9. Since $\frac{|\beta_T|^2\cdots|\beta_0|^2}{|\alpha_T|^2\cdots|\alpha_0|^2} < \frac{1}{1+\delta} = \frac{9}{25}$, the probability that $|0\rangle_W$ is measured in Step 4, that is, the probability of obtaining the outcome 0 when measuring register W in Eq. (4) in the basis $\{|0\rangle, |1\rangle\}$, is

$$\frac{|\alpha_T|^4\cdots|\alpha_0|^4}{|\alpha_T|^4\cdots|\alpha_0|^4+|\beta_T|^4\cdots|\beta_0|^4}=\frac{1}{1+\left(|\beta_T|^4\cdots|\beta_0|^4\right)/\left(|\alpha_T|^4\cdots|\alpha_0|^4\right)}>\frac{1}{1+(9/25)^2}=\frac{625}{706}.$$

If $p_a > 1/2$, then $0 \leq |\alpha_k|^2 < |\beta_k|^2$ for all k, and $(1+\delta)|\alpha_k|^2 < |\beta_k|^2$ for some k and a constant $\delta = 16/9$. Thus, the probability that $|1\rangle_{\mathsf{W}}$ is measured in Step 4 is at least $\frac{625}{706}$ in the same analysis as in the case of $p_a < 1/2$.

For a general $r \in 2^{O(s)}$, the state in the register (W, R, C) after Step 3 is

$$\gamma''\left(\left(|\alpha_T|^2\cdots|\alpha_0|^2\right)^r|0\rangle_{\mathsf{W}}+\left(|\beta_T|^2\cdots|\beta_0|^2\right)^r|1\rangle_{\mathsf{W}}\right)|0\rangle_{\mathsf{R,C}},$$

where γ'' is the normalizing factor. For $p_a < 1/2$, thus, the probability that $|0\rangle$ is measured in Step 4 is

$$\frac{\left(|\alpha_T|^4 \cdots |\alpha_0|^4\right)^r}{\left(|\alpha_T|^4 \cdots |\alpha_0|^4\right)^r + \left(|\beta_T|^4 \cdots |\beta_0|^4\right)^r} > \frac{1}{1 + (9/25)^{2r}} > 1 - \frac{81^r}{625^r + 81^r} > 1 - \frac{1}{2^r}.$$

Similarly, for $p_a > 1/2$, the probability that $|1\rangle$ is measured in Step 4 is at least $1 - \frac{1}{2^r}$.

Finally, we consider the space and gate complexities. The quantum circuit in Figure 2 acts on a single-qubit register W in addition to $(\mathsf{R}, \mathsf{C}, \mathsf{D}, \mathsf{K})$. In this circuit, every gate $g \in G$ used in $(U_+)^r$ and $(U_-)^r$ is replaced with $\wedge(g)$, which can be implemented with $O(1)$ gates in G with $O(1)$ resuable ancilla qubits by Claim 4. Since Step 2 is dominant, and $(U_+)^r$ and $(U_-)^r$ use $O(s)$ qubits and $2^{O(s)}$ gates in G by Lemmas 15 and 16, the entire circuit uses $O(s)$ qubits and $2^{O(s)}$ gates in G.

5 Application to One-Clean Qubit Model

As introduced in Section 1, DQC1 is a model of quantum computing such that the input state is completely mixed except for one qubit, which is initialized to $|0\rangle$.

▶ **Definition 17** ($\mathsf{PostQ_{[1]}SPACE}$). *Let s be any space-constructible function with $s(n) \in \Omega(\log n)$, and let c, d be s-space computable functions.* $\mathsf{PostQ_{[1]}SPACE}(s)[c, d]$ *is the class of promised problems $L = (L_Y, L_N)$ for which there exists an s-space uniform family of unitary quantum circuits $\{U_x : x \in L\}$ consisting of $2^{O(s)}$ elementary gates on $m + 1$ qubits for $m \in O(s)$ such that, when applying U_x to the $m + 1$ qubits in state $|0\rangle\langle 0| \otimes (\mathrm{I}/2)^{\otimes m}$, followed by postselections and measurements, (1) the probability p_{post} of measuring $|1\rangle$ on all postselection qubits is strictly positive; (2) for $x \in L_Y$, conditioned on all the postselection qubits being $|1\rangle$, the probability that U_x accepts is at least $c(|x|)$; (3) for $x \in L_N$, conditioned on all the postselection qubits being $|1\rangle$, the probability that U_x accepts is at most $d(|x|)$. In particular, define* $\mathsf{PostBQ_{[1]}SPACE}(s) \equiv \mathsf{PostQ_{[1]}SPACE}(s)[2/3, 1/3]$, *and* $\mathsf{PostBQ_{[1]}L} \equiv \mathsf{PostBQ_{[1]}SPACE}(\log)$.

In the above definition, we allow postselection to be made on multiple qubits, since it does not seem possible in general to aggregate multiple postselection qubits to a single qubit due to the lack of initialized qubits. Theorem 3 follows from Theorems 10 and 18.

▶ **Theorem 18.** *For any space-constructible function s with $s(n) \in \Omega(\log n)$ and any s-space computable functions c and d such that $c(n) > d(n)$ for sufficiently large $n \in \mathbb{N}$,*

$$\mathsf{PostQ_{[1]}SPACE}(s)[c, d] = \mathsf{PostQuSPACE}(s)[c, d].$$

In particular, $\mathsf{PostBQ_{[1]}SPACE}(s) = \mathsf{PostBQuSPACE}(s)$ *and* $\mathsf{PostBQ_{[1]}L} = \mathsf{PostBQuL}$.

The proof is provided in the full version.

References

1 Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A*, 461(2063):3473–3482, 2005. doi:10.1098/rspa.2005.1546.

2 Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9:143–252, 2013. doi:10.4086/toc.2013.v009a004.

3 Andris Ambainis, Leonard J. Schulman, and Umesh V. Vazirani. Computing with highly mixed states. *Journal of the ACM*, 53(3):507–531, 2006. doi:10.1145/1147954.1147962.

4 R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. *Journal of Computer and System Sciences*, 50(2):191–202, 1995. doi:10.1006/jcss.1995.1017.

5 A. Borodin, S. Cook, and N. Pippenger. Parallel computation for well-endowed rings and space-bounded probabilistic machines. *Information and Control*, 58(1):113–136, 1983. doi:10.1016/S0019-9958(83)80060-6.

6 Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A*, 467:459–472, 2010. doi:10.1098/rspa.2010.0301.

7 Bill Fefferman and Zachary Remscrim. Eliminating intermediate measurements in space-bounded quantum computation. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2021*, pages 1343–1356, 2021. doi:10.1145/3406325.3451051.

8 Lance Fortnow and Nick Reingold. PP is closed under truth-table reductions. *Inf. Comput.*, 124(1):1–6, 1996. doi:10.1006/inco.1996.0001.

9 Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. Power of quantum computation with few clean qubits. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 13:1–13:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.ICALP.2016.13.

10 Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. Impossibility of classically simulating one-clean-qubit model with multiplicative error. *Phys. Rev. Lett.*, 120:200502, 2018. doi:10.1103/PhysRevLett.120.200502.

11 François Le Gall, Harumichi Nishimura, and Abuzer Yakaryilmaz. Quantum logarithmic space and post-selection. In *Proceedings of the 16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 10:1–10:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.TQC.2021.10.

12 Uma Girish, Ran Raz, and Wei Zhan. Quantum logspace algorithm for powering matrices with bounded norm. In *Proceedings of the 48th International Colloquium on Automata, Languages, and Programming, ICALP 2021*, volume 198 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 73:1–73:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ICALP.2021.73.

13 Hermann Jung. On probabilistic time and space. In *Proceedings of the 12th Colloquium on Automata, Languages and Programming*, pages 310–317. Springer-Verlag, 1985. doi:10.1007/BFb0015756.

14 Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. AMS, 2002.

15 E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672–5675, December 1998. doi:10.1103/PhysRevLett.81.5672.

16 Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8(1):1–51, 2012. doi:10.4086/toc.2012.v008a001.

17 Tomoyuki Morimae, Keisuke Fujii, and Joseph F. Fitzsimons. Hardness of classically simulating the one-clean-qubit model. *Phys. Rev. Lett.*, 112:130502, 2014. doi:10.1103/PhysRevLett.112.130502.

18 Tomoyuki Morimae, Keisuke Fujii, and Harumichi Nishimura. Power of one nonclean qubit. *Phys. Rev. A*, 95:042336, 2017. doi:10.1103/PhysRevA.95.042336.

19 Tomoyuki Morimae and Harumichi Nishimura. Merlinization of complexity classes above BQP. *Quantum Info. Comput.*, 17(11–12):959–972, 2017. doi:10.26421/QIC17.11-12-3.

20 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. doi:10.1017/CBO9780511976667.

21 Harumichi Nishimura. Personal communication, 2021.

22 M. Saks. Randomization and derandomization in space-bounded computation. In *Proceedings of Computational Complexity (Formerly Structure in Complexity Theory)*, pages 128–149, 1996. doi:10.1109/CCC.1996.507676.

23 Peter W. Shor and Stephen P. Jordan. Estimating Jones polynomials is a complete problem for one clean qubit. *Quantum Information & Computation*, 8(8):681–714, 2008. doi:10.26421/QIC8.8-9-1.

24 Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, STOC '13*, pages 881–890, 2013. doi:10.1145/2488608.2488720.

25 John Watrous. Quantum simulations of classical random walks and undirected graph connectivity. *Journal of Computer and System Sciences*, 62(2):376–391, 2001. doi:10.1006/jcss.2000.1732.

26 John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12:48–84, 2003. doi:10.1007/s00037-003-0177-8.