Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection

Ryo Hiromasa ✉
Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura, Japan

Akihiro Mizutani ✉
Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura, Japan

Yuki Takeuchi ✉
NTT Communication Science Laboratories, NTT Corporation, Atsugi, Japan

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

Abstract

We define rewinding operators that invert quantum measurements. Then, we define complexity classes RwBQP, CBQP, and $\mathsf{AdPostBQP}$ as sets of decision problems solvable by polynomial-size quantum circuits with a polynomial number of rewinding operators, cloning operators, and adaptive postselections, respectively. Our main result is that $\mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP} = \mathsf{CBQP} = \mathsf{AdPostBQP} \subseteq \mathsf{PSPACE}$. As a byproduct of this result, we show that any problem in $\mathsf{PostBQP}$ can be solved with only postselections of outputs whose probabilities are polynomially close to one. Under the strongly believed assumption that $\mathsf{BQP} \not\supseteq \mathsf{SZK}$, or the shortest independent vectors problem cannot be efficiently solved with quantum computers, we also show that a single rewinding operator is sufficient to achieve tasks that are intractable for quantum computation. In addition, we consider rewindable Clifford and instantaneous quantum polynomial time circuits.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases Quantum computing, Postselection, Lattice problems

Digital Object Identifier 10.4230/LIPIcs.TQC.2023.9

Related Version *Full Version*: https://arxiv.org/abs/2206.05434 [23]

Funding *Akihiro Mizutani*: Supported by JST, ACT-X Grant Number JPMJAX210O, Japan.
Yuki Takeuchi: Supported by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0118067394 and JPMXS0120319794 and JST [Moonshot R&D – MILLENNIA Program] Grant Number JPMJMS2061.
Seiichiro Tani: Supported by the Grant-in-Aid for Transformative Research Areas No.JP20H05966 of JSPS, JST [Moonshot R&D – MILLENNIA Program] Grant Number JPMJMS2061, and the Grant-in-Aid for Scientific Research (A) No.JP22H00522 of JSPS.

Acknowledgements We thank Yasuhiro Takahashi and Yusuke Aikawa for helpful discussions. We also thank Tomoyuki Morimae for fruitful discussions and pointing out Refs. [4, 5] to us.

1 Introduction

1.1 Background and Our Contribution

It is believed that universal quantum computers outperform their classical counterparts. There are two approaches to strengthening this belief. The first is to introduce tasks that seem intractable for classical computers but can be efficiently solved with quantum computers. For example, no known efficient classical algorithm can solve the integer factorization, but Shor's quantum algorithm [33] can do it efficiently. The second approach is to consider what happens if classical computers can efficiently simulate the behaviors of quantum computers. So far, sampling tasks have often been considered in this approach [22]. It has been shown that if any probability distribution obtained from some classes of quantum circuits (e.g., instantaneous quantum polynomial time (IQP) circuits [12]) can be efficiently simulated with classical computers, then PH collapses to its second [17, 27] or third level [12, 3, 26, 24, 13, 34, 35, 18, 20, 25, 10, 21, 11], or BQP is in the second level of PH [28]. Since the collapse of PH and the inclusion of BQP in PH are considered to be unlikely, these results imply quantum advantages.

In this paper, we take the second approach. If efficient classical simulation of quantum measurements is possible, then the measurements become invertible because classical computation is reversible. From the analogy of the rewinding technique used in zero-knowledge (see e.g., [37, 7, 36]), we call such measurements rewindable measurements. They make quantum computation genuinely reversible and *incredibly* powerful. More formally, the following rewinding operator R becomes possible. R receives a post-measurement n-qubit quantum state $(|z\rangle\langle z| \otimes I^{\otimes n-1})|\psi\rangle$ with $z \in \{0,1\}$ and a classical description $\mathcal{D}$ of a pre-measurement quantum state $|\psi\rangle$ and outputs the quantum state $|\psi\rangle$:

$$R\left(\left(|z\rangle\langle z| \otimes I^{\otimes n-1}\right)|\psi\rangle \otimes |\mathcal{D}\rangle\right) = |\psi\rangle, \tag{1}$$

where $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. As an important point, R requires the classical description $\mathcal{D}$ as an input. If it requires only $(|z\rangle\langle z| \otimes I^{\otimes n-1})|\psi\rangle$ as an input, the output state cannot be uniquely determined. For example, in the case of both $|\psi\rangle = |0\rangle|+\rangle$ and $(|0\rangle|+\rangle + |1\rangle|-\rangle)/\sqrt{2}$, the post-measurement state is $|0\rangle|+\rangle$ for $z = 0$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. To circumvent this problem, we require the classical description $\mathcal{D}$ as information about $|\psi\rangle$. As a concrete example, the classical descriptions of $|0\rangle|+\rangle$ and $(|0\rangle|+\rangle + |1\rangle|-\rangle)/\sqrt{2}$ are $I \otimes H$ and $CZ(H \otimes H)$, respectively. Here, $H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$ is the Hadamard gate, $CZ \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$ is the controlled-Z (CZ) gate, and $Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$ is the Pauli-Z operator. These descriptions are proper because $|0\rangle|+\rangle$ and $(|0\rangle|+\rangle + |1\rangle|-\rangle)/\sqrt{2}$ can be prepared by applying $I \otimes H$ and $CZ(H \otimes H)$ on the fixed initial state $|00\rangle$, respectively. Furthermore, we define rewinding operators for only pure states, that is their functionality is arbitrary for mixed states. Due to this restriction, we can avoid contradictions with an ordinary interpretation of mixed states (see Sec. 3) and the no-signaling principle (see the full paper [23]).

It is strongly believed that the rewinding of measurements cannot be performed in ordinary quantum mechanics, i.e., the superposition is destroyed by measurements, and it cannot be recovered after measurements. One may think that if the rewinding were possible against this belief, it could add extra computation power to universal quantum computers. We show that this expectation is indeed correct. More formally, we define RwBQP (BQP with rewinding) as a set of decision problems solvable by polynomial-size quantum circuits with a polynomial number of rewinding operators and show $\mathsf{BQP} \subseteq \mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP}$.

The rewinding operator can be considered a probabilistic postselection. By just repeating measurements and rewinding operations until the target outcome is obtained, we can efficiently simulate the postselection with high probability if the output probability of the target outcome is at least the inverse of some polynomial. However, the original postselection enables us to deterministically obtain a target outcome even if the probability is exponentially small [2]. In this case, the above simple repeat-until-success approach requires an exponential number of rewinding operations on average. Surprisingly, we show that it is possible to exponentially mitigate probabilities of nontarget outcomes with a polynomial number of rewinding operators. By using this mitigation protocol, we can obtain the target outcome with high probability even if the output probability of the target outcome is exponentially small. In this sense, the rewinding and postselection are equivalent. More formally, we show that RwBQP is equivalent to the class AdPostBQP (BQP with adaptive postselection) of decision problems solvable by polynomial-size quantum circuits with a polynomial number of adaptive postselections. Here, an adaptive postselection is a projector $|b\rangle\langle b|$ such that the value of $b \in \{0,1\}$ depends on previous measurement outcomes. From this equivalence, we also obtain RwBQP $\subseteq$ PSPACE.

The rewinding is also related to cloning. By strengthening our rewinding operator in Eq. (1), we define the cloning operator C as follows:

$$C|\mathcal{D}\rangle = |\psi\rangle. \tag{2}$$

Unlike Eq. (1), this operator does not require the post-measurement state $(|z\rangle\langle z| \otimes I^{\otimes n-1})|\psi\rangle$. Since it is easy to duplicate the classical description $\mathcal{D}$, we can efficiently duplicate $|\psi\rangle$, i.e., generate $|\psi\rangle^{\otimes 2}$ by simply applying $C \otimes C$ on $|\mathcal{D}\rangle^{\otimes 2}$. Although the ordinary cloning operator $\tilde{C}$ is defined such that $\tilde{C}(|\psi\rangle|0^m\rangle) = |\psi\rangle^{\otimes 2}$ for some $m \in \mathbb{N}$ [38], we define C as an operator whose input is the classical description $\mathcal{D}$ of $|\psi\rangle$ rather than $|\psi\rangle$ itself. This makes sense because we can always obtain a classical description of $|\psi\rangle$ in our setting[1]. Note that it could be difficult to realize C in quantum polynomial time because $|\psi\rangle$ might be prepared by using measurements. More precisely, it may be defined as a quantum state prepared when the measurement outcome is 0, e.g., $|\psi\rangle = U_2(I \otimes |0\rangle\langle 0| \otimes I^{\otimes n-2})U_1|0^n\rangle$ for some unitary operators U_1 and U_2. We show that RwBQP is also equivalent to the class CBQP (BQP with cloning) of decision problems solvable by polynomial-size quantum circuits with a polynomial number of cloning operators. That is, the difference between Eqs. (1) and (2) does not matter to the computation power. The following theorem summarizes our main results explained above:

▶ **Result 1** (Theorem 16)**.** $\mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP} = \mathsf{CBQP} = \mathsf{AdPostBQP} \subseteq \mathsf{PSPACE}$.

The computation power of the cloning has been addressed in [4] as an open problem. Result 1 gives lower and upper bounds on our class CBQP, and it seems to be a reasonable approach to capturing the power of cloning.

All the above results assume that rewinding operators can be utilized a polynomial number of times. Under the strongly believed assumption that the shortest independent vectors problem (SIVP) [30] cannot be efficiently solved with universal quantum computers, we show that a single rewinding operator is sufficient to achieve a task that is intractable for universal quantum computation:

▶ **Result 2** (Informal Version of Theorem 22)**.** *Assume that there is no polynomial-time quantum algorithm that solves the SIVP. Then, there exists a problem such that it can be efficiently solved with a constant probability if a single rewinding operator is allowed for quantum computation, but the probability is super-polynomially small if it is not allowed.*

We also show a superiority of a single rewinding operator under a different assumption:

▶ **Result 3** (Informal Version of Corollary 24)**.** *Let* RwBQP(1) *be* RwBQP *with a single rewinding operator. Then,* RwBQP(1) $\supset$ BQP *unless* BQP $\supseteq$ SZK.

It is strongly believed that BQP does not include SZK. At least, we can say that it is hard to show BQP $\supseteq$ SZK because there exists an oracle A such that $\mathsf{BQP}^A \not\supseteq \mathsf{SZK}^A$ [1]. For example, by assuming that the decision version of SIVP, gapSIVP, is hard for universal quantum computation, Result 3 implies that a single rewinding operator is sufficient to

[1] Since we are interested in complexity classes, we consider only quantum states generated from quantum circuits in uniform families.

achieve a task that is intractable for universal quantum computation. This is because the gapSIVP (with an appropriate parameter) is in SZK [29]. As a difference from Result 2, Result 3 shows the superiority of a single rewinding operator for promise problems.

As simple observations, we also consider the effect of rewinding operators for restricted classes of quantum circuits. It has been shown that polynomial-size Clifford circuits are classically simulatable [19]. We show that such circuits with rewinding operators are still classically simulatable (for details, see the full paper [23]). It is also known that IQP circuits are neither universal nor classically simulatable under plausible complexity-theoretic assumptions [13]. We show that IQP circuits with rewinding operators can efficiently solve any problem in RwBQP (for details, see the full paper [23]).

Our mitigation protocol used to show AdPostBQP $\subseteq$ RwBQP also has an application for PostBQP [2], which is a class of decision problems solvable by polynomial-size quantum circuits with non-adaptive postselections. By slightly modifying our mitigation protocol and replacing rewinding operators with postselections, we obtain the following corollary:

▶ **Result 4** (Corollary 20). *For any polynomial function $p(|x|)$ in the size $|x|$ of an instance x,* PP = PostBQP *holds even if only non-adaptive postselections of outputs whose probabilities are at least $1-\Omega(1/p(|x|))$ are allowed.*

The equality PP = PostBQP was originally shown in [2] by using postselections of outputs whose probabilities may be exponentially small. Result 4 shows that such postselections can be replaced with those of outputs whose probabilities are polynomially close to one. This result is *optimal* in the sense that polynomially many repetitions of non-adaptive postselections of outputs whose probabilities are $1-1/f(|x|)$ with a super-polynomial function $f(|x|)$ can be simulated in quantum polynomial time. It is worth mentioning that when the probabilities are at least some constant, the above replacement is obvious in PostBPP (or $\mathsf{BPP_{path}}$). This is because any behavior of a probabilistic Turing machine can be represented as a binary tree such that each path is chosen with probability 1/2. However, in its quantum analogue PostBQP, it was open as to whether such replacement is possible even if the probabilities are at least some constant.

Other related works and open problems are introduced in the full paper [23].

1.2 Overview of Techniques

To obtain Result 1, we show (i) RwBQP $\subseteq$ CBQP; (ii) CBQP $\subseteq$ AdPostBQP; (iii) AdPostBQP $\subseteq$ RwBQP; (iv) $\mathsf{BQP^{PP}} \subseteq$ RwBQP, which immediately means $\mathsf{BPP^{PP}} \subseteq$ RwBQP because $\mathsf{BPP^{PP}} \subseteq \mathsf{BQP^{PP}}$; and (v) AdPostBQP $\subseteq$ PSPACE. The first inclusion (i) is obvious from the definitions of the rewinding operator R and cloning operator C (see Eqs. (1) and (2)). The fifth inclusion (v) can also be easily shown by using the Feynman path integral that is used to show BQP $\subseteq$ PSPACE [9]. In BQP, measurements are only performed at the end of quantum circuits. On the other hand, in AdPostBQP, intermediate ordinary and postselection measurements are also allowed. However, this difference does not matter in showing the inclusion in PSPACE.

The second inclusion (ii) is a natural consequence from the simple observation that postselections can simulate the cloning operator C. On the other hand, the third inclusion (iii) is nontrivial because we have to efficiently simulate postselection by using only a polynomial number of rewinding operators. To this end, we give an efficient protocol to exponentially mitigate the amplitude of a nontarget state by using a polynomial number of rewinding operators. Let $|\psi\rangle = \sqrt{2^{-p(n)}}|\psi_t\rangle + \sqrt{1-2^{-p(n)}}|\psi_t^{\perp}\rangle$, where $p(n)$ is some polynomial in the size n of a given AdPostBQP problem, $|\psi_t\rangle$ is a target state that we would like to postselect, and $\langle\psi_t|\psi_t^{\perp}\rangle = 0$. By using our mitigation protocol, from $|\psi\rangle$, we can obtain

$\sqrt{2^{-p(n)}}|\psi_t\rangle + \sqrt{2^{-p(n)}(1-2^{-p(n)})}|\psi_t^{\perp}\rangle$ up to a normalization factor. Since $2^{-p(n)}$ is larger than $2^{-p(n)}(1-2^{-p(n)})$, we now obtain $|\psi_t\rangle$ with probability of at least $1/2$. By repeating these procedures, we can simulate the postselection of $|\psi_t\rangle$ with high probability.

Our mitigation protocol is also useful in showing the fourth inclusion (iv). First, from $\mathsf{PP} = \mathsf{PostBQP}$ [2], we obtain $\mathsf{PP} \subseteq \mathsf{RwBQP}$ by using our mitigation protocol. Then, we show that the completeness-soundness gap in RwBQP can be amplified to a constant exponentially close to 1, and RwBQP is closed under composition. By combining these results, we obtain $\mathsf{BQP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP}^{\mathsf{RwBQP}} = \mathsf{RwBQP}$. Note that $\mathsf{BQP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP}^{\mathsf{PP}}$ is obvious from the definition of RwBQP (see Def. 9).

We show Result 2 as follows. Cojocaru *et al.* have shown that under the hardness of SIVP, there exists a family $\mathcal{F} \equiv \{f_K\}_{K\in\mathcal{K}}$ of functions that is collision resistant against quantum computers, i.e., no polynomial-time quantum algorithm can output a collision pair (x, x') such that $x \neq x'$ and $f_K(x) = f_K(x')$ [15]. Here, $\mathcal{K}$ is a finite set of parameters uniquely specifying each function (see Sec. 2.2 for details). We show that a collision pair can be output with a constant probability if only one rewinding operator is given. From the construction of $\mathcal{F}$, the last bits of collision pairs are different, i.e., there exist x_0 and x_1 such that $x = (x_0, 0)$ and $x' = (x_1, 1)$. Using the idea in [14], we can efficiently prepare

$$\frac{|x_0\rangle|0\rangle + |x_1\rangle|1\rangle}{\sqrt{2}} \tag{3}$$

for some output value $y = f_K(x) = f_K(x')$. Note that since the preparation of Eq. (3) includes a measurement, if we perform it again, we will obtain a quantum state in Eq. (3) for a different output value y', and hence it is difficult to simultaneously obtain x and x' for the same y. When we can use a rewinding operator, the situation changes. By measuring the state in Eq. (3), we can obtain x_0 or x_1. For simplicity, suppose that we obtain x_0. Then, by performing the rewinding operator R on $|x_0\rangle|0\rangle$ and a classical description of Eq. (3), we can prepare the quantum state in Eq. (3) for the *same* y. From this state, we can obtain x_1 with probability $1/2$. As an important point, since the last bits of x and x' differ, a single rewinding operator (i.e., the rewinding of a single qubit) is sufficient to find a collision pair with a constant probability.

Finally, we show Result 3. To this end, we show that a SZK-complete problem is in RwBQP(1) by using a technique inspired by [5].

2 Preliminaries

In this section, we review some preliminaries that are necessary to understand our results. In Sec. 2.1, we introduce a complexity class PostBQP and explain the postselection. In Sec. 2.2, we introduce the SIVP and a collision-resistant and $\delta - 2$ regular family of functions.

2.1 Quantum complexity class

In this subsection, we review PostBQP and explain the postselection. Then, we clarify a difference between PostBQP and our class AdPostBQP (see Def. 11). Note that we assume that readers are familiar with classical complexity classes [8]. PostBQP is defined as follows:

▶ **Definition 5** (PostBQP [2]). *A promise problem $L = (L_{\mathrm{yes}}, L_{\mathrm{no}}) \subseteq \{0,1\}^*$ is in* PostBQP *if and only if there exist polynomials n and q and a uniform family $\{U_x\}_x$ of polynomial-size quantum circuits, such that*

- $\Pr[p = 1] \geq 1/2^q$
- *when* $x \in L_{\mathrm{yes}}$, $\Pr[o = 1 \mid p = 1] \geq 2/3$
- *when* $x \in L_{\mathrm{no}}$, $\Pr[o = 1 \mid p = 1] \leq 1/3$,

where o and p are called output and postselection registers, respectively. Here, for any $z_1 \in \{0,1\}$ and $z_2 \in \{0,1\}$,

$$\Pr[p = z_2] \equiv \langle 0^n | U_x^\dagger \left(I \otimes |z_2\rangle\langle z_2| \otimes I^{\otimes n-2} \right) U_x | 0^n \rangle \tag{4}$$

$$\Pr[o = z_1 \mid p = z_2] \equiv \frac{\langle 0^n | U_x^\dagger \left(|z_1 z_2\rangle\langle z_1 z_2| \otimes I^{\otimes n-2} \right) U_x | 0^n \rangle}{\Pr[p = z_2]}. \tag{5}$$

In this definition, "polynomial" means the one in the length $|x|$ of the instance x.

From Def. 5, we notice that the postselection is to apply a projector. In PostBQP, it is allowed to apply the projector $|1\rangle\langle 1|$ to the qubit in the postselection register at the end of a quantum circuit. Therefore, PostBQP is a set of promise problems solvable by polynomial-size quantum circuits (in uniform families) with a single non-adaptive postselection[2]. On the other hand, in AdPostBQP, we allow the application of a polynomial number of intermediate measurements and projectors. This means that the value $b \in \{0,1\}$ of a projector $|b\rangle\langle b|$ can depend on previous measurement outcomes, while it is determined before executing a quantum circuit in PostBQP.

2.2 SIVP

The SIVP with approximation factor γ (SIVP_γ) is defined as follows:

▶ **Definition 6** (SIVP_γ). *Let n be any natural number and γ (≥ 1) be any real number. Given an n bases of a lattice L, output a set of n linearly independent lattice vectors of length at most $\gamma \cdot \lambda_n(L)$. Here, γ can depend on n, and $\lambda_n(L)$ is the nth successive minimum of L (i.e., the smallest r such that L has n linearly independent vectors of norm at most r).*

Since there is no known polynomial-time quantum algorithm to solve SIVP_γ for polynomial approximation factor, it is used as a basis of the security of lattice-based cryptography [30].

The hardness of the SIVP is also used to construct families of collision-resistant functions against universal quantum computers. From [15], we can immediately obtain the following theorem:

▶ **Theorem 7** (adapted from [15]). *Let n be any natural number, $q = 2^{5\lceil \log n \rceil + 21}$, $m = 23n + 5n\lceil \log n \rceil$, $\mu = 2mn\sqrt{23 + 5\log n}$, and $\mu' = \mu/m$, where $\lceil \cdot \rceil$ is the ceiling function. Let $K \equiv (A, As_0 + e_0) \in \mathcal{K}$ with $\mathcal{K}$ being the multiset $\{(A, As_0 + e_0)\}_{A \in \mathbb{Z}_q^{n\times m}, s_0 \in \mathbb{Z}_q^n, e_0 \in \chi'^m}$, where $\mathbb{Z}_q^{n\times m}$ be the set of $n \times m$ matrices each of whose entry is chosen from $\mathbb{Z}_q \equiv \{0, 1, \ldots, q-1\}$, and χ' is the set of integers bounded in absolute value by μ'. Assume that there is no polynomial-time quantum algorithm that solves $\mathrm{SIVP}_{p(n)}$ for some polynomial $p(n)$ in n. Then, the family $\mathcal{F} \equiv \{f_K : \mathbb{Z}_q^n \times \chi^m \times \{0,1\} \to \mathbb{Z}_q^m\}_{K \in \mathcal{K}}$ of functions*

$$f_K(s, e, c) \equiv As + e + c \cdot (As_0 + e_0) \pmod{q}, \tag{6}$$

where χ is the set of integers bounded in absolute value by μ, is collision resistant[3] and δ-2 regular[4] for a constant δ.

---

[2] Note that a polynomial number of postselections are allowed if they can be unified as a single non-adaptive postselection.

[3] Let $\mathcal{F} \equiv \{f_K : \mathcal{D} \to \mathcal{R}\}_{K \in \mathcal{K}}$ be a function family. We say that $\mathcal{F}$ is collision resistant if for any polynomial-time quantum algorithm A, which receives K and outputs two bit strings $x, x' \in \mathcal{D}$, the probability $\Pr_K[A(K) = (x, x')$ such that $x \neq x'$ and $f_K(x) = f_K(x')]$ is super-polynomially small. Note that K is chosen from $\mathcal{K}$ uniformly at random, and the probability is also taken over the randomness in A.

[4] Let $\mathcal{F} \equiv \{f_K : \mathcal{D} \to \mathcal{R}\}_{K \in \mathcal{K}}$ be a function family. For a fixed K, we say that $y \in \mathcal{R}$ has two preimages if there exist exactly two different inputs $x, x' \in \mathcal{D}$ such that $f(x) = f(x') = y$. Let $\mathcal{Y}_K^{(2)}$ be the set of y having two preimages for K. The function family $\mathcal{F}$ is said to be δ-2 regular when $\Pr_{K,x}[f_K(x) \in \mathcal{Y}_K^{(2)}] \geq \delta$, where K and x are chosen from $\mathcal{K}$ and $\mathcal{D}$, respectively, uniformly at random.

From Eq. (6), the function f_K has a collision pair[5] $(s, e, 1)$ and $(s + s_0, e + e_0, 0)$, and Theorem 7 shows that it is difficult to find them simultaneously. This function family will be used to show that a single rewinding operator is sufficient to achieve a task that seems difficult for universal quantum computers.

Note that in [15], the matrix A is constructed so that it has a trapdoor to efficiently invert $As + e$, and its distribution is statistically close to uniform over $\mathbb{Z}_q^{n\times m}$. In Theorem 7, we consider a simplified variant of the function family of [15] in which the matrix A is chosen uniformly at random.

3 Computational Complexity of Rewinding

In this section, we show Results 1 and 4. To this end, first, we define the rewinding operator R and cloning operator C as follows:

▶ **Definition 8** (Rewinding and Cloning Operators). *Let n be any natural number, Q be any n-qubit linear operator composed of unitary operators and the Z-basis projective operators $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, $\mathcal{D}$ be a classical description of the linear operator Q, and I be the single-qubit identity operator. The rewinding and cloning operators R and C are maps from a quantum state to a quantum state such that for any $s \in \{0,1\}$, when $\left(|s\rangle\langle s| \otimes I^{\otimes n-1}\right) Q|0^n\rangle \neq 0$,*

$$R\left(\frac{\left(|s\rangle\langle s| \otimes I^{\otimes n-1}\right) Q|0^n\rangle}{\sqrt{\langle 0^n|Q^\dagger \left(|s\rangle\langle s| \otimes I^{\otimes n-1}\right) Q|0^n\rangle}} \otimes |\mathcal{D}\rangle\right) = \frac{Q|0^n\rangle}{\sqrt{\langle 0^n|Q^\dagger Q|0^n\rangle}} \tag{7}$$

$$C|\mathcal{D}\rangle = \frac{Q|0^n\rangle}{\sqrt{\langle 0^n|Q^\dagger Q|0^n\rangle}}. \tag{8}$$

For other input states, the functionality of R and C is undefined, that is outputs are arbitrary n-qubit states. Particularly when it depends on a value of classical bits whether R and C are applied, we call them classically controlled rewinding and cloning operators, respectively.

Note that since the linear operator Q may include projective operators (e.g., $Q = U_2(I \otimes |0\rangle\langle 0| \otimes I^{\otimes n-2})U_1$ for some n-qubit unitary operators U_1 and U_2), in general, $Q^\dagger Q \neq I^{\otimes n}$. An example of classically controlled rewinding operators is an operator such that if a measurement outcome is 0, the identity operator is applied to the post-measurement state, but if the outcome is 1, the rewinding operator R is applied to it. Classically controlled rewinding and cloning operators play an important role in giving our main result.

Simply speaking, the rewinding operator R rewinds the state projected onto $|s\rangle$ to the state before the measurement. As an important point, Def. 8 implies that the rewinding operator R only works for pure states. The following contradiction for an ordinary interpretation of mixed states occurs without the restriction to pure states. Suppose that we measure a maximally mixed state $I/2$ in the computational basis[6], and then obtain the measurement outcome 0. In this case, it is natural that even if we rewind this measurement and perform the same measurement again, the outcome is always 0. However, if we define the rewinding operator R so that it also works for mixed states, then we can obtain $I/2$ from $|0\rangle$ with the rewinding operator, and the measurement on it may output 1. In other words, if the rewinding operator works for a mixed state ρ, we can measure ρ again and again, and thus

[5] Since q is larger than μ, the second element $e + e_0$ of the second input may not be in the set χ^m. Therefore, the probability of f_K having a collision pair is not 1.

[6] We sometimes call the Z basis the computational basis.

we obtain its information as much as we want without changing ρ. This situation contradicts with the natural interpretation that mixed states arise due to the lack of knowledge about them. Furthermore, the restriction to pure states would be useful in circumventing the contradiction with the no-signaling principle as explained in the full paper [23]. From Def. 8, it is easily observed that the cloning operator C can efficiently simulate the rewinding operator R.

By using the rewinding and cloning operators and postselections, we define three complexity classes – RwBQP (BQP with rewinding), CBQP (BQP with cloning), and AdPostBQP (BQP with adaptive postselection) – as follows:

▶ **Definition 9** (RwBQP and CBQP). *Let n and k be any natural number, ℓ be a polynomial in n, and $0 \leq s < c \leq 1$. A promise problem $L = (L_{\rm yes}, L_{\rm no}) \subseteq \{0,1\}^*$ is in* $\mathsf{RwBQP}(c,s)(k)$ *if and only if there exists a polynomial-time deterministic Turing machine that receives 1^n as an input and generates a ℓ-bit description $\tilde{\mathcal{D}}$ of an operator Q_n such that it consists of a polynomial number of elementary gates in a universal gate set, single-qubit measurements in the computational basis, and k (classically controlled) rewinding operators R defined in Def. 8 and satisfies, for the instance $x \in \{0,1\}^n$ and a polynomial m, that*

- *if* $x \in L_{\rm yes}$, $\left|\left|\left(|1\rangle\langle 1| \otimes I^{\otimes n+m+\ell-1}\right) Q_n \left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)\right|\right|^2 \geq c$
- *if* $x \in L_{\rm no}$, $\left|\left|\left(|1\rangle\langle 1| \otimes I^{\otimes n+m+\ell-1}\right) Q_n \left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)\right|\right|^2 \leq s$.

Here, $|||v\rangle|| \equiv \sqrt{\langle v|v\rangle}$ for any vector $|v\rangle$, and "polynomial" is the abbreviation of "polynomial in n." Particularly, for the set $\mathrm{poly}(n)$ of all polynomial functions, we denote $\bigcup_{k\in\mathrm{poly}(n)} \mathsf{RwBQP}(2/3,1/3)(k)$ as RwBQP.

By replacing R with the cloning operator C defined in Def. 8, $\mathsf{CBQP}(c,s)(k)$ *and* CBQP *are defined in a similar way.*

To perform a rewinding operator R to recover an intermediate state $|\psi\rangle$, a classical description $\mathcal{D}$ of $|\psi\rangle$ is neccessary. It can always be generated from $\tilde{\mathcal{D}}$ and measurement outcomes obtained before preparing $|\psi\rangle$. As in the case of BQP, computations performed to solve RwBQP problems can be written as uniform families of quantum circuits. A concrete circuit diagram of a RwBQP computation is given in Appendix A.

From Def. 9, we immediately obtain the following lemma:

▶ **Lemma 10.** RwBQP $\subseteq$ CBQP.

Proof. The only difference between RwBQP and CBQP is whether the rewinding or cloning operator is allowed. Since the cloning operator C can exactly simulate the rewinding operator R, this lemma holds. ◀

▶ **Definition 11** (AdPostBQP). *Let n be any natural number, ℓ be a polynomial in n, and $0 \leq s < c \leq 1$. A promise problem $L = (L_{\rm yes}, L_{\rm no}) \subseteq \{0,1\}^*$ is in* $\mathsf{AdPostBQP}(c,s)$ *if and only if there exists a polynomial-time deterministic Turing machine that receives 1^n as an input and generates a ℓ-bit description $\tilde{\mathcal{D}}$ of an operator Q_n such that it consists of a polynomial number of elementary gates in a universal gate set, single-qubit measurements in the computational basis, and single-qubit projectors $|1\rangle\langle 1|$ and satisfies, for the instance $x \in \{0,1\}^n$ and a polynomial m, that*

- *if* $x \in L_{\rm yes}$, $\left|\left|\left(|1\rangle\langle 1| \otimes I^{\otimes n+m+\ell-1}\right) \mathcal{N}[Q_n \left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)]\right|\right|^2 \geq c$
- *if* $x \in L_{\rm no}$, $\left|\left|\left(|1\rangle\langle 1| \otimes I^{\otimes n+m+\ell-1}\right) \mathcal{N}[Q_n \left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)]\right|\right|^2 \leq s$,

where $\mathcal{N}[\cdot]$ denotes the normalization of the vector in the square brackets. Here, "polynomial" is the abbreviation of "polynomial in n." Note that for $1 \leq i \leq n$, a projector $|1\rangle\langle 1|_i$ on the ith qubit can be applied only when a quantum state $|\psi\rangle$ to be applied satisfies

$$||(|1\rangle\langle 1|_i) |\psi\rangle||^2 \geq 2^{-p(n)} \tag{9}$$

for a polynomial $p(n)$ in n. Particularly, we denote $\mathsf{AdPostBQP}(2/3, 1/3)$ *as* $\mathsf{AdPostBQP}$.

Note that Q_n can include adaptive postselections because depending on previous measurement outcomes, we can decide whether X is applied before and after applying $|1\rangle\langle 1|$. Here, $X \equiv |1\rangle\langle 0| + |0\rangle\langle 1|$ is the Pauli-X operator. It is worth mentioning that it is unknown whether the adaptive postselection can be efficiently done in PostBQP as discussed in [2]. Indeed, if it is possible, SZK $\subseteq$ PP should be immediately obtained from the argument in [4, 5], while it is a long-standing problem. Eq. (9) can be automatically satisfied by using standard gate sets whose elementary gates involve only square roots of rational numbers. From Defs. 9 and 11, we notice that the main difference between RwBQP, CBQP, and AdPostBQP is whether the rewinding or cloning operators or projectors are allowed.

From Def. 11, we immediately obtain the following lemma:

▶ **Lemma 12.** AdPostBQP $\subseteq$ PSPACE.

Proof. The proof is essentially the same as that of BQP $\subseteq$ PSPACE [9]. The details are given in Appendix B. ◀

The following three corollaries also hold:

▶ **Corollary 13.** RwBQP*,* CBQP*, and* AdPostBQP *are closed under complement.*

▶ **Corollary 14.** $\mathsf{RwBQP} = \mathsf{RwBQP}(1-2^{-p(n)}, 2^{-p(n)})$*,* $\mathsf{CBQP} = \mathsf{CBQP}(1-2^{-p(n)}, 2^{-p(n)})$*, and* $\mathsf{AdPostBQP} = \mathsf{AdPostBQP}(1-2^{-p(n)}, 2^{-p(n)})$ *for any polynomial function $p(n)$ in the size n of a given instance x.*

▶ **Corollary 15.** RwBQP*,* CBQP*, and* AdPostBQP *are closed under composition.*

Since they are obvious from Defs. 9 and 11 and can be shown by using standard techniques, proofs are given in Appendix C.

In the rest of this section, we consider a relation between the rewinding, cloning, and postselection (i.e., RwBQP, CBQP, and AdPostBQP), and also obtain lower and upper bounds on them. More formally, we show the following theorem:

▶ **Theorem 16.** $\mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP} = \mathsf{CBQP} = \mathsf{AdPostBQP} \subseteq \mathsf{PSPACE}$.

Proof. This theorem can be obtained by showing (i) RwBQP $\subseteq$ CBQP; (ii) CBQP $\subseteq$ AdPostBQP; (iii) AdPostBQP $\subseteq$ RwBQP; (iv) $\mathsf{BQP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP}$, which immediately means $\mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{RwBQP}$ because $\mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{BQP}^{\mathsf{PP}}$; and (v) AdPostBQP $\subseteq$ PSPACE. The inclusions (i) and (v) are already shown in Lemmas 10 and 12, respectively. The remaining inclusions (ii), (iii), and (iv) will be shown in Lemma 17 and Corollary 19. ◀

To simplify our argument in proofs of Lemma 17 and Theorem 18, we particularly consider the universal gate set $\{X, CH, CCZ\} \cup \{H_k \mid k \in \mathbb{Z}, -p(|x|) \leq k \leq p(|x|)\}$ with a polynomial $p(|x|)$ in the instance size $|x|$ of a given problem. Here, $CH \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes H$ is the controlled-Hadamard gate, $CCZ \equiv |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$ is the controlled-controlled-Z (CCZ) gate, and H_k is the generalized Hadamard gate such that $H_k|0\rangle = (|0\rangle + 2^k|1\rangle)/\sqrt{1+4^k}$ and $H_k|1\rangle = (2^k|0\rangle - |1\rangle)/\sqrt{1+4^k}$. Therefore, H_0 is the ordinary Hadamard gate H, and hence, from [32], our gate set is universal. By using our universal gate set, we can make output probabilities of any Pauli-Z measurement in any polynomial-size quantum circuit 0 or at least $2^{-q(|x|)}$ for some polynomial $q(|x|)$. Due to this property, we can postselect any outcome for any polynomial-size quantum circuit [see Eq. (9)], which simplifies a proof of Lemma 17. Furthermore, by using this gate set, we can perform all quantum operations required in a proof of Theorem 18 without any approximation. Note that our argument can also be applied to other universal gate sets such as $\{H, T, CZ\}$ with $T \equiv |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$ by using the Solovay-Kitaev algorithm [16].

We show the second inclusion (ii) (for the proof, see Appendix D):

▶ **Lemma 17.** CBQP $\subseteq$ AdPostBQP.

As the first step to obtain inclusions (iii) and (iv), we show the following theorem:

▶ **Theorem 18.** RwBQP $\supseteq$ PP.

The proof is given in Appendix E.

From Theorem 18, we obtain the following corollary (for the proof, see Appendix H):

▶ **Corollary 19.** $\mathsf{BQP}^{\mathsf{PP}} \subseteq$ AdPostBQP $\subseteq$ RwBQP.

As the most important difference between the proof of Theorem 18 and that of PostBQP $\supseteq$ PP in [2], we have not used postselections of outputs whose probabilities are exponentially small by proposing the mitigation protocol (see Appendix E). To state the difference more explicitly on the technical level, we show the following corollary (for the proof, see Appendix I):

▶ **Corollary 20.** *For any polynomial function $p(|x|)$ in the size $|x|$ of an instance x,* PP $=$ PostBQP *holds even if only non-adaptive postselections of outputs whose probabilities are at least $1 - \Omega(1/p(|x|))$ are allowed.*

4 Restricted Rewindable Quantum Computation

In Sec. 3, a polynomial number of rewinding operators was available. If the number is restricted to a constant, the question is: how is the rewinding useful for universal quantum computation? We show that a single rewinding operator is sufficient to solve the following problem with a constant probability, which seems hard for universal quantum computation:

▶ **Definition 21** (Collision-finding Problem)**.** *Given the function family $\mathcal{F} \equiv \{f_K\}_{K\in\mathcal{K}}$ in Theorem 7 and a parameter K for $\mathcal{F}$, output a pair (x, x') with $x, x' \in \mathbb{Z}_q^n \times \chi^m \times \{0,1\}$ such that (i) $x \neq x'$ and (ii) $f_K(x) = f_K(x')$.*

▶ **Theorem 22.** *Assume that a rewinding operator can be applied in one step, and there is no polynomial-time quantum algorithm solving $\mathrm{SIVP}_{p(n)}$ for some polynomial $p(n)$ in n. Then, the problem in Def. 21 can be solved with probability of at least $\delta/2(1 - o(1))$ by uniformly generated polynomial-size quantum circuits with a single rewinding operator, but it cannot be achieved without rewinding operators. Here, the probability is taken over the uniform distribution on $\mathcal{K}$ and the randomness used in a quantum circuit to solve the problem.*

The proof is given in Appendix J.

We also show a superiority of a single rewinding operator under a different assumption. To this end, we use the statistical difference (SD) problem, which is SZK-complete [31], and show the following theorem:

▶ **Theorem 23.** *The SD problem defined in Def. 25 is in* $\mathsf{RwBQP}(1/2-2^{-O(n^c)}, 2\cdot 2^{-O(n^c)})(1)$, *where* n *and* c *are the problem size and some positive constant as defined in Def. 25.*

The proof is given in Appendix K. From Theorem 23, we obtain the following corollary:

▶ **Corollary 24.** *Let* $\mathsf{RwBQP}(1) \equiv \bigcup_{1/(c-s)\in \mathrm{poly}(|x|)} \mathsf{RwBQP}(c,s)(1)$ *for the set* $\mathrm{poly}(|x|)$ *of all polynomial functions in the size* $|x|$ *of an instance* x*. Then,* $\mathsf{RwBQP}(1) \supset \mathsf{BQP}$ *unless* $\mathsf{BQP} \supseteq \mathsf{SZK}$*.*

Proof. From Theorem 23, if $\mathsf{RwBQP}(1) \subseteq \mathsf{BQP}$, then $\mathsf{SZK} \subseteq \mathsf{BQP}$. ◀

The implication of Theorem 22 and Corollary 24 is given in Appendix L. As simple observations, in the full paper [23], we consider the computational capability of rewinding operators for two restricted classes of quantum circuits: Clifford and IQP circuits.

References

1 S. Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 635–642, 2002.

2 S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482, 2005.

3 S. Aaronson and A. Arkhipov. The computational complexity of linear optics. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, pages 333–342, 2011.

4 S. Aaronson, A. Bouland, J. Fitzsimons, and M. Lee. The space "just above" BQP, 2014. arXiv:1412.6507.

5 S. Aaronson, A. Bouland, J. Fitzsimons, and M. Lee. The space "just above" BQP. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 271–280, 2016.

6 D. S. Abrams and S. Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for *NP*-complete and # *P* problems. *Phys. Rev. Lett.*, 81(18):3992, 1998.

7 A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 474–483, 2014.

8 S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

9 E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

10 S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595–600, 2018.

11 A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019.

12 M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011.

13 M. J. Bremner, A. Montanaro, and D. J. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.*, 117(8):080501, 2016.

14 A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden. Qfactory: Classically-instructed remote secret qubits preparation. In *Proceedings of the 25th Annual International Conference on the Theory and Application of Cryptology and Information Security*, pages 615–645, 2019.

15 A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden. On the possibility of classical client blind quantum computing. *Cryptography*, 5(1):3, 2021.

16 C. M. Dawson and M. A. Nielsen. The solovay-kitaev algorithm. *Quantum Information and Computation*, 6(1):81–95, 2006.

17 K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani. Impossibility of classically simulating one-clean-qubit model with multiplicative error. *Phys. Rev. Lett.*, 120(20):200502, 2018.

18 X. Gao, S.-T. Wang, and L.-M. Duan. Quantum supremacy for simulating a translation-invariant ising spin model. *Phys. Rev. Lett.*, 118(4):040502, 2017.

19 D. Gottesman. The heisenberg representation of quantum computers. In *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1999.

20 C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex. Gaussian boson sampling. *Phys. Rev. Lett.*, 119(17):170501, 2017.

21 D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert. Anticoncentration theorems for schemes showing a quantum speedup. *Quantum*, 2:65, 2018.

22 A. W. Harrow and A. Montanaro. Quantum computational supremacy. *Nature*, 549(7671):203–209, 2017.

23 R. Hiromasa, A. Mizutani, Y. Takeuchi, and S. Tani. Rewindable quantum computation and its equivalence to cloning and adaptive postselection, 2022. arXiv:2206.05434.

24 A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph. Boson sampling from a gaussian state. *Phys. Rev. Lett.*, 113(10):100502, 2014.

25 J. Miller, S. Sanders, and A. Miyake. Quantum supremacy in constant-time measurement-based computation: A unified architecture for sampling and verification. *Phys. Rev. A*, 96(6):062320, 2017.

26 T. Morimae, K. Fujii, and J. F. Fitzsimons. Hardness of classically simulating the one-clean-qubit model. *Phys. Rev. Lett.*, 112(13):130502, 2014.

27 T. Morimae, Y. Takeuchi, and H. Nishimura. Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy. *Quantum*, 2:106, 2018.

28 T. Morimae, Y. Takeuchi, and S. Tani. Sampling of globally depolarized random quantum circuit, 2019. arXiv:1911.02220.

29 C. Peikert and V. Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *Proceedings of the 28th International Cryptology Conference*, pages 536–553, 2008.

30 O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 84–93, 2005.

31 A. Sahai and S. Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, 2003.

32 Y. Shi. Both toffoli and controlled-not need little help to do universal quantum computation, 2002. arXiv:quant-ph/0205115.

33 P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

34 Y. Takahashi, S. Tani, T. Yamazaki, and K. Tanaka. Commuting quantum circuits with few outputs are unlikely to be classically simulatable. *Quantum Information and Computation*, 16(3&4):251–270, 2016.

35 Y. Takeuchi and Y. Takahashi. Ancilla-driven instantaneous quantum polynomial time circuit for quantum supremacy. *Phys. Rev. A*, 94(6):062336, 2016.

36 D. Unruh. Computationally binding quantum commitments. In *Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 497–527, 2016.

37 J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

38 W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

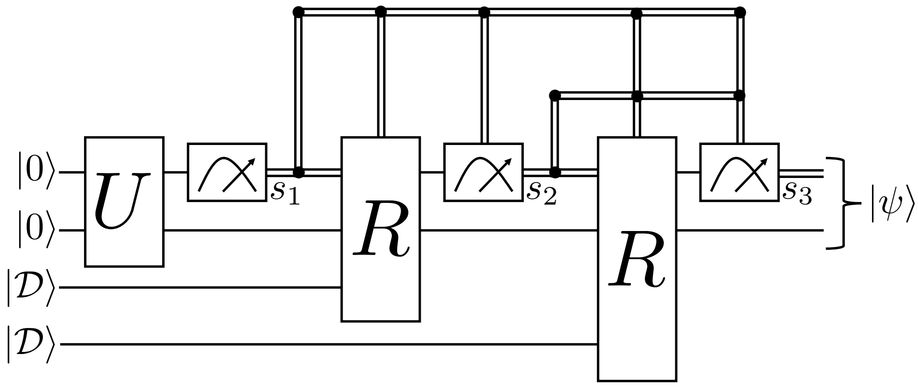

Figure 1 Concrete example of RwBQP computation. $\mathcal{D}$, U, R, and $|\psi\rangle$ are a classical description of $U|00\rangle$, a two-qubit unitary operator, the rewinding operator, and the output state, respectively. More precisely, when $U=\prod_i u_i$ for elementary quantum gates u_i in a universal gate set, $\mathcal{D}$ is a bit string representing $\prod_i u_i$. Note that since $|\psi\rangle$ is prepared by using only the unitary operator U, its classical description $\mathcal{D}$ does not include projectors and can be generated from only $\tilde{\mathcal{D}}$. Meter symbols represent the Pauli-Z measurements, and $s_i\in\{0,1\}$ is the ith measurement outcome for $1\leq i\leq 3$. We represent $|s_i\rangle$ as a classical bit s_i to emphasize that it can be copied. When the first measurement outcome s_1 is 1, the first rewinding operator R is applied. On the other hand, when $s_1=0$, we do not apply R, because the target state is obtained. Since the second and third measurements and the second rewinding operator are applied only when $s_1=1$, they are also conditioned on s_1. In a similar way, since it is not necessary to apply the second rewinding operator if $s_2=0$, the second rewinding operator and the third measurement are also conditioned on s_2. Finally, $|\psi\rangle$ becomes the target state when $s_1=0$, $(s_1,s_2)=(1,0)$, or $(s_1,s_2,s_3)=(1,1,0)$.

A Example of RwBQP Computation

Due to the addition of rewinding operators, it may be difficult to imagine quantum circuits used in RwBQP. To clarify them, as an example, we give a concrete circuit diagram for the following RwBQP computation. Suppose that we would like to prepare a two qubit state $(|0\rangle\langle 0|\otimes I)U|00\rangle$ (up to normalization) for a two-qubit unitary operator U. To this end, we use at most two classically controlled rewinding operators. More precisely, the rewinding operator R is applied if and only if the measurement outcome is 1. This computation can be depicted as a fixed quantum circuit in Fig. 1.

B Proof of Lemma 12

We give a proof of Lemma 12.

Proof. To show this lemma, it is sufficient to show that the acceptance probability

$$p_{\rm acc}=\left|\left|\left(|1\rangle\langle 1|\otimes I^{\otimes n+m+\ell-1}\right)\mathcal{N}[Q_n\left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)]\right|\right|^2 \tag{10}$$

can be computed in polynomial space. To this end, we use the Feynman path integral. Let k be some polynomial in n. By using q_i that is an elementary gate in a universal gate set, a single-qubit measurement in the computational basis, or a single-qubit postselection onto $|1\rangle\langle 1|$ for $1\leq i\leq k$, we can decompose $\mathcal{N}[Q_n(\cdot)]$ as $\mathcal{N}[Q_n(\cdot)]=\prod_{i=1}^k q_i(\cdot)$. Let $N\equiv n+m+\ell$.

Therefore,

$$\begin{aligned}&\left(|1\rangle\langle 1|\otimes I^{\otimes N-1}\right)\mathcal{N}[Q_n\left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)]\\ =&\left[|1\rangle\langle 1|\otimes\left(\sum_{d\in\{0,1\}^{N-1}}|d\rangle\langle d|\right)\right]q_k\left[\prod_{i=1}^{k-1}\left(\sum_{s^{(i)}\in\{0,1\}^N}|s^{(i)}\rangle\langle s^{(i)}|\right)q_i\right]|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle.\end{aligned} \tag{11}$$

Let s be a shorthand notation of a $(k-1)N$-bit string $s^{(1)}s^{(2)}\ldots s^{(k-1)}$. By defining

$$g(s,d)\equiv\langle 1|\langle d|\left[q_k\left(\prod_{i=1}^{k-1}|s^{(i)}\rangle\langle s^{(i)}|q_i\right)\right]|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle, \tag{12}$$

$p_{\rm acc}$ can be written as

$$\sum_{s,\tilde{s}\in\{0,1\}^{(k-1)N},d\in\{0,1\}^{N-1}} g(s,d)g^*(\tilde{s},d). \tag{13}$$

Sine q_i is just a constant-size matrix, each term $g(s,d)g^*(\tilde{s},d)$ can be computed in polynomial space[7]. Therefore, Eq. (13) can also be computed in polynomial space. ◀

C Proofs of Corollaries 13, 14, and 15

The proof of Corollary 13 is as follows:

Proof. Since proofs are essentially the same for all three classes, we only write a concrete proof for RwBQP. Let $\overline{L}$ be the complement of L. From Def. 9, when $x\in\overline{L}_{\rm yes}$ (i.e., $x\in L_{\rm no}$),

$$\left|\left|\left(|1\rangle\langle 1|\otimes I^{\otimes n+m+\ell-1}\right)\left(X\otimes I^{\otimes n+m+\ell-1}\right)Q_n\left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)\right|\right|^2\geq 2/3. \tag{14}$$

On the other hand, when $x\in\overline{L}_{\rm no}$ (i.e., $x\in L_{\rm yes}$),

$$\left|\left|\left(|1\rangle\langle 1|\otimes I^{\otimes n+m+\ell-1}\right)\left(X\otimes I^{\otimes n+m+\ell-1}\right)Q_n\left(|x\rangle|0^m\rangle|\tilde{\mathcal{D}}\rangle\right)\right|\right|^2\leq 1/3. \tag{15}$$

Therefore, coRwBQP $\subseteq$ RwBQP. By using the same argument, we can also show coRwBQP $\supseteq$ RwBQP and thus RwBQP $=$ coRwBQP. ◀

The proof of Corollary 14 is as follows:

Proof. Since proofs are essentially the same for all three classes, we only write a concrete proof for RwBQP. By repeating the same RwBQP computation m times and taking the majority vote on the outcomes, due to the Chernoff bound [8], the error probability is improved from $1/3$ to $2^{-q(m)}$ for a positive polynomial function $q(m)$ in m. Therefore, by setting m so that $q(m)\geq p(n)$, we obtain this corollary. ◀

The proof of Corollary 15 is as follows:

Proof. Since proofs are essentially the same for all three classes, we only write a concrete proof for RwBQP. From Def. 9, when a polynomial-time algorithm calls another polynomial-time algorithm as a subroutine, the resultant algorithm can still be realized in polynomial time. Since the RwBQP computation has some error probability, a remaining concern is that errors may accumulate every time polynomial-time algorithms are called. However, the accumulation of errors is negligible from Corollary 14. As a result, we obtain $\mathsf{RwBQP}^{\mathsf{RwBQP}}=\mathsf{RwBQP}$. ◀

[7] It may not be able to be computed in polynomial time, because q_i may be a measurement.

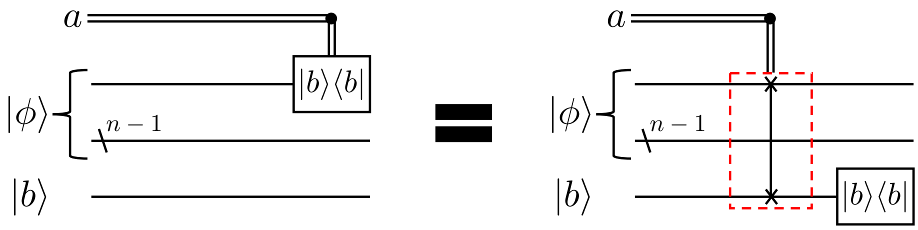

Figure 2 Replacement of a classically controlled projector with the classically controlled SWAP gate. $|\phi\rangle$ is a quantum state immediately before applying $P^{(i)} = |b\rangle\langle b|$, where $b \in \{0,1\}$. The SWAP gate is depicted as a vertical line enclosed by a dotted red rectangle. The projector $|b\rangle\langle b|$ and the SWAP gate is applied only when $a \in \{0,1\}$ is 1.

D Proof of Lemma 17

We give a proof of Lemma 17.

Proof. To obtain Lemma 17, it is sufficient to show that for any polynomial-size linear operator Q and its classical description $\mathcal{D}$, the cloning operator C can be simulated in quantum polynomial time by using the postselection. That is, our purpose is to perform the cloning operator C on the input state $|\mathcal{D}\rangle$. Let m be the number of Z-basis projective operators included in Q. By using n-qubit unitary operators $\{U^{(i)}\}_{i=1}^{m+1}$ and Z-basis projective operators $\{P^{(i)}\}_{i=1}^{m}$, $Q = U^{(m+1)}\prod_{i=1}^{m}(P^{(i)}U^{(i)})$. We can obtain the classical description $\mathcal{D}$ of Q by measuring the state $|\mathcal{D}\rangle$ in the Pauli-Z basis. The description $\mathcal{D}$ informs us about whether $P^{(i)}$ is $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$ and how to construct $U^{(i)}$ from $\{X, H_k, CH, CCZ\}$ for all i. Therefore, by using the postselection, we can prepare $Q|0^n\rangle$ (up to normalization) in quantum polynomial time. When we would like to apply $U^{(i)}$, we just apply it. On the other hand, when we apply $P^{(i)}$, we use the postselection. Since we assume the universal gate set $\{X, H_k, CH, CCZ\}$, the postselection is possible in any case. These efficient procedures simulate the non classically-controlled cloning operator C.

We next show that the above procedures can also be applied to simulate a classically controlled cloning operator. To this end, a classically controlled postselection is necessary. Suppose that when $a \in \{0,1\}$ is 1, we would like to apply the cloning operator C. On the other hand, when $a = 0$, we do not apply C. Note that without loss of generality, we can assume that C is controlled by a single bit a because C is applied or not. Only when $a = 1$, we must apply $P^{(i)}$ to simulate the classically controlled cloning operator. Let $P^{(i)} = |b\rangle\langle b|$ for $b \in \{0,1\}$. Such classically controlled $P^{(i)}$ can be simulated by adding an ancillary qubit $|b\rangle$ and applying the classically controlled SWAP gate as shown in Fig. 2. Classically controlled quantum gates are allowed in $\mathsf{AdPostBQP}$ computation because any classically controlled quantum gate can be realized by combining elementary quantum gates in a universal gate set. In conclusion, we obtain $\mathsf{CBQP} \subseteq \mathsf{AdPostBQP}$. ◀

E Proof of Theorem 18

We give a proof of Theorem 18.

Proof. We show Theorem 18 by replacing the postselection used in the proof of $\mathsf{PP} \subseteq \mathsf{PostBQP}$ in [2] with a polynomial number of rewinding operators. To this end, we consider the following PP-complete problem [2]: let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function computable in classical polynomial time, and $s \equiv \sum_{x\in\{0,1\}^n} f(x)$. Decide $0 < s < 2^{n-1}$ or $s \geq 2^{n-1}$. Note that it is promised that one of them is definitely satisfied.

To solve this problem with an exponentially small error probability using rewinding operators, first, we prepare

$$\sqrt{p}|\psi_t^{\perp}\rangle+\sqrt{1-p}|\psi_t\rangle, \tag{16}$$

where

$$p \equiv \frac{2\alpha^2(2^n-s)^2+\beta^2 4^n}{2[(2^n-s)^2+s^2]} \tag{17}$$

$$|\psi_t^{\perp}\rangle \equiv \frac{\sqrt{2}\alpha(2^n-s)|0\rangle+\beta 2^n|1\rangle}{\sqrt{2\alpha^2(2^n-s)^2+\beta^2 4^n}}\otimes|0\rangle \tag{18}$$

$$|\psi_t\rangle \equiv \frac{\sqrt{2}\alpha s|0\rangle+\beta(2^n-2s)|1\rangle}{\sqrt{2\alpha^2 s^2+\beta^2(2^n-2s)^2}}\otimes|1\rangle \tag{19}$$

for positive real numbers α and β such that $\alpha^2+\beta^2=1$ and $\beta/\alpha=2^k$, where k is an integer whose absolute value is upper bounded by n. As shown in Appendix F, this preparation can be done in quantum polynomial time with probability of at least $1-1/2^n$.

If the second qubit in Eq. (16) is projected onto $|1\rangle$, we can obtain

$$|\phi_{\beta/\alpha}\rangle \equiv \frac{\sqrt{2}\alpha s|0\rangle+\beta(2^n-2s)|1\rangle}{\sqrt{2\alpha^2 s^2+\beta^2(2^n-2s)^2}}. \tag{20}$$

Aaronson has shown that if n copies of $|\phi_{\beta/\alpha}\rangle$ can be prepared for all $-n\leq k\leq n$, then we can decide whether $0<s<2^{n-1}$ or $s\geq 2^{n-1}$ with an exponentially small error probability $p_{\rm err}$ in quantum polynomial time [2].

However, since p may be exponentially close to 1, the efficient preparation of Eq. (20) is difficult without postselection. We resolve this problem by using rewinding operators. Our idea is to amplify the probability of $|1\rangle$ being observed by mitigating the probability of $|0\rangle$ being observed. We propose the following mitigation protocol:

1. Set $i=0$ and $c=0$.
2. By using the state in Eq. (16), prepare
$$\sqrt{p_i}|\psi_t^{\perp}\rangle|+\rangle+\sqrt{1-p_i}|\psi_t\rangle|0\rangle, \tag{21}$$
where $p_0=p$, and measure the last register in the Pauli-Z basis. Let z be the measurement outcome. Furthermore, replace c with $c+1$.
3. Depending on the values of z, i, and c, perform one of following steps:
   a. When $z=0$, replace i with $i+1$, reset c to 0, and obtain
   $$\sqrt{p_{i+1}}|\psi_t^{\perp}\rangle+\sqrt{1-p_{i+1}}|\psi_t\rangle, \tag{22}$$
   where
   $$p_{i+1}=\frac{p_i}{2-p_i}. \tag{23}$$
   If $i+1<2n+3$, do step 2 by using the state in Eq. (22). On the other hand, if $i+1=2n+3$, output the state in Eq. (22) and halt the mitigation protocol.
   b. When $z=1$ and $c<3n$, apply the rewinding operator R and do step 2 again for the same i.
   c. When $z=1$ and $c=3n$, answer $0<s<2^{n-1}$ or $s\geq 2^{n-1}$ uniformly at random, and halt the mitigation protocol.

In this protocol, i and c count how many times the mitigation succeeds and how many times the mitigation fails for a single i, respectively. From Eq. (23),

$$\frac{1-p_{i+1}}{p_{i+1}}=2\frac{1-p_i}{p_i}, \tag{24}$$

and hence we succeed in mitigating the amplitude of the nontarget state $|\psi_t^{\perp}\rangle$.

From Appendix G,

$$\sqrt{p_{2n+3}}|\psi_t^\perp\rangle + \sqrt{1-p_{2n+3}}|\psi_t\rangle \tag{25}$$

is output with probability of at least $1-5n/8^n$. Since $(1-p_{2n+3})/p_{2n+3} = 2^{2n+3}(1-p)/p \geq 1$ as shown in Appendix G, we can obtain the outcome 1 with probability of at least 1/2 by measuring the second qubit in Eq. (25). If we obtain 0, we do the same measurement again by using the rewinding operator. Therefore, by repeating this procedure n times, we obtain the outcome 1 with probability of at least $1-1/2^n$. In total, with probability of at least

$$p_{\mathrm{suc}} \equiv \left[\left(1-\frac{1}{2^n}\right)^2\left(1-\frac{5n}{8^n}\right)\right]^{n(2n+1)}, \tag{26}$$

we obtain n copies of $|\phi_{\beta/\alpha}\rangle$ for all $-n \leq k \leq n$. As a result, we can correctly decide whether $0 < s < 2^{n-1}$ or $s \geq 2^{n-1}$ in polynomial time with probability of at least $p_{\mathrm{suc}}(1-p_{\mathrm{err}})$ that is exponentially close to 1. ◀

F Preparation of State in Eq. (16)

Although the procedure in this appendix has been proposed in [2], we explain it for the completeness of our paper. First, we prepare

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(H^{\otimes n}|x\rangle)|f(x)\rangle \tag{27}$$

in quantum polynomial time. Then, we measure all n qubits in the first register in the Pauli-Z basis. We repeat these procedures until we obtain the outcome 0^n or the repetition number reaches n. Since the probability[8] of 0^n being output in each repetition is at least 1/2, we can obtain at least one 0^n with probability of at least $1-1/2^n$. When the measurement outcome is 0^n, we obtain

$$|\psi\rangle \equiv \frac{(2^n-s)|0\rangle + s|1\rangle}{\sqrt{(2^n-s)^2+s^2}}. \tag{28}$$

From this state, for any positive real numbers α and β such that $\alpha^2+\beta^2=1$ and $\beta/\alpha = 2^k$, where k is an integer whose absolute value is upper bounded by n, we can prepare

$$CH[(\alpha|0\rangle+\beta|1\rangle)|\psi\rangle] = \alpha|0\rangle|\psi\rangle + \beta|1\rangle H|\psi\rangle = \sqrt{p}|\psi_t^\perp\rangle + \sqrt{1-p}|\psi_t\rangle \tag{29}$$

in quantum polynomial time.

G Success Probability of Our Mitigation Protocol

We show that the probability that the state in Eq. (25) is output in our mitigation protocol is at least $1-5n/8^n$ and that $(1-p_{2n+3})/p_{2n+3} \geq 1$. For clarity, we show a schematic diagram of our mitigation protocol in Fig. 3.

[8] In previous calculations [2, 6], this probability is lower bounded by 1/4. However, by calculating it more precisely, we tighten the lower bound.

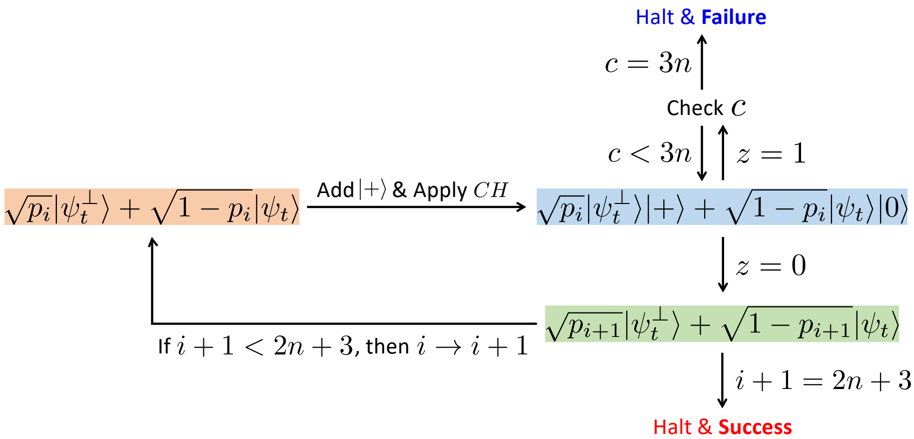

Figure 3 Schematic diagram of our mitigation protocol. **Failure** and **Success** indicate step (c) and the case that the state in Eq. (25) is output, respectively.

When the outcome 0 is obtained by measuring the last register of Eq. (21) in the Z basis, the amplitude of the nontarget state $|\psi_t^\perp\rangle$ is mitigated with the factor $1/\sqrt{2}$ (up to normalization) because

$$\left(I^{\otimes 2} \otimes \langle 0|\right)\left(\sqrt{p_i}|\psi_t^\perp\rangle|+\rangle + \sqrt{1-p_i}|\psi_t\rangle|0\rangle\right) = \sqrt{\frac{p_i}{2}}|\psi_t^\perp\rangle + \sqrt{1-p_i}|\psi_t\rangle. \tag{30}$$

Therefore, for any i, the probability q_i that the outcome 0 is obtained by measuring the last register of Eq. (21) in the Z basis is

$$q_i = \frac{p2^{-(i+1)} + (1-p)}{1-(1-2^{-i})p}, \tag{31}$$

where we have used $p_0 = p$. Therefore, for any i, the probability that we obtain 0 by measuring the last register of Eq. (21) in the Z basis before or at $c = 3n$ is

$$1-(1-q_i)^{3n} \geq 1-(1-q_0)^{3n} = 1-\left(\frac{p}{2}\right)^{3n}. \tag{32}$$

Our purpose is to sufficiently mitigate the amplitude of $|\psi_t^\perp\rangle$ so that we obtain the outcome 1 by measuring the second register of Eq. (22) in the Z basis with probability of at least $1/2$. To this end, it is sufficient to run our mitigation protocol until $i = N$ such that

$$\frac{1-p_N}{p_N} \geq 1. \tag{33}$$

From Eq. (24), this condition can be satisfied by setting

$$N = \left\lceil \log\left(\frac{p}{1-p}\right)\right\rceil. \tag{34}$$

By combining Eqs. (32) and (34), the probability that the state in Eq. (25) is output in our mitigation protocol (i.e., the probability of our mitigation protocol reaching to **Success** in Fig. 3) is at least

$$\left[1-\left(\frac{p}{2}\right)^{3n}\right]^N \geq 1-\left[\log\left(\frac{p}{1-p}\right)+1\right]\left(\frac{p}{2}\right)^{3n} \tag{35}$$

$$\geq 1-\left[\log\left(\frac{p}{1-p}\right)+1\right]\left(\frac{1}{2}\right)^{3n}. \tag{36}$$

Since $\log[p/(1-p)]$ is a monotonically increasing function of p in the range of $0<p<1$, the remaining task is to upper bound p. (Recall that our goal in this appendix is to show that Eq.(36) is lower bounded by $1-5n/8^n$ and $N \le 2n+3$.)

From the simple observation that $2[(2^n-s)^2+s^2]$, which is the denominator of p in Eq. (17), is a symmetric convex downward function that becomes minimum at $s=2^{n-1}$, and that $(2^n-s)^2$ in the numerator of p is a monotonically decreasing function in the range of $0<s\le 2^n$, the value of s maximizing p (for any α, β, and n) is between 1 and 2^{n-1}. To upper bound p, we separately consider three cases: (i) $1\le s\le(1-1/\sqrt{2})2^n$, (ii) $(1-1/\sqrt{2})2^n<s\le 2^{n-1}-1$, and (iii) $s=2^{n-1}$.

(i) When $1\le s\le(1-1/\sqrt{2})2^n$, the inequality $2(2^n-s)^2\ge 4^n$ holds. Therefore, from Eq. (17),

$$\begin{aligned} p &\le \frac{(2^n-s)^2}{(2^n-s)^2+s^2} && (37)\\ &\le \frac{(2^n-1)^2}{(2^n-1)^2+1} && (38)\\ &= 1-\frac{1}{(2^n-1)^2+1}. && (39)\end{aligned}$$

(ii) When $(1-1/\sqrt{2})2^n<s\le 2^{n-1}-1$, the inequality $2(2^n-s)^2<4^n$ holds, and hence

$$\begin{aligned} p &\le \frac{4^n}{2[(2^n-s)^2+s^2]} && (40)\\ &\le \frac{4^n}{2[(2^{n-1}+1)^2+(2^{n-1}-1)^2]} && (41)\\ &= 1-\frac{1}{4^{n-1}+1}. && (42)\end{aligned}$$

(iii) When $s=2^{n-1}$,

$$\begin{aligned} p &= \frac{\alpha^2}{2}+\beta^2 && (43)\\ &\le 1-\frac{1}{2(4^n+1)}, && (44)\end{aligned}$$

where we have used $2^{-n}\le\beta/\alpha\le 2^n$ and $\alpha^2+\beta^2=1$.

From Eqs. (39), (42), and (44), $p\le 1-1/[2(4^n+1)]\equiv p_{\max}$, and hence

$$N\le\log\frac{p}{1-p}+1\le\log\frac{p_{\max}}{1-p_{\max}}+1\le 2n+3. \tag{45}$$

This implies that Eq.(36) is lower bounded by

$$1-\left[\log\left(\frac{p_{\max}}{1-p_{\max}}\right)+1\right]\left(\frac{1}{2}\right)^{3n}\ge 1-\frac{2n+3}{2^{3n}}\ge 1-\frac{5n}{8^n}. \tag{46}$$

H Proof of Corollary 19

We give a proof of Corollary 19.

Proof. From Lemmas 10 and 17, it is sufficient to show $\mathsf{BQP}^{\mathsf{PP}}\subseteq\mathsf{RwBQP}$ and $\mathsf{AdPostBQP}\subseteq\mathsf{RwBQP}$ to obtain Corollary 19. First, we show the former inclusion. From Def. 9, it is obvious that any process in BQP can be simulated by a process in RwBQP in polynomial time. Furthermore, from Corollary 14 and Theorem 18, the PP oracle can be replaced with the RwBQP oracle. Therefore, from Corollary 15, $\mathsf{BQP}^{\mathsf{PP}}\subseteq\mathsf{RwBQP}^{\mathsf{RwBQP}}=\mathsf{RwBQP}$.

To obtain the latter inclusion, we show that each postselection can be simulated by rewinding operators. From Def. 11, each postselection (i.e., each projector) acts on a single qubit. Therefore, we can write a quantum state immediately before a postselection as $\alpha|0\rangle_p|\psi_0\rangle + \beta|1\rangle_p|\psi_1\rangle$ for some quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ and complex numbers α and β such that $|\alpha|^2 + |\beta|^2 = 1$. Here, the subscript p denotes the postselection register. Although $|\beta|^2$ may be exponentially small, the postselection onto $|1\rangle$ can be simulated by using our mitigation protocol. ◀

I Proof of Corollary 20

We give a proof of Corollary 20.

Proof. We can obtain Corollary 20 by slightly modifying our mitigation protocol and showing that it can be realized with non-adaptive postselections of outputs whose probabilities are at least $q \equiv 1 - \Omega(1/p(|x|))$. For some natural number m, we prepare

$$\sqrt{p}|\psi_t^\perp\rangle \left(\sqrt{q}|0\rangle + \sqrt{1-q}|1\rangle\right)^{\otimes m} + \sqrt{1-p}|\psi_t\rangle|0\rangle^{\otimes m} \tag{47}$$

instead of the state in Eq. (21). By postselecting m qubits in the second register onto $|0\rangle$ one by one, we obtain

$$\frac{\sqrt{pq^m}|\psi_t^\perp\rangle + \sqrt{1-p}|\psi_t\rangle}{\sqrt{1-p+pq^m}}. \tag{48}$$

These m postselections are non-adaptive ones of outputs whose probabilities are at least q. If the amplitude of $|\psi_t\rangle$ in Eq. (48) is at least $\sqrt{1/2}$, we can obtain $|\psi_t\rangle$ with at least a constant probability, and hence we can solve the PP-complete problem. Such the amplitude is realized by setting $m \geq \log\left[p/(1-p)\right]/\log\left(1/q\right)$. Since $\log\left[p/(1-p)\right]/\log\left(1/q\right) \leq 2(n+1)/\log\left(1/q\right) \leq 2(n+1)O(p(|x|))$ from Appendix G, where n is at most a polynomial function in $|x|$, a polynomial number of postselections are sufficient in the above argument. ◀

J Proof of Theorem 22

The proof of Theorem 22 is as follows:

Proof. To solve the problem in Def. 21 with a constant probability, we use the idea used in [14]. We prepare the state

$$\frac{\sum_{s\in\mathbb{Z}_q^n, e\in\chi^m, d\in\{0,1\}} |s,e,d\rangle|f_K(s,e,d)\rangle}{\sqrt{2q^n(2\mu+1)^m}}, \tag{49}$$

where $1/\sqrt{2q^n(2\mu+1)^m}$ is the normalization factor (see Theorem 7). When there exists a natural number N satisfying $2^N = 2q^n(2\mu+1)^m$, this preparation is trivially possible in quantum polynomial time with unit probability. If this is not the case, we prepare

$$\frac{\sum_{(s,e,d)\in\mathbb{Z}_q^n\times\chi^m\times\{0,1\}} |s,e,d\rangle|f_K(s,e,d)\rangle|1\rangle + \sum_{(s,e,d)\notin\mathbb{Z}_q^n\times\chi^m\times\{0,1\}} |s,e,d\rangle|0^{m\log q}\rangle|0\rangle}{\sqrt{2^{\tilde{N}}}} \tag{50}$$

with unit probability, where $\tilde{N}$ is the smallest natural number satisfying $2^{\tilde{N}} \geq 2q^n(2\mu+1)^m$. If we obtain the outcome 1 by measuring the third register in the computational basis, we can prepare the state in Eq. (49). From $2q^n(2\mu+1)^m > 2^{\tilde{N}-1}$, the probability of 1 being observed is larger than 1/2. Therefore, by repeating these procedures, we can obtain the outcome 1 at least once with probability of at least $1-o(1)$.

By measuring the second register in Eq. (49), we obtain a value of $f_K(s,e,d)$. From the δ-2 regularity of $\mathcal{F}$, the obtained output $f_K(s,e,d)$ has exactly two different preimages with probability of at least δ. When $f_K(s,e,d)$ has exactly two different preimages, the state of the first register becomes

$$\frac{|s,e,1\rangle + |s+s_0,e+e_0,0\rangle}{\sqrt{2}}, \tag{51}$$

where $f_K(s,e,1) = f_K(s+s_0,e+e_0,0)$. Then, we measure the state in Eq. (51) and obtain the values of $(s,e,1)$ or $(s+s_0,e+e_0,0)$.

To obtain the other one with probability 1/2, we would like to obtain the state in Eq. (51) again. It is possible by applying the rewinding operator R on $|s,e,1\rangle$ or $|s+s_0,e+e_0,0\rangle$ and a classical description[9] of the state in Eq. (51). As an important point, since the state in Eq. (51) becomes $|s,e,1\rangle$ or $|s+s_0,e+e_0,0\rangle$ by measuring only the last single qubit in the Z basis, a single rewinding operator is sufficient to rewind it.

On the other hand, if rewinding operator is not allowed, the probability of the problem being solved is super polynomially small from the collision resistance of the function family $\mathcal{F}$. ◀

K Proof of Theorem 23

In this proof, we use the statistical difference (SD) problem:

▶ **Definition 25** (Statistical Difference Problem [31]). *Given classical descriptions of two Boolean circuits $C_0, C_1 : \{0,1\}^n \to \{0,1\}^m$ with natural numbers n and m, let P_0 and P_1 be distributions of $C_0(x)$ and $C_1(x)$ with uniformly random inputs $x \in \{0,1\}^n$, respectively. Decide whether $D_{\mathrm{TV}}(P_0,P_1) < 2^{-O(n^c)}$ or $D_{\mathrm{TV}}(P_0,P_1) > 1-2^{-O(n^c)}$ for some positive constant c, where $D_{\mathrm{TV}}(\cdot,\cdot)$ is the total variation distance.*

We show that the $\mathsf{RwBQP}(1)$ machine can solve the SD problem with probabilities at least $1/2-2^{-O(n^c)}$ and $1-2\cdot 2^{-O(n^c)}$ when $D_{\mathrm{TV}}(P_0,P_1) < 2^{-O(n^c)}$ and $D_{\mathrm{TV}}(P_0,P_1) > 1-2^{-O(n^c)}$, respectively. To this end, we use an argument inspired by [5][10]. First, the $\mathsf{RwBQP}(1)$ machine prepares

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{b\in\{0,1\},x\in\{0,1\}^n} |b\rangle|x\rangle|C_b(x)\rangle. \tag{52}$$

By measuring the last register in the computational basis, it obtains the outcome $y \in \{0,1\}^m$ and

$$\frac{|0\rangle\left(\sum_{x:C_0(x)=y}|x\rangle\right) + |1\rangle\left(\sum_{x:C_1(x)=y}|x\rangle\right)}{\sqrt{2^n(P_0(y)+P_1(y))}}, \tag{53}$$

where for $b \in \{0,1\}$, $P_b(y) = |\{x \in \{0,1\}^n : C_b(x) = y\}|/2^n$ is the probability of C_b outputting y for uniformly random inputs $x \in \{0,1\}^n$. This event occurs with probability $(P_0(y)+P_1(y))/2$. Then, it measures the first register in Eq. (53) in the computational basis

9 More precisely, the classical description means a transcript of how to prepare the state in Eq. (51) from a tensor product of $|0\rangle$'s. Let V be a unitary that prepares the state in Eq. (49) from $|0\rangle$'s and ℓ be the number of qubits required in the first register in Eq. (49). Then, the classical description is $(I^{\otimes \ell} \otimes |f_K(s,e,d)\rangle\langle f_K(s,e,d)|)V$. Note that V can be decomposed into a polynomial number of elementary gates in a universal gate set.

10 As a difference between their argument in [5] and ours, we replace their non-collapsing measurement with a single rewinding operator and an ordinary (i.e., a collapsing) measurement. Furthermore, although they use three non-collapsing measurements, we can perform the rewinding operator only once.

and obtain the outcome $b_1 \in \{0,1\}$. By using a single rewinding operator, it can perform the same measurement again and obtain another outcome $b_2 \in \{0,1\}$. Finally, it outputs 1 if $b_1 \neq b_2$. Otherwise, it outputs 0.

We now calculate error probabilities, i.e., probabilities of the machine outputting 0 and 1 when $D_{\mathrm{TV}}(P_0, P_1) < 2^{-O(n^c)}$ and $D_{\mathrm{TV}}(P_0, P_1) > 1-2^{-O(n^c)}$, respectively. First, we consider the case of $D_{\mathrm{TV}}(P_0, P_1) < 2^{-O(n^c)}$. The probability p_{err} of the machine outputting 0, i.e., that of $b_1 = b_2$ is

$$p_{\mathrm{err}} = \sum_{y \in \{0,1\}^m} \frac{P_0(y) + P_1(y)}{2} \frac{P_0(y)^2 + P_1(y)^2}{(P_0(y) + P_1(y))^2}. \tag{54}$$

Let $\delta(y) \equiv \max\{P_0(y) - P_1(y), P_1(y) - P_0(y)\}$ and $P_{\min}(y) \equiv \min\{P_0(y), P_1(y)\}$. From Eq. (54),

$$p_{\mathrm{err}} = \frac{1}{2}\left(1 + \sum_{y \in \{0,1\}^m} \delta(y) \frac{P_{\min}(y) + \delta(y)}{2P_{\min}(y) + \delta(y)}\right) \leq \frac{1}{2}\left(1 + \sum_{y \in \{0,1\}^m} \delta(y)\right) < \frac{1}{2} + 2^{-O(n^c)}, \tag{55}$$

where we have used $\sum_{y \in \{0,1\}^m} \delta(y) = 2D_{\mathrm{TV}}(P_0, P_1)$ in the last inequality.

Then, we consider the case of $D_{\mathrm{TV}}(P_0, P_1) > 1 - 2^{-O(n^c)}$. The probability p'_{err} of the machine outputting 1, i.e., that of $b_1 \neq b_2$ is

$$p'_{\mathrm{err}} = \sum_{y \in \{0,1\}^m} \frac{P_0(y) + P_1(y)}{2} \frac{2P_0(y)P_1(y)}{(P_0(y) + P_1(y))^2}. \tag{56}$$

Since $D_{\mathrm{TV}}(P_0, P_1) > 1 - 2^{-O(n^c)}$, there exists a set S such that $\sum_{y \in S} P_0(y) \geq 1 - 2^{-O(n^c)}$ and $\sum_{y \in S} P_1(y) \leq 2^{-O(n^c)}$. Let $\bar{S}$ be a complement of S. From Eq. (56),

$$p'_{\mathrm{err}} = \sum_{y \in S} \frac{P_0(y)P_1(y)}{P_0(y) + P_1(y)} + \sum_{y \in \bar{S}} \frac{P_0(y)P_1(y)}{P_0(y) + P_1(y)} \leq \sum_{y \in S} P_1(y) + \sum_{y \in \bar{S}} P_0(y) \leq 2 \cdot 2^{-O(n^c)}, \tag{57}$$

where we have used $\sum_{y \in S \cup \bar{S}} P_0(y) = 1$ in the last inequality.

L Implication of Theorem 22 and Corollary 24

We first explain the implication of Theorem 22. In Sec. 3, we have shown the equivalence between the postselection and rewinding. In contrast, Theorem 22 may represent their difference. A possible approach to solving the problem in Def. 21 is to generate two copies of the state in Eq. (3) (more precisely, Eq. (51) in Appendix J) by using the postselection. As a straightforward way, this can be achieved by postselecting the second register in the state $\sum_x |x\rangle|f_K(x)\rangle$ (more precisely, Eq. (49) in Appendix J) onto the same $f_K(x)$. However, it requires the postselection of a polynomial number of qubits (or the postselection of states whose amplitudes are exponentially small), while a single qubit is sufficient for the rewinding. Furthermore, since we do not know which $f_K(x)$ has exactly two different preimages, the postselection applied to the second copy of $\sum_x |x\rangle|f_K(x)\rangle$ needs to be adaptive, i.e., it depends on $f_K(x)$ obtained from the first copy. On the other hand, a non-adaptive (i.e., non classically-controlled) rewinding operator is sufficient for solving the problem (with a constant probability). Although there may be other ways to solve the problem by using a non-adaptive postselection of a single qubit, the above discussion may imply that the rewinding is superior to the postselection in some situations where the number of qubits to be rewound or postselected is restricted, and copies (i.e., $(\sum_x |x\rangle|f_K(x)\rangle)^{\otimes 2}$) are not processed collectively.

We next explain a difference between Theorem 22 and Corollary 24. For example, by assuming that the decision version of SIVP, gapSIVP, is hard for universal quantum computation, Corollary 24 implies that a single rewinding operator is sufficient to achieve a task that is intractable for universal quantum computation. This is because the gapSIVP (with an appropriate parameter) is in SZK [29]. Therefore, Corollary 24 shows the superiority of a single rewinding operator for promise problems, while Theorem 22 shows it for the search problem.