

Analytical Lower Bound on Query Complexity for Transformations of Unknown Unitary Operations

Tatsuki Otake,¹ Satoshi Yoshida^{1,*} and Mio Murao^{1,2,†}

¹*Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan*

²*Trans-Scale Quantum Science Institute, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan*



(Received 10 November 2024; revised 22 September 2025; accepted 5 November 2025; published 5 December 2025)

Recent developments have revealed deterministic and exact protocols for performing complex conjugation, inversion, and transposition of a general d -dimensional unknown unitary operation using a finite number of queries to a black-box unitary operation. In this Letter, we establish analytical lower bounds for the query complexity of unitary inversion, transposition, and complex conjugation, which hold even if the input unitary is an unknown logarithmic-depth unitary. Specifically, our lower bound of d^2 for unitary inversion demonstrates the asymptotic optimality of the deterministic exact inversion protocol, which operates with $O(d^2)$ queries. We introduce a novel framework utilizing differentiation to derive these lower bounds on query complexity for general differentiable functions $f: \text{SU}(d) \rightarrow \text{SU}(d)$. As a corollary, we prove that a catalytic protocol—a new concept recently noted in the study of exact unitary inversion—is impossible for unitary complex conjugation. Furthermore, we extend our framework to the partially known setting, where the input unitary operation is promised to be within a subgroup of $\text{SU}(d)$ and the probabilistic setting, where transformations succeed probabilistically.

DOI: [10.1103/drp2-rzzw](https://doi.org/10.1103/drp2-rzzw)

Introduction—No-go theorems have played a vital role in the history of quantum information theory. The no-cloning theorem prohibits cloning of an *unknown* quantum state, and this property of quantum mechanics led to the invention of cryptographic primitives such as quantum key distribution [1,2]. Researchers have considered information processing tasks for unknown quantum states, such as broadcasting quantum information, and shown no-go theorems for these tasks. These no-go theorems play a complementary role to the go results, which are probabilistic or approximate protocols to implement transformations of unknown quantum states [3–5]. They provide an understanding of the nature of quantum states as an information carrier, which leads to ideas for implementing quantum protocols and establishes the foundation of quantum mechanics.

Recently, transformations of unknown *unitary operations*, which implement a unitary operation $f(U)$ using multiple queries to an unknown unitary operation U for a given function $f: \text{SU}(d) \rightarrow \text{SU}(d)$, have been extensively studied. Such a transformation is relevant for remote

quantum computing [6], quantum control [7], learning of quantum dynamics [8,9] and quantum functional programming [10]. One of the tasks in remote quantum computing is to perform $f(U)$ for a unitary operation U held by Charlie on a quantum state $|\psi\rangle$ held by David [6]. Alice has a blind access to a quantum state $|\psi\rangle$, Bob has a blind access to a unitary operation U , and Alice and Bob communicate quantum states to implement $f(U)|\psi\rangle$. In the quantum control, we can cancel out an unwanted Hamiltonian dynamics given by unitary operation U by implementing unitary inversion, which implements $f(U) = U^{-1}$ with multiple queries to U [7,11–20]. Beyond quantum control, unitary inversion also has an application in the measurement of the out-of-time-order correlators [8,9,21,22] and quantum singular value transformations [23–26]. In quantum functional programming, one would like to execute a unitary operation $f(U)$ for a quantum program representing U without looking into the detail of the quantum program. In these applications, the unknown nature of the input unitary is essential for ensuring both the *blindness* of the input and the *universality* of the algorithm.

Similarly to unknown quantum states, no-go theorems are known for several transformations of a unitary operation with a single query of the black-box unitary operation [11,27]. One way to circumvent this problem is to consider the algorithms using multiple queries of the black-box unitary operations. However, deterministic and exact transformations of unknown unitary operations were considered

*Contact author: satoshiyoshida.phys@gmail.com

†Contact author: murao@phys.s.u-tokyo.ac.jp

to be impossible with finite queries since implementing such transformations was believed to require exact knowledge about at least a part of the unknown unitary operations, namely, the exact value of at least one of the parameters of the unitary operation. To obtain such an exact value via process tomography [28–31], an infinite number of queries is necessary. Thus, many previous works focus on the investigation of go and no-go results of probabilistic or approximate transformations [6,7,11–17,27,32–43].

Contrary to intuition, recent works [18,19,44] have proven that deterministic and exact transformations of an unknown unitary operation to its complex conjugation, inversion, and transposition can be achieved with a *finite* number of queries of the black-box unitary operation. In addition, the existence of *catalytic transformations* was found for unitary inversion [18]. These discoveries suggest that these transformations of an unknown unitary operation can be achieved fully within a quantum regime with a finite number of multiple queries without extracting classical knowledge about the black-box unitary operation. That is, the queries served as a resource solely for transformation, not for extracting classical knowledge. Further, such a resource can be catalytic for some transformations. The lower bound of the number of queries characterizes the resource required for each transformation.

However, no-go theorems for deterministic and exact transformations for a d -dimensional unknown unitary operation are still missing in general, and thus, the analytic lower bounds were not established except for unitary complex conjugation for which the tight lower bound $d - 1$ is proven in [13], and nonlinear transformations such as unitary controlization, which requires an infinite number of queries. No-go theorems for parallel implementations are obtained for unitary transposition and inversion in Ref. [12], but showing no-go theorems for sequential implementations remains a hard task. Numerical lower bounds for unitary inversion and transposition are obtained to be 4 for $d = 2$ [18,45], but it is difficult to extend to general d due to the complexity of the problem. Regarding catalytic transformations, no condition for catalytic transformations for unknown unitary operations was known.

In this Letter, we provide a general framework for deriving no-go theorems for deterministic and exact transformations of a d -dimensional unknown unitary operation U given as a differentiable function $f(U)$ mapping to another d -dimensional unitary operation. From the no-go theorems, we obtain a lower bound of the required number of queries of the unitary operation to implement a function f deterministically and exactly in terms of semidefinite programming (SDP). Our lower bound is tight for unitary complex conjugation [$f(U) = U^*$] and asymptotically tight for unitary inversion [$f(U) = U^{-1}$]. Our lower bound also holds when the input unitary operation is an unknown logarithmic-depth unitary. We have also shown the relationship between the tightness of the SDP and the nonexistence

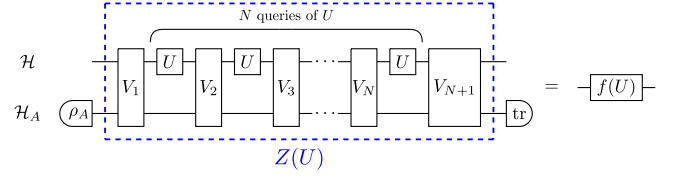


FIG. 1. Quantum circuit implementing deterministic and exact transformation $f(U)$ for a black-box unitary operation U with N queries to U , where ρ_A is a fixed state of the auxiliary system, and $V_1, \dots, V_{N+1}$ are unitary operations. $Z(U)$ is the unitary operation corresponding to the circuit without ρ_A and tracing out.

of catalytic transformations. Finally, we present extensions of our framework to relaxed requirements where the input unitary operation is partially known or the transformation is implemented exactly but probabilistically.

General lower bound for the query complexity of functions of unitary operations—Within a quantum computation model of quantum computation, a transformation $f(U)$ of a d -dimensional unknown unitary operation $U \in \text{SU}(d)$ to another unitary $f(U) \in \text{SU}(d)$ is deterministically and exactly possible with N queries of the black-box unitary operation U if such a transformation can be implemented by a fixed-order quantum circuit (also known as a quantum comb [46]) including N queries to U in the middle of the quantum circuit as shown in Fig. 1. We call the minimum number of the queries as the *query complexity* of f . If the deterministic and exact implementation of f is impossible with finite queries, the query complexity of f is defined as ∞ . When the query complexity of a function f is shown to be larger than or equal to a number N , then a no-go theorem forbidding deterministic and exact implementation of f with a query less than N is derived.

Note that in the context of the property testing, it is often considered the situation where the queries of U^{-1} and/or the controlled unitary operation $\text{ctrl-}U$ can also be applicable in addition to the queries of U [47,48]. However, the exact transformation of U to U^{-1} requires at least d^2 queries (as we will show in this Letter), and that of U to $\text{ctrl-}U$ is impossible with finite queries (query complexity ∞) [49] for an unknown U . We choose a setting that only the black-box unitary operation U can be used in the protocol to evaluate the query complexity of $f(U)$.

We first derive a lower bound of a query complexity of a *differentiable* function f . We call a function $f: \text{SU}(d) \rightarrow \text{SU}(d)$ is differentiable around $U_0 \in \text{SU}(d)$ if there exists a linear map $g_{U_0}: \mathfrak{su}(d) \rightarrow \mathfrak{su}(d)$ such that

$$f(e^{ieH}U_0) = f(U_0)e^{ieg_{U_0}(H)+O(\epsilon^2)} \quad \forall H \in \mathfrak{su}(d), \quad (1)$$

where $\mathfrak{su}(d)$ is given by $\mathfrak{su}(d) = \{H \in \mathcal{L}(\mathbb{C}^d) | \text{tr}(H) = 0, H = H^\dagger\}$. We define the Choi operator [50,51] of g_{U_0} by

$$J_{g_{U_0}} := \sum_{j=1}^{d^2-1} G_j^* \otimes g_{U_0}(G_j), \quad (2)$$

where $\{G_j\}_j$ is an orthonormal basis (in terms of the Hilbert-Schmidt inner product) of $\mathfrak{su}(d)$, and $*$ is the complex conjugation in the computational basis. Then, we show the following theorem on the query complexity of f .

Theorem 1—Given any differentiable function $f: \text{SU}(d) \rightarrow \text{SU}(d)$, the query complexity of f is at least the solution of the following SDP:

$$\begin{aligned} \min \quad & \text{tr } \beta_{U_0} \\ \text{s.t.} \quad & \beta_{U_0} \in \mathcal{L}(\mathbb{C}^d), \\ & J_{g_{U_0}} + \beta_{U_0} \otimes I \geq 0, \end{aligned} \quad (3)$$

where $J_{g_{U_0}}$ is defined in Eq. (2).

Proof sketch—Any fixed-order circuit transforming an arbitrary unitary U with N queries can be represented by the quantum circuit using unitary operations $V_1, \dots, V_{N+1}$ and a fixed state ρ_A of the auxiliary system, as shown in Fig. 1 [46]. We define the unitary operator $Z(U)$ as shown in Fig. 1. We choose $U = e^{i\epsilon H} U_0$ where $H \in \mathfrak{su}(d)$ is a Hermitian operator, ϵ is a real parameter, and U_0 is an arbitrarily unitary operator. By considering the differentiation of the unitary operator $Z(e^{i\epsilon H} U_0)$ in terms of ϵ around $\epsilon = 0$, we obtain $\mathcal{E}_{U_0}(H)$ represented by a linear map $\mathcal{E}_{U_0}$, which is a completely positive map defined by $V_1, \dots, V_{N+1}$ and satisfies $\mathcal{E}_{U_0}(I) = NI$. On the other hand, the differentiation of $f(e^{i\epsilon H} U_0)$ is determined by f as shown in Eq. (1). The equality for all $H \in \mathfrak{su}(d)$ identifies $\mathcal{E}_{U_0}$ up to some degree of freedom. When N is too small, the resulting $\mathcal{E}_{U_0}$ cannot be taken completely positive. Thus, the corresponding circuit with N queries to U does not exist, providing a no-go theorem. This validity condition of N is represented as the SDP constraints in Eq. (3). See Appendix A of Supplemental Material (SM) [52] for the details of the proof. ■

Since the proof of Theorem 1 relies on the differentiation, the lower bound of the query complexity shown in Theorem 1 holds even if we restrict the input unitary operation to be within the set $\{e^{iP_j\theta}\}_{\theta \in (-\epsilon, \epsilon), j}$ for a basis $\{P_j\}_j$ of $\mathfrak{su}(d)$ and a sufficiently small $\epsilon > 0$, but j and θ are unknown (see Appendix A of the SM [52] for the details). For n -qubit systems ($d = 2^n$), the set of Pauli operators $\{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$ is a basis of $\mathfrak{su}(d)$. The Pauli rotation $e^{iP_j\theta}$ can be implemented by a single-qubit X rotation, two multi-target-CNOT gates (or quantum fan-out gates), and two layers of single-qubit Clifford gates. Since the multi-target-CNOT gate can be implemented in depth $O(\log n)$ using the divide-and-conquer method [53], the query complexity lower bound in Theorem 1 also holds for the case where the input unitary operation is restricted to be

within the logarithmic-depth unitaries. By applying Theorem 1 to unitary inversion, transposition, and complex conjugation, we obtain the exponential hardness of these transformations for the logarithmic-depth n -qubit unitary operations.

Corollary 2—The query complexities of unitary inversion, transposition, and complex conjugation for the unknown logarithmic-depth n -qubit unitary are given by $\exp[\Theta(n)]$.

Proof sketch—The SDP in Theorem 1 yields $d^2 - 1$ for unitary inversion, $d + 1$ for unitary transposition, and $d - 1$ for unitary complex conjugation, i.e., the query complexities are given by $\exp[\Omega(n)]$ for n -qubit systems. These lower bounds are tight since the query complexities of these transformations for general n -qubit unitary operations are given by $\exp[O(n)]$ as shown in Refs. [18,19,44]. See Appendix A 4 of SM [52] for the details of the proof. ■

For the unitary inversion and transposition, we can further improve the lower bounds by considering an extra argument based on the fact that the conditions used for the derivation of the SDP should hold for *all* $U_0 \in \text{SU}(d)$, leading to the following corollary. See Appendix B of SM [52] for the details of the proof. Note that this corollary for the unitary inversion and transposition is not shown for the case when we restrict the input unitary operation to be within the logarithmic-depth unitaries.

Corollary 3—The query complexity of unitary inversion $[f(U) = U^{-1}]$, unitary transposition $[f(U) = U^T]$, and unitary complex conjugation $[f(U) = U^*]$ for $U \in \text{SU}(d)$ are lower bounded by

$$\begin{cases} d^2 & [f(U) = U^{-1}] \\ 4 & [f(U) = U^T, d = 2], \\ d + 3 & [f(U) = U^T, d \geq 3], \\ d - 1 & [f(U) = U^*]. \end{cases} \quad (4)$$

Comparison with previous works—Previously known analytical lower bounds were $d - 1$ for unitary inversion and 2 for unitary transposition [12]. They were obtained by the polynomial degree analysis or the Fourier series analysis. These lower bounds were strictly smaller than the minimum number of queries required to implement unitary inversion or transposition in the $d = 2$ case, which is numerically shown to be 4 for unitary inversion [18], and for unitary transposition [45].

Our lower bounds are tight at $d = 2$ and scale at the same rate $O(d^2)$ as the number of queries obtained by the recently discovered algorithm [19] for unitary inversion. Therefore, the analytical optimality of both the qubit-unitary inversion algorithm in [18], and the asymptotic optimality of the algorithm in [19] are obtained from our result. The unitary inversion algorithm in [19] can be modified to a unitary transposition algorithm by swapping U and U^* in the algorithm. By implementing U^* by using

TABLE I. Comparison of the lower bound of the query complexity of the deterministic and exact implementation of $f(U)$ for a d -dimensional unitary U obtained by Corollary 3 and the minimum number of queries achievable by the algorithms given in [18,19,44,45].

	Lower bound		Minimum known	
	Previous methods	Our method	$d = 2$	$d \geq 3$
$f(U) = U^{-1}$	4^a ($d = 2$ [18]), 6^a ($3 \leq d \leq 7$ [18]), $d - 1$ ($d \geq 8$ [12])	d^2	4^a [18]	$\sim(\pi/2)d^2$ [19]
$f(U) = U^T$	4^a ($d = 2$), 5^a ($d \geq 3$) [45]	$4(d = 2), d + 3(d \geq 3)$	4^a [45]	$\sim(\pi/2)d^2$ [19]
$f(U) = U^*$	$d - 1$ [12]	$d - 1$		$d - 1$ [44]

^aThese are the lower bounds obtained numerically.

$d - 1$ calls of U [44], the modified algorithm implements unitary transposition by using $O(d^2)$ queries of U . In contrast, our bound for unitary transposition scales only linearly on d , which indicates the possibility of an asymptotically more efficient algorithm.

We summarize the previously known lower bounds and the ones shown in Corollary 3, and minimum queries achieved by proposed algorithms in Table I for the deterministic and exact transformations, unitary inversion $f(U) = U^{-1}$, transposition $f(U) = U^T$, and complex conjugation $f(U) = U^*$. The lower bounds shown in Table I are not guaranteed to be tight in general. Nevertheless, they are tight in all three transformations for $d = 2$ and in unitary complex conjugation for general d . Our lower bound also gives a matching lower bound $\Omega(d^2)$ for unitary inversion achievable with $O(d^2)$ queries. This observation implies that our method potentially provides sufficiently tight bounds for certain types of f .

Necessary condition for the existence of catalytic transformation—In deterministic and exact unitary inversion for $d = 2$ [18], a novel property of “catalytic” transformation is observed. In short, the algorithm proposed in [18] implements unitary inversion U^{-1} using three queries to the black-box unitary U and one query to the “catalytic state,” which is generated using one query to U . While implementation of a single output of U^{-1} requires four queries in total, the same catalytic state is output in the auxiliary system (which is why the adjective “catalytic” is used), thus additional production of U^{-1} requires only three more queries to U . More generally, implementation of n copies of U^{-1} requires $3n + 1$ queries. Even though the catalytic property of unitary transformation algorithms enhances their applicability by reducing the asymptotic cost, we can show the nonexistence of optimal and catalytic algorithms for some transformations by following the theorem.

Theorem 4—When the SDP solution N of Eq. (3) is tight for a function f satisfying $f(U_0) = I$, then the optimal and catalytic algorithm for implementing f does not exist.

Proof—We show this theorem from Theorem 1 by comparing the derivative $g_{U_0}(H)$ in Eq. (1) for $U \mapsto f(U)$ and $U \mapsto f(U)^n$. Let us define $g'_1(H)$ and $g'_n(H)$ by $g_{U_0}(H)$ for $f(U)$ and $f(U)^n$, respectively. Using the product rule

(or the Leibniz rule) of differentiation, $g'_n(H)$ is expressed in terms of $g'_1(H)$ as

$$\begin{aligned}
 g'_n(H) &= -i \frac{d}{d\epsilon} \bigg|_{\epsilon=0} [f(U_0)^{-n} f(e^{i\epsilon H} U_0)^n] \\
 &= \sum_{k=0}^{n-1} f(U_0)^{-k} g'_1(H) f(U_0)^k \\
 &= n g'_1(H),
 \end{aligned} \tag{5}$$

thus the solution of the SDP given in Eq. (3) is nN for $f(U)^n$. If a catalytic transformation is possible, there exists a catalytic state that is prepared by the first run of the protocol and makes the further run of the protocol with M queries of the input unitary for $M < N$. Then, we can implement $f(U)^n$ with $N + (n - 1)M$ queries, which is smaller than nN and contradicts the SDP solution. ■

Theorem 4 shows that the optimal algorithm for unitary complex conjugation is not catalytic, since the lower bound $d - 1$ is tight for unitary complex conjugation. We also prove that the optimal algorithm for the unitary iteration $U \mapsto U^n$ for a positive integer n is not catalytic since the SDP solution for unitary iteration is n as shown in Appendix B of the SM [52], which is tight since the consecutive application of U for n times implements U^n . In contrast, the SDP solutions for unitary inversion and transposition ($d^2 - 1$ and $d + 1$, respectively) are strictly smaller than the numbers given by Corollary 3. Thus, they do not satisfy the assumption of Theorem 4 indicating the possibility of catalytic algorithms.

Extension of Theorem 1 to relaxed situations—Theorem 1 shows a lower bound of query complexity for a deterministic and exact implementation of a completely unknown unitary operation U . However, this situation may be too restricted in a realistic setting. For instance, partial information of U may be available, and probabilistic implementation may be enough for a practical application. We extend Theorem 1 to these relaxed situations.

We first consider the partially known situation where a partial information of U is given in terms of a Lie subgroup S of $SU(d)$, i.e., U is promised to satisfy $U \in S$. In this case, the linear map $\mathcal{E}_{U_0}$ is only determined on the Hamiltonian

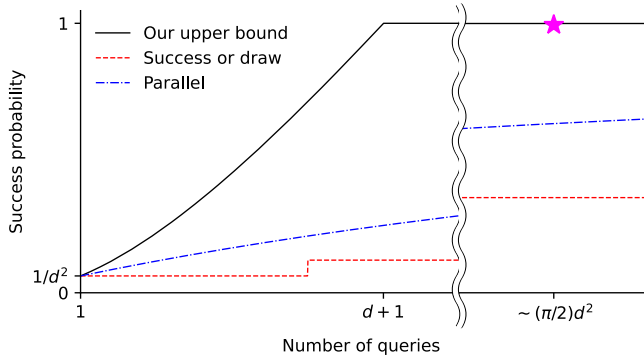


FIG. 2. Summary of upper (“Our upper bound”) and lower (other lines) bounds of the success probability of unitary transposition. “Our upper bound” shows the analytical solution of the SDP for the probabilistic transformation. “Success or draw” and “Parallel” refer to the lower bounds corresponding to the success probability of protocols given in Sec. E and Theorem 2 of [12], respectively. Magenta star shows the number of queries $\sim(\pi/2)d^2$ required in the deterministic exact transposition algorithm given by modifying the algorithm in [19].

H within its Lie algebra $\mathfrak{g}$ and consequently, the resulting SDP will have a solution that is smaller than or equal to the solution for the $SU(d)$ case. We give the SDP for this partially known situation and show a lower bound for implementing the unitary inversion in $SO(d)$, which is given by $d-1$ and tight for $d=2$. This suggests a possibility to reduce the query complexity by using a partial knowledge about the input unitary operation. See Appendix C of the SM [52] for the detail.

For the probabilistic situation, we provide a lower bound on query complexity to implement $f(U)$ with a success probability above $p(U)$ with a differentiable function $p: SU(d) \rightarrow \mathbb{R}_{\geq 0}$ in terms of SDP. We show the upper bound of the success probability of probabilistic exact unitary transposition given by

$$p_{\text{trans}}(U_0) \leq \left(\frac{d}{[(d^2-1)/N] + 1} \right)^2 \quad (6)$$

for an arbitrary $U_0 \in SU(d)$, as shown in Fig. 2. This upper bound reproduces the tight upper bound $1/d^2$ of the success probability $p(U)$ of unitary transposition for $N=1$, which is achieved by the gate teleportation-based algorithm [12]. In addition, this upper bound shows that the success probability $p(U_0)$ for a fixed number of queries tends to 0 in the limit of $d \rightarrow \infty$ for any N . Note that this upper bound is obtained only using the property of function $p(\cdot)$ in a neighbor of an arbitrary unitary U_0 , thus our lower bound holds even if we allow low success probability outside the neighbor of U_0 . See Appendix D of SM [52] for the details.

Conclusion—This work derives a lower bound for the query complexity of any differentiable function $f: SU(d) \rightarrow SU(d)$ in terms of SDP. This framework

shows the exponential hardness of unitary inversion, transposition, and complex conjugation even if the input n -qubit unitary is an unknown logarithmic-depth unitary. The lower bounds for unitary inversion and unitary transposition are tight for $d=2$ and asymptotically tight for unitary inversion. This framework also gives a necessary condition for a function f to have optimal and catalytic transformations of a unitary operation, which excludes the possibility of catalytic transformation for unitary complex conjugation. We also provide a generalization of our framework to partially known and probabilistic situations. Our Letter sets a line in between “what is possible” and “what is impossible” in transformation of unitary operations, which will serve as a guideline for improvement of existing protocols (e.g., unitary inversion [18,19]) by using partial knowledge about the input unitary operation or relaxing the protocols to be probabilistic ones.

This Letter introduces a new technique based on differentiation of unitary operations to analyze the query complexity of transformation of unitary operations (see Proof sketch of Theorem 1), which is also used in the concurrent work of the authors [54]. We believe that this technique has more applications in the analysis of query complexity. This Letter also opens up a new direction of research to extend this Letter as shown below. First, we can consider extending the SDP to cover higher-order differentiation of $Z(U)$ to obtain tighter bounds, whereas we only consider first-order differentiation of $Z(U)$ in this Letter. We can also consider a combination of our differentiation-based method with the polynomial degree-based method [12], which is used to prove the no-go results for probabilistic implementation of complex conjugation in less than $d-1$ queries, to obtain stronger no-go theorems. Our lower bound for unitary transposition does not match with the best-known query complexity given in Ref. [19]. We leave it a future work to investigate protocols achieving the query complexity given by lower bounds shown in this Letter.

Note added—Recently, Ref. [55] shows a lower bound on the query complexity of approximate unitary inversion using a different technique than ours.

Acknowledgments—We would like to thank David Trillo Fernández, Jisho Miyazaki, Marco Túlio Quintino, Jessica Bavaresco, Philip Taranto, Seiseki Akibue, and Hlér Kristjánsson for fruitful discussions. This work was supported by MEXT Quantum Leap Flagship Program (MEXT QLEAP) JPMXS0118069605, JPMXS0120351339, Japan Society for the Promotion of Science (JSPS) KAKENHI Grants No. 23K21643 and No. 23KJ0734, FoPM, WINGS Program, the University of Tokyo, DAIKIN Fellowship Program, the University of Tokyo, and IBM Quantum.

Data availability—No data were created or analyzed in this Letter.

- [1] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature (London)* **299**, 802 (1982).
- [2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [3] R. F. Werner, Optimal cloning of pure states, *Phys. Rev. A* **58**, 1827 (1998).
- [4] P. Agrawal and A. K. Pati, Probabilistic quantum teleportation, *Phys. Lett. A* **305**, 12 (2002).
- [5] V. Bužek and M. Hillery, Optimal manipulations with qubits: Universal quantum entanglers, *Phys. Rev. A* **62**, 022303 (2000).
- [6] Y. Yang, R. Renner, and G. Chiribella, Optimal universal programming of unitary gates, *Phys. Rev. Lett.* **125**, 210501 (2020).
- [7] M. Navascués, Resetting uncontrolled quantum systems, *Phys. Rev. X* **8**, 031008 (2018).
- [8] M. Gärttner, J. G. Bohnet, A. Safavi-Naini, M. L. Wall, J. J. Bollinger, and A. M. Rey, Measuring out-of-time-order correlations and multiple quantum spectra in a trapped-ion quantum magnet, *Nat. Phys.* **13**, 781 (2017).
- [9] J. Li, R. Fan, H. Wang, B. Ye, B. Zeng, H. Zhai, X. Peng, and J. Du, Measuring out-of-time-order correlators on a nuclear magnetic resonance quantum simulator, *Phys. Rev. X* **7**, 031011 (2017).
- [10] A. Bisio and P. Perinotti, Theoretical framework for higher-order quantum theory, *Proc. R. Soc. A* **475**, 20180706 (2019).
- [11] G. Chiribella and D. Ebler, Optimal quantum networks and one-shot entropies, *New J. Phys.* **18**, 093053 (2016).
- [12] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Probabilistic exact universal quantum circuits for transforming unitary operations, *Phys. Rev. A* **100**, 062339 (2019).
- [13] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Reversing unknown quantum transformations: Universal quantum circuit for inverting general unitary operations, *Phys. Rev. Lett.* **123**, 210502 (2019).
- [14] I. S. Sardharwalla, T. S. Cubitt, A. W. Harrow, and N. Linden, Universal refocusing of systematic quantum noise, *arXiv:1602.07963*.
- [15] M. T. Quintino and D. Ebler, Deterministic transformations between unitary operations: Exponential advantage with adaptive quantum circuits and the power of indefinite causality, *Quantum* **6**, 679 (2022).
- [16] D. Trillo, B. Dive, and M. Navascués, Translating uncontrolled systems in time, *Quantum* **4**, 374 (2020).
- [17] D. Trillo, B. Dive, and M. Navascués, Universal quantum rewinding protocol with an arbitrarily high probability of success, *Phys. Rev. Lett.* **130**, 110201 (2023).
- [18] S. Yoshida, A. Soeda, and M. Murao, Reversing unknown qubit-unitary operation, deterministically and exactly, *Phys. Rev. Lett.* **131**, 120602 (2023).
- [19] Y.-A. Chen, Y. Mo, Y. Liu, L. Zhang, and X. Wang, Quantum advantage in reversing unknown unitary evolutions, *arXiv:2403.04704*.
- [20] Y. Mo, L. Zhang, Y.-A. Chen, Y. Liu, T. Lin, and X. Wang, Parameterized quantum comb and simpler circuits for reversing unknown qubit-unitary operations, *npj Quantum Inf.* **11**, 32 (2025).
- [21] A. I. Larkin and Y. N. Ovchinnikov, Quasiclassical method in the theory of superconductivity, *Sov. Phys. JETP* **28**, 1200 (1969).
- [22] J. Maldacena, S. H. Shenker, and D. Stanford, A bound on chaos, *J. High Energy Phys.* **08** (2016) 106.
- [23] G. H. Low and I. L. Chuang, Optimal Hamiltonian simulation by quantum signal processing, *Phys. Rev. Lett.* **118**, 010501 (2017).
- [24] G. H. Low and I. L. Chuang, Hamiltonian simulation by qubitization, *Quantum* **3**, 163 (2019).
- [25] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (ACM, New York, 2019), pp. 193–204.
- [26] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, Grand unification of quantum algorithms, *PRX Quantum* **2**, 040203 (2021).
- [27] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Optimal cloning of unitary transformation, *Phys. Rev. Lett.* **101**, 180504 (2008).
- [28] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, *J. Mod. Opt.* **44**, 2455 (1997).
- [29] C. H. Baldwin, A. Kalev, and I. H. Deutsch, Quantum process tomography of unitary and near-unitary maps, *Phys. Rev. A* **90**, 012110 (2014).
- [30] J. Haah, R. Kothari, R. O’Donnell, and E. Tang, Query-optimal estimation of unitary channels in diamond distance, in *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2023), pp. 363–390.
- [31] Y. Yang, R. Renner, and G. Chiribella, Optimal universal programming of unitary gates, *Phys. Rev. Lett.* **125**, 210501 (2020).
- [32] Q. Dong, S. Nakayama, A. Soeda, and M. Murao, Controlled quantum operations and combs, and their applications to universal controllization of divisible unitary operations, *arXiv:1911.01645*.
- [33] A. Bisio, G. Chiribella, G. M. D’Ariano, S. Facchini, and P. Perinotti, Optimal quantum learning of a unitary transformation, *Phys. Rev. A* **81**, 032324 (2010).
- [34] M. Sedláč, A. Bisio, and M. Ziman, Optimal probabilistic storage and retrieval of unitary channels, *Phys. Rev. Lett.* **122**, 170502 (2019).
- [35] M. Sedláč and M. Ziman, Probabilistic storage and retrieval of qubit phase gates, *Phys. Rev. A* **102**, 032618 (2020).
- [36] A. Bisio, G. M. D’Ariano, P. Perinotti, and M. Sedláč, Optimal processing of reversible quantum channels, *Phys. Lett. A* **378**, 1797 (2014).
- [37] W. Dür, P. Sekatski, and M. Skotiniotis, Deterministic superreplication of one-parameter unitary transformations, *Phys. Rev. Lett.* **114**, 120503 (2015).
- [38] G. Chiribella, Y. Yang, and C. Huang, Universal superreplication of unitary gates, *Phys. Rev. Lett.* **114**, 120504 (2015).
- [39] M. Soleimanifar and V. Karimipour, No-go theorem for iterations of unknown quantum gates, *Phys. Rev. A* **93**, 012344 (2016).

- [40] D. Ebler, M. Horodecki, M. Marciniak, T. Mynik, M. T. Quintino, and M. Studziski, Optimal universal quantum circuits for unitary complex conjugation, *IEEE Trans. Inf. Theory* **69**, 5069 (2023).
- [41] M. Araújo, A. Feix, F. Costa, and Č. Brukner, Quantum circuits cannot control unknown operations, *New J. Phys.* **16**, 093026 (2014).
- [42] A. Bisio, M. Dall’Arno, and P. Perinotti, Quantum conditional operations, *Phys. Rev. A* **94**, 022340 (2016).
- [43] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Successor-draw: A strategy allowing repeat-until-success in quantum computation, *Phys. Rev. Lett.* **126**, 150504 (2021).
- [44] J. Miyazaki, A. Soeda, and M. Murao, Complex conjugation supermap of unitary quantum maps and its universal implementation protocol, *Phys. Rev. Res.* **1**, 013007 (2019).
- [45] D. Grinko and M. Ozols, Linear programming with unitary-equivariant constraints, *Commun. Math. Phys.* **405**, 278 (2024).
- [46] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Quantum circuit architecture, *Phys. Rev. Lett.* **101**, 060401 (2008).
- [47] A. Montanaro and R. D. Wolf, A survey of quantum property testing, *Theory Comput. Libr. Grad. Surv.* **7**, 1 (2016).
- [48] A. W. Harrow, C. Y.-Y. Lin, and A. Montanaro, Sequential measurements, disturbance and property testing, in *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, Pennsylvania, 2017), pp. 1598–1611.
- [49] Z. Gavorová, M. Seidel, and Y. Touati, Topological obstructions to quantum computation with unitary oracles, *Phys. Rev. A* **109**, 032625 (2024).
- [50] M.-D. Choi, Completely positive linear maps on complex matrices, *Linear Algebra Appl.* **10**, 285 (1975).
- [51] A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, *Rep. Math. Phys.* **3**, 275 (1972).
- [52] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/drp2-rzzw> for details.
- [53] M. Fang, S. Fenner, F. Green, S. Homer, and Y. Zhang, Quantum lower bounds for fanout, *Quantum Inf. Comput.* **6**, 46 (2006).
- [54] J. Bavaresco, H. Kristjánsson, M. Murao, T. Odake, M. T. Quintino, P. Taranto, and S. Yoshida, Simulating the quantum switch with quantum circuits is computationally hard, *Nat. Commun.* **16**, 10216 (2025).
- [55] K. Chen, N. Yu, and Z. Zhang, Tight bound for quantum unitary time-reversal, [arXiv:2507.05736](https://arxiv.org/abs/2507.05736).