# Topological obstructions to implementing controlled unknown unitaries

**Extended abstract**

Zuzana Gavorová[1], Matan Seidel[2], and Yonathan Touati[1]

[1] *School of Computer Science and Engineering, The Hebrew University of Jerusalem, Jerusalem, Israel*
[2] *School of Mathematical Sciences, Tel Aviv University, Tel Aviv, Israel*

## Introduction

Many important quantum algorithms make use of the quantum if clause, a primitive which given a unitary $U \in U(d)$ builds $control(U) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$. For example, the famous algorithms for factoring integers [Sho94], solving linear systems of equations [HHL09], solving semidefinite programs [BS17, VAGGdW20], or characterising quantum many-body systems [TOV+11, WBAG11] all use quantum phase estimation [Kit95, CEMM98], which, in turn, requires calls to $control(U)$. If a classical description of $U$ is available, as is the case in the fast algorithms mentioned above, there is the following general, implementation-independent way to build $control(U)$ from $U$: Given its classical description, find $U$'s decomposition to elementary gates and add a control to each of them, then run the controlled elementary gates to implement $control(U)$ [BBC+95].

It is a very natural question whether a quantum circuit can implement $control(U)$ when treating $U$ as an oracle [AK07]. One solution is immediately available; call $U$ sufficiently many times to apply process tomography [CN97, PCZ97], providing a classical description of $e^{i\alpha}U$ for some $\alpha \in [0, 2\pi]$ (the procedure must be insensitive to the global phase of $U$), then continue as described above - implementing $control(e^{i\alpha}U)$. Much simpler solutions exist in specific physical implementations; in optics [ZRK+11], computation with trapped ions [FDDB14] or superconducting qubits [FMKB15]. For example in optics, since the oracle gate $U$ occupies a certain physical space, an interferometer with polarising beamsplitters can control whether a photon passes through the gate $U$ or not depending on the polarisation degree of freedom. This implementation-dependent solution does not require measurements. We ask whether a unitary solution exists in a quantum circuit. Our answer is in the negative: A unitary quantum circuit implementing $control(e^{i\alpha}U)$ is impossible. Equivalently, in any quantum circuit with measurements that does implement $control(e^{i\alpha}U)$ (as the one corresponding to the process tomography approach), the measurements are necessary for disentangling the gained phase $\alpha$ from ancilla registers.

First we introduce the notion of *task* to simplify the discussion of preceding works and the formulation of our result. Several works studied the possibility of using oracle access to $U$ for implementing *functions* of $U$; the *control* function [AFCB14, TMVG18, DNSM19], but also complex conjugation [MSM19], transpose and inverse [QDS+19a, QDS+19b], raising $U$ to some fractional

power [SMM09, GSLW19], and more. In all these works, one is interested in viewing the access to the subroutines $U$ as an oracle access, and treating the process achieving the desired function of $U$, $t(U)$, as an algorithm. Treating subroutines $U$ as oracles has a great deal of flexibility; replacing the subroutines by different ones (different $U$'s) preserves the *functionality* of the algorithm (namely, the function $t$). Since the algorithm itself may be used as a subroutine, the $t(U)$ it should achieve is an *operator* - i.e. the algorithm should *implement* $t(U)$. At the same time, it makes sense to specify what ways to access the oracle $U$ are available to the algorithm. To this end we define:

**Definition 1 (Task).** A task is a pair $(t, \Sigma)$, where

1. The *task function* $t : U(d) \to L(\mathcal{H}_t)$ indicates that given an oracle $U \in U(d)$, we wish to implement the operator $t(U)$ to the *task Hilbert space*, $\mathcal{H}_t$.
2. The *query alphabet* $\Sigma$ is a set of functions on $U(d)$, such that if the oracle is $U \in U(d)$ and $\sigma \in \Sigma$, then the algorithm is allowed to query $\sigma(U)$. The set $\Sigma$ usually contains the identity $id : U \mapsto U$,

where $L(\mathcal{H})$ is the set of linear operators from the finite-dimensional Hilbert space $\mathcal{H}$ to itself.

Roughly, we say that an algorithm *exactly achieves* (*$\epsilon$-approximates*) the task $(t, \Sigma)$, if it exactly (approximately) implements $t(U)$ while accessing $U$ only via the functions in the query alphabet $\Sigma$. We distinguish worst-case algorithms, which implement $t(U)$ for all $U \in U(d)$, and average-case algorithms, which can fail for some $U \in U(d)$. All the algorithms we mention throughout this paper are worst-case unless we explicitly indicate otherwise.

We restate some of the previous works in this 'task' $(t, \Sigma)$ terminology. First of all, phase estimation is concerned with a task whose query alphabet contains *control*. Miyazaki et al. [MSM19] presented an algorithm for the task of complex conjugation $(t, \Sigma) = (U \mapsto U^*, \{id\})$. This was followed by algorithms by Quintino et al. [QDS$^+$19b, QDS$^+$19a] for transpose $(U \mapsto U^T, \{id\})$ and inversion $(inv : U \mapsto U^\dagger, \{id\})$. Sheridan et. al. [SMM09] presented the $q$-th power algorithm, an average-case algorithm achieving $(U \mapsto U^q, \{id, inv\})$ for any fixed $q \in \mathbb{R}$.

The specific question of implementing $control(U)$ for all $U \in U(d)$, and some variations of this question, have already been studied quite extensively before. Araújo et al. [AFCB14] and Thompson et al. [TMVG18] observed that the $(control, \{id\})$ task is impossible; any algorithm that can implement $control(U)$ from calls to $U$ is unphysical - if applied to the correct input and followed by the correct measurement, it would give a physical process distinguishing $U$ from $-U$, contradicting the fact that a difference in global phase is physically indistinguishable. Araújo et al. [AFCB14] asked about implementing control up to a global phase on $U$, i.e. about the task $(control_\phi, \{id\})$ with $control_\phi(U) = |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)} |1\rangle\langle 1| \otimes U$ for any real function $\phi$. They proved that with one call to $U \in U(2)$ this task is impossible for a quantum circuit. Dong et al. [DNSM19] found an algorithm for $(U \mapsto control_\phi(U^d), \{id\})$ for $d$ the dimension of $U$. Together with the $\frac{1}{d}$-th power algorithm of Sheridan et al. [SMM09] these two results compose to an algorithm for $(control_\phi, \{id, inv\})$. Unfortunately, due to its [SMM09] component, this algorithm fails for some $U \in U(d)$.

## Overview of Main Result

The main result of this paper is concerned with the worst-case achievability of the task c-$U$ := $(control_\phi, \{id, inv\})$. We generalise the impossibility of Araújo et al. [AFCB14] to oracles of any fixed dimension $d$, $U \in U(d)$ and to any finite number of $id$ and $inv$ queries, and show that for any

such unitary circuit c-$U$ is impossible. It remains impossible also if we add postselection, calling the resulting model *postselection oracle algorithm*. Most importantly, the impossibility holds even when one allows only approximate implementation of $control_\phi(U)$. We will compare this impossibility result to the above mentioned combination of the algorithms of Sheridan et al. [SMM09] and Dong et al. [DNSM19] which achieves the c-$U$ task for *most* $U$s. We will also contrast it with the process tomography strategy. To get our impossibility, we prove a stronger result, regarding a more general task: c-$U^m := (U \mapsto control_\phi(U^m), \{id, inv\})$ for $m \in \mathbb{Z}$. We phrase our result as a dichotomy theorem regarding the possibility of this task, as a function of the relation between $m$ and $d$:

**Theorem 1 (The Exact Dichotomy).** *Let $m \in \mathbb{Z}$ and let $d \in \mathbb{N}$ be the dimension of the oracle, $U \in U(d)$.*

- *If $d|m$ there exists a postselection oracle algorithm exactly achieving the task*

$$c\text{-}U^m := (U \mapsto |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)} |1\rangle\langle 1| \otimes U^m, \{id, inv\}),$$

  *for some $\phi : U(d) \to \mathbb{R}$.*
- *If $d \nmid m$ no such algorithm exists.*

Since the $m = 1$ case of the task c-$U^m$, is the task c-$U$, the following impossibility, which is our main result, follows from our Dichotomy theorem:

**Corollary 1 (Main: Impossibility of Controlled $U$).** *Exactly achieving the task c-$U$ is impossible in the postselection oracle algorithm model.*

The $d|m$ part of Theorem 1 is a corollary of Dong et al.'s [DNSM19] construction of the algorithm that achieves c-$U^d$. Our main contribution is the $d \nmid m$ direction, for which we prove the following topological lemma, closely related to the Borsuk-Ulam theorem [Bor33]:

**Lemma 1.** *Let $d \in \mathbb{N}$ and $m \in \mathbb{Z}$ such that there exists a function $f : U(d) \to S^1$ which is continuous and $m$-homogeneous, i.e. $f(\lambda U) = \lambda^m f(U)$ for each $\lambda \in S^1$. Then $m$ is a multiple of $d$.*

As we mentioned, our main result generalises for the approximate setting. In that case we require that the postselection oracle algorithm implements the operator $t(U) = |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)} |1\rangle\langle 1| \otimes U^m$ only approximately. We say that the postselection oracle algorithm $\epsilon$-*approximates* the task, if the algorithm's superoperator is within distance $\epsilon$ from the task superoperator $\rho \mapsto t(U)\rho t(U)^\dagger$. We need a new notion of distance, because the algorithm includes postselection - its output must be renormalised before comparing it to an output of the trace-preserving task superoperator. In our technical paper [Gav20] we define postselection equivalents of trace-induced distance and diamond distance and prove some inequalities we find useful. In the main paper we use them to get:

**Theorem 2 (The Approximate Dichotomy) (Roughly).** *Theorem 1 and Corollary 1 hold also when "exactly achieving" in their statement is replaced by "$\epsilon$-approximating" for any $\epsilon < \frac{1}{2}$.*

Our main result about c-$U^m$ affects other tasks; we prove corollaries about the transpose and the inversion tasks studied by Quintino et al. [QDS$^+$19a, QDS$^+$19b] and present a new proof, in addition to the existing proof of [SMM09], that any algorithm for the fractional power task must be average-case.

## References


[AFCB14] Mateus Araújo, Adrien Feix, Fabio Costa, and Časlav Brukner. Quantum circuits cannot control unknown operations. *New Journal of Physics*, 16(9):093026, 2014.

[AK07] Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 115–128. IEEE, 2007.

[BBC+95] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995.

[Bor33] Karol Borsuk. Drei sätze über die n-dimensionale euklidische sphäre. *Fundamenta Mathematicae*, 20(1):177–190, 1933.

[BS17] Fernando GSL Brandao and Krysta M Svore. Quantum speed-ups for solving semidefinite programs. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 415–426. IEEE, 2017.

[CEMM98] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, 1998.

[CN97] Isaac L Chuang and Michael A Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.

[DNSM19] Qingxiuxiong Dong, Shojun Nakayama, Akihito Soeda, and Mio Murao. Controlled quantum operations and combs, and their applications to universal controllization of divisible unitary operations. *arXiv preprint arXiv:1911.01645*, 2019.

[FDDB14] Nicolai Friis, Vedran Dunjko, Wolfgang Dür, and Hans J Briegel. Implementing quantum control for unknown subroutines. *Physical Review A*, 89(3):030303, 2014.

[FMKB15] Nicolai Friis, Alexey A Melnikov, Gerhard Kirchmair, and Hans J Briegel. Coherent controlization using superconducting qubits. *Scientific reports*, 5(1):1–11, 2015.

[Gav20] Zuzana Gavorová. Notes on distinguishability of postselected computations, 2020.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan 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*, pages 193–204, 2019.

[HHL09] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[Kit95] A Yu Kitaev. Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995.

[MSM19] Jisho Miyazaki, Akihito Soeda, and Mio Murao. Complex conjugation supermap of unitary quantum maps and its universal implementation protocol. *Physical Review Research*, 1(1):013007, 2019.

[PCZ97] JF Poyatos, J Ignacio Cirac, and Peter Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Physical Review Letters*, 78(2):390, 1997.

[QDS+19a] Marco Túlio Quintino, Qingxiuxiong Dong, Atsushi Shimbo, Akihito Soeda, and Mio Murao. Probabilistic exact universal quantum circuits for transforming unitary operations. *Physical Review A*, 100(6):062339, 2019.

[QDS+19b] Marco Túlio Quintino, Qingxiuxiong Dong, Atsushi Shimbo, Akihito Soeda, and Mio Murao. Reversing unknown quantum transformations: Universal quantum circuit for inverting general unitary operations. *Physical Review Letters*, 123(21):210502, 2019.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[SMM09] Lana Sheridan, Dmitri Maslov, and Michele Mosca. Approximating fractional time quantum evolution. *Journal of Physics A: Mathematical and Theoretical*, 42(18):185302, 2009.

[TMVG18] Jayne Thompson, Kavan Modi, Vlatko Vedral, and Mile Gu. Quantum plug n'play: modular computation in the quantum regime. *New Journal of Physics*, 20(1):013004, 2018.

[TOV+11] Kristan Temme, Tobias J Osborne, Karl G Vollbrecht, David Poulin, and Frank Verstraete. Quantum metropolis sampling. *Nature*, 471(7336):87–90, 2011.

[VAGGdW20] Joran Van Apeldoorn, András Gilyén, Sander Gribling, and Ronald de Wolf. Quantum sdp-solvers: Better upper and lower bounds. *Quantum*, 4:230, 2020.

[WBAG11] James D Whitfield, Jacob Biamonte, and Alán Aspuru-Guzik. Simulation of electronic structure hamiltonians using quantum computers. *Molecular Physics*, 109(5):735–750, 2011.

[ZRK+11] Xiao-Qi Zhou, Timothy C Ralph, Pruet Kalasuwan, Mian Zhang, Alberto Peruzzo, Benjamin P Lanyon, and Jeremy L O'brien. Adding control to arbitrary unknown quantum operations. *Nature communications*, 2(1):1–8, 2011.