Topological obstructions to implementing controlled unknown unitaries

Zuzana Gavorová, Matan Seidel, Yonathan Touati

HUJI

arXiv:2011.10031
arXiv:2011.08487

Outline

Introduction to the problem

Definitions

- Task
- Our model of computation

Main Result ← **Impossibility of controlled unknown unitary**

Proof of the topological lemma ← **Basic algebraic topology**

Insights ← **An interesting difference between two models**

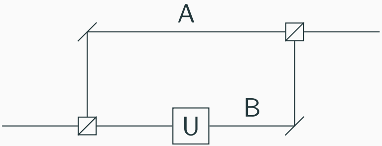
Outline

The problem

Given $U \in U(d)$ as a black-box implement
control$(U) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$

Background

- Implementation using Mach-Zehnder interferometer



$\boxslash : |H\rangle \leftrightarrow |A\rangle$
$|V\rangle \leftrightarrow |B\rangle$

✔ implements $|H\rangle\langle H| \otimes \mathbb{1} + |V\rangle\langle V| \otimes U$

✘ **not black-box!** - we know the oracle's location

The problem

Given $U \in U(d)$ as a black-box implement
$\textit{control}(U) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$

Background

- Implementation using Mach-Zehnder interferometer - **not black box**
- $\textit{control}(U)$ impossible [Ara+14; Tho+18]

assume $\textit{control}(U)$ possible

U	$\mathbb{1}$	$-\mathbb{1}$
$\textit{control}(U)$	$\mathbb{1}_{\text{control}} \otimes \mathbb{1}_{\text{target}}$	$Z_{\text{control}} \otimes \mathbb{1}_{\text{target}}$
$\textit{control}(U)\left(\lvert+\rangle \otimes \lvert v\rangle\right)$	$\lvert+\rangle \otimes \lvert v\rangle$	$\lvert-\rangle \otimes \lvert v\rangle$

but distinguishing $\mathbb{1}$ from $-\mathbb{1}$ is unphysical!

The problem

Given $U \in U(d)$ as a black-box implement
$\textit{control}(U) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$

Background

- Implementation using Mach-Zehnder interferometer - **not black box**
- $\textit{control}(U)$ impossible [Ara+14; Tho+18]

Change the task function

$\textit{control} : U(d) \to L(\mathcal{H}_t)$ to $\textit{control}_\phi : U(d) \to L(\mathcal{H}_t)$

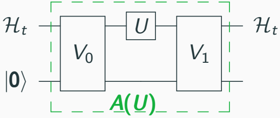
where $\textit{control}_\phi(U) = |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)} |1\rangle\langle 1| \otimes U$

The modified problem

Given $U \in U(d)$ as a black-box implement
control$_\phi$ $(U) = |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)}\, |1\rangle\langle 1| \otimes U$ for any real function ϕ

Further background

- *control*$_\phi(U)$ impossible from one use of U [Ara+14]



$\boldsymbol{A(U)} = V_1\,(U \otimes \mathbb{1})\,V_0$ linear in U

$\Rightarrow$ impossibility by linearity arguments

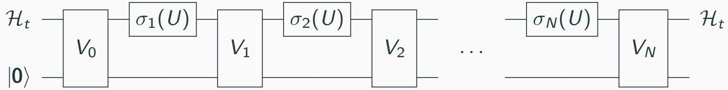
➜ multiple queries to U?

The modified problem

Given $U \in U(d)$ as a black-box implement
control$_\phi$ $(U) = |0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)} |1\rangle\langle 1| \otimes U$ for any real function ϕ

Further background

- *control*$_\phi(U)$ impossible from one use of U [Ara+14]
- process tomography? - **not *control*$_\phi$**
- *control*$_\phi(U)$ possible from queries to U^q, $q \in \mathbb{Q}$ [Don+19]



$\sigma_i \in \{U \mapsto U^q\}_{q \in \mathbb{Q}}$

Our problem

task function $U \mapsto$ ***control$_\phi$***(U)
query functions ***id*** $: U \mapsto U$, ***inv*** $: U \mapsto U^\dagger$

Outline

Implementing controlled unitary is a "Task"

Two kinds of operator functions

- task function $t : U(d) \to L(\mathcal{H}_t)$ we want to implement
- query function $\sigma_i : U(d) \to L(\mathcal{H}_i)$ we are allowed to assume, $\sigma_i \in \Sigma$

Definition

Task is a pair (t, Σ)

t task function

Σ query alphabet

Controlled unitary as a Task

? $(U \mapsto control_\phi(U), \{id, inv\})$

✔ $(U \mapsto control_\phi(U), \{U \mapsto U^q\}_{q \in \mathbb{Q}})$

✔ $(U \mapsto control_\phi(U^d), \{id\})$

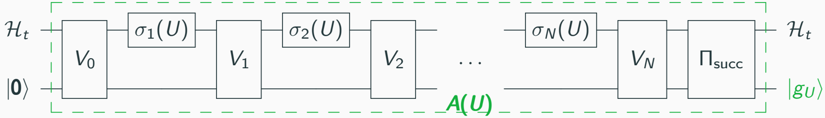
The generalised problem:

? Achieve a task **c-U^m**$=(U \mapsto control_\phi(U^m), \{id, inv\})$ for $m \in \mathbb{Z}$

Our model of computation

Postselection oracle algorithm

- any finite number of queries from $\mathbf{\Sigma}$
- unitary followed by a binary measurement $\{\mathbf{\Pi}_{\mathbf{succ}}, \Pi_{\text{fail}}\}$



- worst-case: $p_{\text{succ}}(U) = \| \, |g_U\rangle \, \|^2 > 0$ for all $U \in U(d)$
- represented by $\boldsymbol{A} : U(d) \to L(\mathcal{H}_t \otimes \mathcal{K})$

ϵ-approximate[1]

ϵ-approximates the task $(\boldsymbol{t}, \mathbf{\Sigma})$ if $\boldsymbol{A(U)} \, (\mathbb{1} \otimes |\mathbf{0}\rangle\langle\mathbf{0}|) \approx_\epsilon \boldsymbol{t(U)} \otimes |g_U\rangle\langle\mathbf{0}|$

for some nonzero $|g_U\rangle$

[1] ϵ measured by diamond norm if $p_{\text{succ}}(U) = 1$, for $p_{\text{succ}}(U) \neq 1$ see arXiv:2011.08487

Outline

The dichotomy $\quad$ $\text{c-}U^m = (U \mapsto control_\phi(U^m), \{id, inv\})$

Theorem

Let $d \in \mathbb{N}$ be the oracle dimension, $m \in \mathbb{Z}$, $\epsilon < \frac{1}{2}$

✔ if $d \mid m$ then **c-U^m** is

✘ if $d \nmid m$ then **c-U^m** is not

ϵ-approximable.

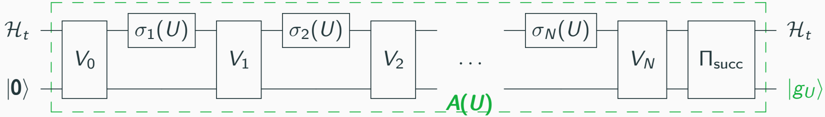
The Topological Lemma

Let $d \in \mathbb{N}$, $m \in \mathbb{Z}$. A continuous m-homogeneous function $U(d) \rightarrow S^1$ exists iff $d \mid m$.

$f(\lambda U) = \lambda^m f(U)$

proof of Theorem given The Topological Lemma

$\boldsymbol{A} : U(d) \rightarrow L(\mathcal{H}_t \otimes \mathcal{K})$ $\quad$ $\boldsymbol{A(U)} = \Pi_{\text{succ}} V_N (\sigma_N(U) \otimes \mathbb{1}) \dots V_1 (\sigma_1(U) \otimes \mathbb{1}) V_0$



Theorem

Let $d \in \mathbb{N}$ be the oracle dimension, $m \in \mathbb{Z}$, $\epsilon < \frac{1}{2}$

- ✔ if $d \mid m$ then **c-U^m** is
- ✘ if $d \nmid m$ then **c-U^m** is not

ϵ-approximable.

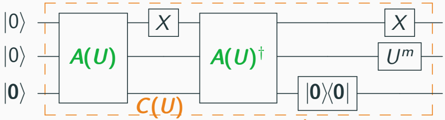
The Topological Lemma

Let $d \in \mathbb{N}$, $m \in \mathbb{Z}$. A continuous m-homogeneous function $U(d) \to S^1$ exists iff $d \mid m$.

proof of Theorem given The Topological Lemma

$A : U(d) \to L(\mathcal{H}_t \otimes \mathcal{K})$

- continuous, w-homogeneous
- $A(U)\,(\mathbb{1} \otimes |\mathbf{0}\rangle\langle\mathbf{0}|) = \left(|0\rangle\langle 0| \otimes \mathbb{1} + e^{i\phi(U)}\,|1\rangle\langle 1| \otimes U^m\right) \otimes |g_U\rangle\langle\mathbf{0}|$



continuous, m-homogeneous

$$f(U) := \frac{\langle\mathbf{0}|\, C(U)\, |\mathbf{0}\rangle}{\langle\mathbf{0}|\, A(U)^\dagger A(U)\, |\mathbf{0}\rangle}$$

Outline

Proof of the topological lemma

The Topological Lemma

Let $d \in \mathbb{N}$, $m \in \mathbb{Z}$. A continuous m-homogeneous function $U(d) \to S^1$ exists iff $d \mid m$.

The case of even d and odd m (i.e. when the function is odd) can be proven via **Borsuk-Ulam Theorem**

Proof of the topological lemma

The Topological Lemma

Let $d \in \mathbb{N}$, $m \in \mathbb{Z}$. A continuous m-homogeneous function $U(d) \to S^1$ exists iff $d \mid m$.

direct proof

$$t \in [0,1]$$

$$U(t) = e^{i2\pi t}\,\mathbb{1} \quad U'\left(\tfrac{j+\Delta}{d}\right) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & e^{i2\pi\Delta} & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \quad U''\left(\tfrac{j+\Delta}{d}\right) = \begin{pmatrix} e^{i2\pi\Delta} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

Outline

Insights

- ✘ $control_\phi(U)$ for all $U \in U(d)$ impossible even with postselection and **even approximately!** - in particular **via process tomography:**
  - ✔ process tomography approximates $control_{\phi_x}(U)$, $x \sim X$ where X set of "success" measurement outcomes, $|X| \geq 2$
  - ✘ cannot drop the x-dependence: cannot rotate continuously to a canonical phase ϕ follows from our topological lemma[2]
- **!** note that our **Postselection oracle algorithm** has one "success" outcome $\implies$ it cannot approximate $control_{\phi_x}(U)$, $x \sim X$

algorithm with measurement	$control_\phi$	$control_{\phi_x}$, $x \sim X$
$\{\mathbf{\Pi_{succ}}, \Pi_{fail}\}$	✘	✘
$\{\mathbf{\Pi_1}, \mathbf{\Pi_2} \ldots \mathbf{\Pi_{\lvert X \rvert}}, \Pi_{fail}\}$	✘	✔

[2] we thank an anonymous referee for noting another proof via $SU(d)/Z(SU(d))$ covering spaces.

References

[Ara+14] Mateus Araújo, Adrien Feix, Fabio Costa, and Časlav Brukner. "Quantum circuits cannot control unknown operations". In: *New Journal of Physics* 16.9 (2014), p. 093026.

[Don+19] Qingxiuxiong Dong, Shojun Nakayama, Akihito Soeda, and Mio Murao. "Controlled quantum operations and combs, and their applications to universal controllization of divisible unitary operations". In: *arXiv preprint arXiv:1911.01645* (2019).

[Gav20] Zuzana Gavorová. *Notes on distinguishability of postselected computations*. 2020. arXiv: 2011.08487 [quant-ph].

[GST20] Zuzana Gavorová, Matan Seidel, and Yonathan Touati. *Topological obstructions to implementing controlled unknown unitaries*. 2020. arXiv: 2011.10031 [quant-ph].

[Tho+18] Jayne Thompson, Kavan Modi, Vlatko Vedral, and Mile Gu. "Quantum plug n'play: modular computation in the quantum regime". In: *New Journal of Physics* 20.1 (2018), p. 013004.