Quantum circuits cannot control unknown operations

You may also be interested in:

Quantum circuits cannot control unknown operations

Mateus Araújo[1,2]**, Adrien Feix**[1,2]**, Fabio Costa**[1,2] **and Časlav Brukner**[1,2]

[1] Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria
[2] Institute of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria
E-mail: mateus.santos@univie.ac.at

Abstract
One of the essential building blocks of classical computer programs is the 'if' clause, which executes a subroutine depending on the value of a control variable. Similarly, several quantum algorithms rely on applying a unitary operation conditioned on the state of a control system. Here we show that this control cannot be performed by a quantum circuit if the unitary is completely unknown. The task remains impossible even if we allow the control to be done modulo a global phase. However, this no-go theorem does not prevent implementing quantum control of unknown unitaries in practice, as any physical implementation of an unknown unitary provides additional information that makes the control possible. We then argue that one should extend the quantum circuit formalism to capture this possibility in a straightforward way. This is done by allowing unknown unitaries to be applied to subspaces and not only to subsystems.

Keywords: quantum computation, quantum information, quantum algorithms

Quantum computation harnesses quantum effects to significantly outperform classical computation in solving specific problems. The most widely used model for quantum computation—referred to as the *quantum circuit model*—is formulated in terms of wires, representing quantum systems, which connect boxes, representing unitary operations [1]. The

formalism of quantum circuits is often considered as the standard language for describing quantum algorithms.

The difference between the classical and the quantum models of computation is not only in the computational complexity: quantum information processing differs in fundamental, and often counterintuitive, ways from classical computing. One of the most striking examples is the fact that it is impossible to produce a perfect copy of an unknown quantum state [2], whereas copying of classical information is a standard operation for classical computers.

Another standard operation in classical computer programs, usually expressed by an '**if**' clause, is the conditional execution of a part of the program depending on the value of a variable. A typical programming line of this kind has the form '**if** $x = 0$, **do** A', where A represents an arbitrary set of commands, i.e., a subroutine. Crucially, the construction of the **if** clause is independent of the subroutine A, allowing the latter to be used as a variable in the program.

The quantum analogue of the '**if**' clause is the control of a unitary operation U depending on the value of a control quantum bit (qubit). This is represented by the transformation

$$(\alpha \, | 0\rangle_C + \beta \, | 1\rangle_C) | \psi \rangle \mapsto \alpha \, | 0\rangle_C \, | \psi \rangle + \beta \, | 1\rangle_C \, U \, | \psi \rangle,$$

where the subscript C stands for the control qubit and $| \psi \rangle$ is the initial state of the target system. This control-U gate is a fundamental tool for quantum computation. It is used for example in Kitaev's phase estimation algorithm [3], Shor's factoring [4], Metropolis sampling [5], and in the deterministic quantum computing on the one qubit (DQC1) computing model [6].

The standard strategy to implement this gate in a quantum circuit is to decompose U into elementary gates, for which one knows how to add control [7]. This approach requires the unitary to be *known*, thus it cannot be used for solving problems in which the unitary itself is a variable. A genuine quantum analogue of the **if** clause would be an implementation of the control-U gate in which U can be treated as a blackbox. Although the knowledge that such a construction is impossible seems to be part of the folklore (e.g., it is mentioned *en passant* by Kitaev in [3]), there is no published proof to the best of our knowledge.

Classically, the control can be achieved by encoding the operation to be controlled as a bit string in the input, in what is known as the 'von Neumann' architecture, or a stored-program computer. In the quantum case, however, it is not possible to encode U as an input state, due to the no-programming theorem [8]; for this reason, computations in which U is a variable have to be considered as transformations of operations rather than states [9, 10].

Here we prove a no-go theorem that states the impossibility of controlling an arbitrary unknown unitary in the quantum circuit model, if the unitary is used only once. An immediate proof can be obtained by noticing that, in a quantum circuit, substituting U with $e^{i\varphi}U$ does not produce any physical difference, since the two circuits only differ by a global phase $e^{i\varphi}$. In contrast, control-U and control-$e^{i\varphi}U$ differ by a measurable relative phase. However, precisely because this global phase is not physical, it is not meaningful to demand that the control-U gate depends on it. Therefore, the proper question to ask is not whether one can build a control-U gate out of a blackbox U, but instead whether one can implement the gate control-$e^{iu}U$ for some phase factor e^{iu} that can in general depend on U. Note also that if one's goal in implementing the control-U is to measure the energy of a Hamiltonian such that $U = e^{iH}$ via phase estimation, the fact that this global phase is arbitrary is equivalent to the fact that one can apply an arbitrary shift to the spectrum of the Hamiltonian.

Formalising the question, we want to know whether there exists a quantum circuit that can implement the control-$e^{iu}U$ gate, given as input a single copy of the unknown $d \times d$ gate U. Thus we ask whether there exist unitaries A and B such that the following circuit identity is satisfied:
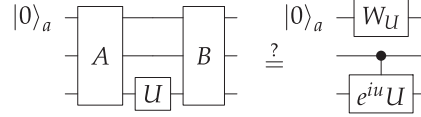
where the topmost line represents an additional a-dimensional quantum system (ancilla) and W_U is an arbitrary unitary on the ancilla, possibly depending on U. Note that the left hand side depicts the most general transformation that a quantum circuit can effect on U [11].

To translate this question into an equation, note that the matrix representation of the control-U operation is given by $\mathbb{1}_d \oplus U$. Defining $|U\rangle_a := W_U |0\rangle_a$, the question is whether the identity

$$B\left(\mathbb{1}_a \otimes \mathbb{1}_2 \otimes U\right)A |0\rangle_a = |U\rangle_a\left(\mathbb{1}_d \oplus e^{iu}U\right), \tag{1}$$

holds for some arbitrary phase factor e^{iu}, possibly depending on U. This is not possible, due to the nonlinearity of the transformation $U \mapsto \mathbb{1}_d \oplus e^{iu}U$. To see this, assume that equation (1) is valid for the qubit unitaries X, Z, and $H = \alpha X + \beta Z$, where X and Z are Pauli matrices, and α, β are non-zero real numbers such that $\alpha^2 + \beta^2 = 1$. One has then

$$B\left[\mathbb{1}_a \otimes \mathbb{1}_2 \otimes (\alpha X + \beta Z)\right]A|0\rangle_a = |H\rangle_a\left(\mathbb{1}_2 \oplus e^{ih}H\right). \tag{2}$$

Expanding the lhs by linearity and using equation (1) again we get

$$\alpha |X\rangle_a\left(\mathbb{1}_2 \oplus e^{ix}X\right) + \beta |Z\rangle_a\left(\mathbb{1}_2 \oplus e^{iz}Z\right) = |H\rangle_a\left(\mathbb{1}_2 \oplus e^{ih}H\right). \tag{3}$$

Taking the inner product with $|H\rangle_a$ in the ancilla subsystem gives us the equations

$$\alpha\langle H|X\rangle + \beta\langle H|Z\rangle = 1, \tag{4a}$$

$$\alpha\langle H|X\rangle e^{ix}X + \beta\langle H|Z\rangle e^{iz}Z = e^{ih}(\alpha X + \beta Z). \tag{4b}$$

Since X and Z are orthogonal, equation (4b) implies that $\langle H|X\rangle = e^{i(h-x)}$ and $\langle H|Z\rangle = e^{i(h-z)}$. Substituting into the equation (4a) we get that

$$e^{i(h-x)}\left(\alpha + \beta e^{i(x-z)}\right) = 1. \tag{5}$$

Taking the modulus squared of the equation shows us that $\cos(x-z) = 0$. Repeating these calculations for the matrices $\alpha X + \beta Y$ and $\alpha Y + \beta Z$, we also get the conditions $\cos(x-y) = 0$ and $\cos(y-z) = 0$; but this is a contradiction, since there exist no angles x, y, and z such that

$$\cos(x-z) = \cos(x-y) = \cos(y-z) = 0. \tag{6}$$

□

This shows that it is not possible to add control to a single copy of a blackbox unitary in the quantum circuit model, even modulo a global phase. However, it leaves open the possibility of controlling unitaries belonging to known, specific sets. For example, if one eigenvector of U and its eigenvalue are known, there is a circuit that performs the control [3]. In a similar vein, if one knows that U belongs to a given set of orthogonal unitaries, it is also possible to control it [12].
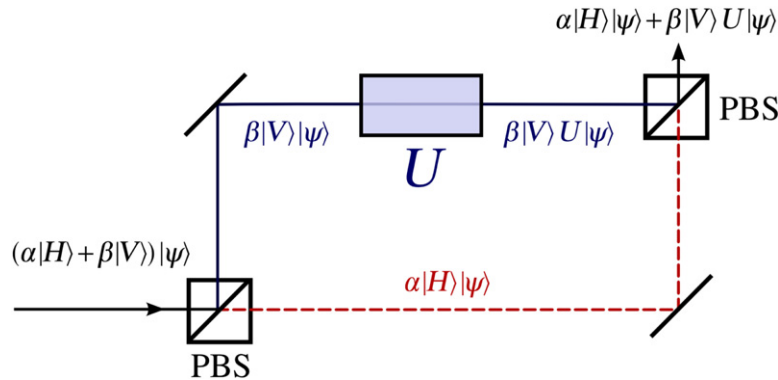
Figure 1. Interferometer that controls a qudit blackbox U. Here the control qubit is the polarization of the photon, and U acts on some additional degree of freedom of the same photon. The PBSs are polarizing beam splitters. A photon with polarization $|H\rangle$ takes the lower (red) path, while one with polarization $|V\rangle$ takes the upper (blue) path.

Furthermore, it is possible to have quantum control over classical operations on classical inputs. To see this, we restrict the target system $|\psi\rangle$ to be a classical bit string, i.e., to belong to the computational basis, and the unitary to be a classically allowed transformation U_{cl}, i.e., a permutation matrix. Then the following circuit implements the control-U_{cl}:
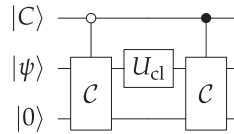
where $\mathcal{C}$ represents a classical cloning operation (a controlled-NOT for a two-level system). The symbol ─●─ means that the operation is applied if the control bit is $|1\rangle$ and ─○─ means that the operation is applied when the control bit is $|0\rangle$.

We will now show that our no-go theorem does not prevent quantum control of unknown operations from being performed in practice. In fact, control of blackbox quantum gates has been experimentally demonstrated [13–15]. In order to illustrate how this is possible, we propose here a simple interferometric setup, depicted in figure 1, that exploits a similar idea, but implements the control-U operation in a very direct way.

Consider a single photon in the state $(\alpha|H\rangle_C + \beta|V\rangle_C)|\psi\rangle$, where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states of the photon and $|\psi\rangle$ is the state of some other degree of freedom of the same photon (it could be its orbital angular momentum, a qudit of spatial or temporal bins, etc). Let then U be a unitary gate acting on this additional degree of freedom. It is straightforward to check that the interferometer in figure 1 applies the transformation

$$\left(\alpha\,|\,H\rangle_C + \beta\,|\,V\rangle_C\right)|\,\psi\rangle \mapsto \alpha\,|\,H\rangle_C\,|\,\psi\rangle + \beta\,|\,V\rangle_C U\,|\,\psi\rangle, \tag{7}$$

for any blackbox unitary U.

This interferometer is not scalable, since the whole Hilbert space is encoded in a single photon. One can, however, generalize it to a scalable implementation of a controlled n-qubit unitary, in which each qubit is encoded in a different photon, as shown in figure 2.

How does this interferometric implementation circumvent the no-go theorem we have just proved? The crucial point is the difference between the unitary matrix U that appears in a quantum circuit, and the physical device that implements it in the interferometer $U_{physical}$. While
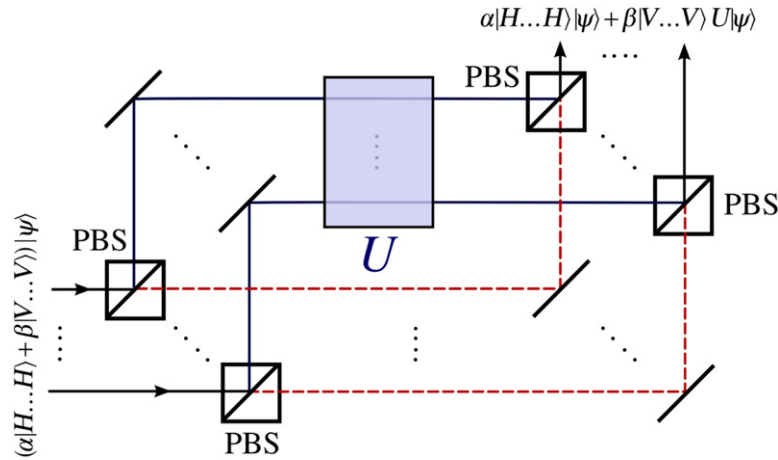
$$\alpha|H...H\rangle|\psi\rangle + \beta|V...V\rangle U|\psi\rangle$$

Figure 2. Scalable implementation of an *n*-qubit blackbox *U*. The control qubit is encoded in the polarization state of *n* photons as $\alpha \mid H\rangle^{\otimes n} + \beta \mid V\rangle^{\otimes n}$ (this can be prepared with a linear amount of elementary gates). Each photon goes through a different interferometer and *U* acts across the upper arms of all interferometers. The total number of PBSs required for this implementation is $2n$.

U is completely unknown, the *position* of the physical unitary is known, and therefore we know that it acts trivially on modes that do not pass through it. This knowledge is sufficient to control *U*, because when we extend the description of *U* to include this trivial subspace, we see that it is represented as $U_{\text{physical}} = \mathbb{1}_d \oplus U$, which is the control-*U* gate.

To be more explicit, let $\{\mid 0\rangle, ..., \mid d-1\rangle\}$ be a basis spanning the space in which *U* acts, and $\{\mid r\rangle, \mid b\rangle\}$ denote the red and blue paths. Then, in the basis $\{\mid r\rangle, \mid b\rangle\} \otimes \{\mid 0\rangle, ..., \mid d-1\rangle\}$, the physical operation is represented by

$$U_{\text{physical}} = \begin{pmatrix} \mathbb{1}_d & 0 \\ 0 & U \end{pmatrix},$$

which is exactly the matrix representation of the control-*U* gate. We stress again that *U* is still completely unknown, but the physical operation U_{physical} is not—some of its eigenvalues are known—and therefore the theorem does not apply to it.

This knowledge about a subspace in which the physical unitary acts trivially is not a particularity of this photonic implementation, but rather it must be present in any physical implementation of a quantum gate, since every physical operation acts non-trivially only on a limited region of space and time, and limited number of electronic or nuclear levels, frequency modes, and so on.

In general, knowing that the physical implementation of a unitary *U* acts trivially on a d'-dimensional subspace allows one to write it as $\mathbb{1}_{d'} \oplus U$; in fact, even a one-dimensional extension $1 \oplus U$ allows one to implement a control-*U* using the scheme of [3], because one eigenvector and the corresponding eigenvalue of $1 \oplus U$ are known.

This is similar to the implicit knowledge that physical operations only act on a limited number of *subsystems*. In the quantum circuit model, this is taken into account by adding additional wires, which correspond to the map $U \mapsto \mathbb{1} \otimes U$. Therefore, a natural way of accounting for the fact that physical operations act only on restricted *subspaces* would be to consider a generalized circuit model that allows extensions of the form $U \mapsto \mathbb{1} \oplus U$.

The above analysis applies when the unitary U has a direct interpretation as a physical evolution, so that it is natural to consider subsystems and subspaces on which the evolution acts trivially. This is not necessarily the case, for example, in schemes for fault-tolerant quantum computation [16] where computation is performed on a subspace of a physical system and a non-trivial encoding of logical unitaries in physical ones is needed.

Our results have profound implications for quantum algorithms that rely on estimating properties of unknown unitaries. Taking into account the fact that unitaries can be applied to subspaces, it becomes possible to use algorithms such as DQC1 trace estimation [6] and Kitaev's phase estimation [3] with unknown unitaries, which would be impossible in the quantum circuit framework. Note that, however, Kitaev's algorithm is not efficient when used on blackboxes, since it must compute the unitaries U^{2^k}, and this requires an exponential amount of copies of U. Additionally, it should be noted that there exist protocols that, although formulated in terms of control-U gates, can also be implemented without the control while accessing U as a blackbox [17, 18].

The scheme presented could also be used to simplify the implementation of the control-U gate even when the unitary in question is known, since adding control in the traditional way incurs a constant overhead [7] that, while irrelevant in complexity theory, is usually important for physical implementations. One concrete example would be using the setup of figure 1 to approximate the Jones polynomial with DQC1 [19].

In conclusion, we have proved a no-go theorem that shows that an unknown arbitrary unitary cannot be controlled in a quantum circuit, even modulo a global phase. This control is, however, possible for any physical implementation of a unitary transformation. This shows that the language of quantum circuits should be extended in order to capture all information processing possibilities allowed by quantum physics. Other extensions of the quantum circuit formalism have been proposed, in which the wires between gates can be in a superposition [20–22]. Allowing for such 'superpositions of circuits' can simplify the implementation of some information processing tasks [21, 22], or even reduce the computational complexity of some problems [23]. It is an intriguing open question whether further extensions are possible [24].

After this work was submitted, we became aware that similar results were obtained independently by Akihito Soeda [25], and related work was developed by Thompson *et al* [26].

Acknowledgments

References

[1] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3
[3] Kitaev A Y *Quantum Measurements and the Abelian Stabilizer Problem* (arXiv:quant-ph/9511026)

[4] Shor P 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Annual Symp. on Foundations of Computer Science* pp 124–34

[5] Temme K, Osborne T J, Vollbrecht K G, Poulin D and Verstraete F 2011 Quantum metropolis sampling *Nature* **471** 87–90

[6] Knill E and Laflamme R 1998 Power of one bit of quantum information *Phys. Rev. Lett.* **81** 5672–5

[7] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev.* A **52** 3457–67

[8] Nielsen M A and Chuang I L 1997 Programmable quantum gate arrays *Phys. Rev. Lett.* **79** 321–4

[9] Gutoski G and Watrous J 2006 Toward a general theory of quantum games *Proc. 39th ACM STOC* 565–74

[10] Chiribella G, D'Ariano G M and Perinotti P 2008 Quantum circuit architecture *Phys. Rev. Lett.* **101** 060401

[11] Chiribella G, D'Ariano G M and Perinotti P 2009 Theoretical framework for quantum networks *Phys. Rev.* A **80** 022339

[12] Bisio A, Perinotti P and Sedlák M in preparation

[13] Lanyon B P, Barbieri M, Almeida M P, Jennewein T, Ralph T C, Resch K J, Pryde G J, O'Brien J L, Gilchrist A and White A G 2009 Simplifying quantum logic using higher-dimensional Hilbert spaces *Nature Phys.* **5** 134–40

[14] Zhou X-Q, Ralph T C, Kalasuwan P, Zhang M, Peruzzo A, Lanyon B P and O'Brien J L 2011 Adding control to arbitrary unknown quantum operations *Nat. Commun.* **2** 413

[15] Zhou X-Q, Kalasuwan P, Ralph T C and O'Brien J L 2013 Calculating unknown eigenvalues with a quantum algorithm *Nature Photon.* **7** 223–8

[16] Gottesman D 2010 An introduction to quantum error correction and fault-tolerant quantum computation *Quantum Information Science and its Contribution to Mathematics: Proc. Symp. on Applied Mathematics 68* (Providence, RI: American Mathematical Society) pp 13–58

[17] Janzing D and Beth T 2002 Quantum algorithm for finding periodicities in the spectrum of a black-box Hamiltonian or unitary transformation *Quantum Inf. Comput.* **2** 192–7

[18] Sheridan L, Maslov D and Mosca M 2009 Approximating fractional time quantum evolution *J. Phys. A: Math. Gen.* **42** 185302

[19] Shor P W and Jordan S P 2008 Estimating Jones polynomials is a complete problem for one clean qubit *Quantum Inf. Comput.* **8** 681–714

[20] Chiribella G, D'Ariano G M, Perinotti P and Valiron B 2013 Quantum computations without definite causal structure *Phys. Rev.* A **88** 022318

[21] Chiribella G 2012 Perfect discrimination of no-signalling channels via quantum superposition of causal structures *Phys. Rev.* A **86** 040301

[22] Colnaghi T, D'Ariano G M, Facchini S and Perinotti P 2012 Quantum computation with programmable connections between gates *Phys. Lett.* A **376** 2940–3

[23] Araújo M, Costa F and Brukner Č Computational advantage from quantum-controlled ordering of gates (arXiv:1401.8127 [quant-ph])

[24] Oreshkov O, Costa F and Brukner Č 2012 Quantum correlations with no causal order *Nat. Commun.* **3** 1092

[25] Soeda A 2013 Limitations on quantum subroutine designing due to the linear structure of quantum operators *Talk at* International Conference on Quantum Information (ICQIT) (Tokyo, 16–18 January 2013)

[26] Thompson J, Gu M, Modi K and Vedral V Quantum computing with black-box subroutines (arXiv:1310.2927 [quant-ph])