Term Paper: Quantum circuits cannot control unknown operations (until circumvented)

Arnav Metrani - MS21254

January 2, 2025

Abstract

This is a review of the paper Quantum circuits cannot control unknown operations by Mateus Araújo et al. that will cover some of the prerequisites for understanding the work undertaken in the paper, as well as the paper itself. The paper itself discusses the following:
An "if" clause cannot be implemented in a quantum circuit if the action is unknown: The controlled gate version of an unknown unitary cannot be implemented in the quantum circuit formalism. This holds for control- $e^{i\phi}U$ gates as well. The paper then shows that this poses no problem in practical implementations, highlighting the need to extend the quantum circuit formalism to account for this in a straightforward manner.

0.1 Objective

The objective of the paper is to answer the following question: Is it possible to construct a fixed quantum circuit, such that if any arbitrary unitary gate is provided as input, the circuit will function as a controlled-U gate?

0.2 Workarounds

Before discussing why it is not possible (as alluded to in the abstract), we must first analyse if there exist any such quick-fix workarounds.

0.2.1 Why universal gate decomposition does not work

The decomposition method to create a controlled-U gate only works when we have a complete characterization of the unitary gate/its matrix representation. The method [1] described below will not work.

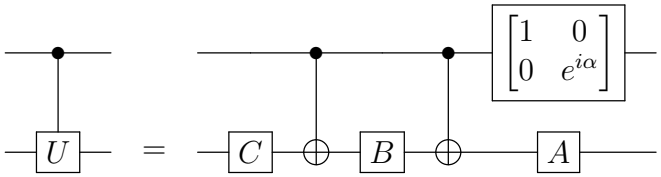


Figure 1: Circuit implementing the controlled-U operation for single qubit. α, A, B and C satisfy $U = \exp(i\alpha)AXBXC$, $ABC = \mathbb{I}$.

0.2.2 Why an unknown unitary gate cannot be stored and used

It is possible to do so quite easily in classical computing. We could store U (its description) as a bitstring in memory, and call it as required, based on the trigger.

One would believe this should be possible for quantum circuits as well; we provide all the information required for "building" the arbitrary unitary U via one set of registers, and the state it shall act on via another set. The "master" circuit will then map the first set of qubits to the intended unitary state, after which the operation will be carried out, giving us $U|\psi\rangle$.

The unitary matrix acting on m qubits is a $2^m \times 2^m$ matrix, so roughly 2^{2m} real numbers are needed to describe them, while the number of real numbers needed to represent a $2m$ qubit state is $2^{2m+1} - 1$.
Easy to do classically, it will be an $m2^m \to m2^m$ bit mapping.

This is prevented by the no-programming theorem. [2]

No-Programming Theorem

Nielsen et al. [2] define the fixed quantum circuit that stores and applies a unitary gate in the following manner:
Given an m-qubit data register $|d\rangle$ and an n-qubit program register $|P_U\rangle$ which maps to U, let us assume the existence of a fixed circuit (whose operations are defined by G) such that:

$$|d\rangle \otimes |P_U\rangle \to G[|d\rangle \otimes |P_U\rangle] \to U|d\rangle \otimes |P'_U\rangle$$

Right away, there are some concerns which we must first address:

The output program is independent of the data state:
If the input registers are allowed to be entangled, the unitary applied itself will change based on the data input, making it ill-defined.
We can show $|P'_U\rangle$ does not depend on $|d\rangle$ either:

$$G[|d_1\rangle \otimes |P_U\rangle] \to U|d_1\rangle \otimes |P'_{U_1}\rangle$$
$$G[|d_2\rangle \otimes |P_U\rangle] \to U|d_2\rangle \otimes |P'_{U_2}\rangle$$

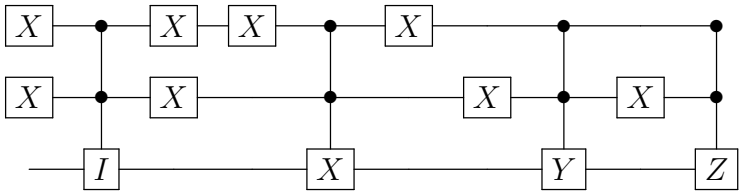
Taking inner product of both, we see that $\langle P'_{U_2}|P'_{U_1}\rangle = 1$ when $\langle d_2|d_1\rangle \neq 1$. We can do for orthogonal states as well by taking an extra state $|d_3\rangle$ that is non-orthogonal to both and using transitivity.

Proof of No-Programming Theorem

We show that for every distinct unitary operation that the fixed circuit must implement, the dimension of the program register must be increased by 1. We show this by proving that distinct unitaries must correspond to orthogonal states.

∞ distinct unitary gates, ∞ dimensional system, ∞ qubits. Impossible to implement, for every time the circuit is fixed, its input space must be expanded.

We first establish that a program register of dimension "n" can deterministically implement "n" distinct unitary operations (ignoring global phase) on the data register via control gates. We do this by simply showing such a construction: Eg. for $n = 4$:



(Expanded for simplicity. First two qubits correspond to the program register. Description allows one to implement unitary operators depending on the state of the program register, thus making it one possible implementation of the fixed circuit.)

Next, we postulate that any such satisfactory fixed circuit is a *deterministic* implementation and implements $\{U_1, U_2, ..., U_n\}$. Then the program register is atleast n dimensional ($log_2(n)$) qubits. The corresponding program states $\{|P_{U_1}\rangle, ..., |P_{U_n}\rangle\}$ are orthogonal.

We prove this via contradiction.

Let us assume that the above postulate does not hold. Let $|P\rangle$ and $|Q\rangle$ implement U_P and U_Q which are distinct, but the states themselves are not orthogonal.

$$G[|d\rangle \otimes |P_U\rangle] \rightarrow U_P|d\rangle \otimes |P'\rangle$$
$$G[|d\rangle \otimes |P_Q\rangle] \rightarrow U_Q|d\rangle \otimes |Q'\rangle$$

Taking inner product:

$$\langle Q|P\rangle = \langle Q'|P'\rangle\langle d|U_Q^\dagger U_P|d\rangle$$

Assume $\langle Q'|P'\rangle \neq 0$. Then the following must hold:

$$\frac{\langle Q|P\rangle}{\langle Q'|P'\rangle} = \langle d|U_Q^\dagger U_P|d\rangle$$

LHS is not dependent on $|d\rangle$ (as seen before), so RHS must be a constant value.
RHS can only be constant if $U_Q^\dagger U_P = \text{constant} * \mathbb{I}$
But this contradicts our initial condition that U_P and U_Q are distinct. So, the only other resolution is to say that our initial assumption $\langle Q'|P'\rangle \neq 0$ is wrong. (We arrive at this conclusion since one is a given condition, and the other is a postulate.)

From this, the rest follows. A fixed circuit will have to implement an infinite number of unitary gates. This would require it to be able to take an infinite number of orthogonal states as input, which is impossible for a fixed circuit.

0.2.3 A probabilistic implementation is possible

Quite curiously, a probabilistic implementation is possible!

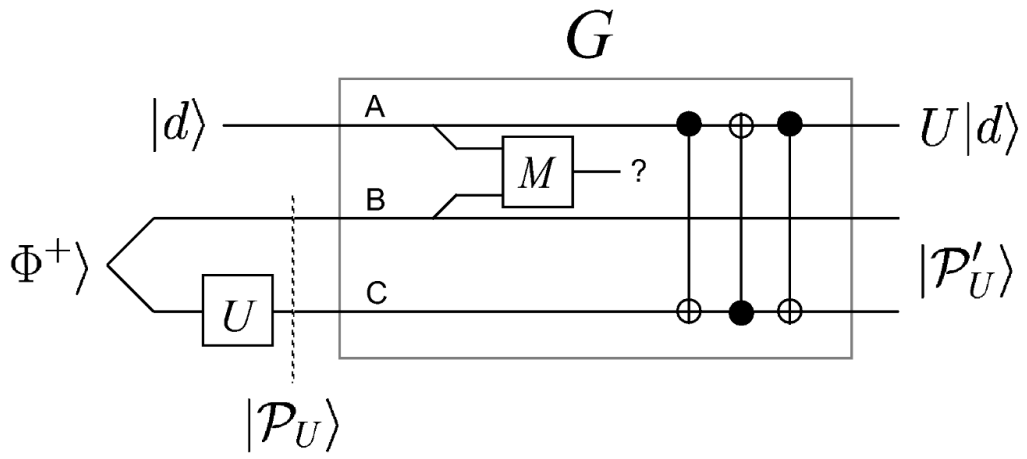


Figure 2: Implementation for a 1-qubit input unitary.

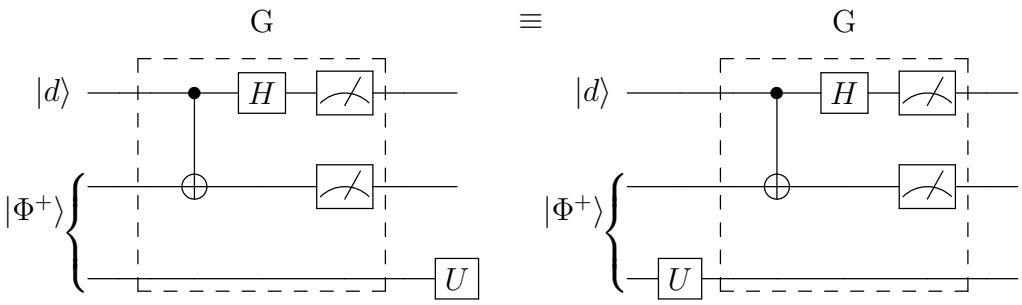
The following procedure has only been described for $m = 1$ qubits, but a generalization is possible.
The above programmable quantum gate array functions as follows: The data qubit upon which the unitary is applied is $|d\rangle$. The Bell state $|\Phi^+\rangle$ is prepared, of which one is passed as input to the unitary. The data qubit and the remaining Bell state qubit are jointly measured. In the end, we perform a SWAP operation between the data qubit and the Bell state qubit on which the unknown unitary acts.
It is straightforward to see $|P_U\rangle = \frac{|0\rangle U|0\rangle + |1\rangle U|1\rangle}{\sqrt{2}}$. This will be the state that will effectively encode U into the gate array G.
If we define the data qubit as $|d\rangle = \alpha|0\rangle + \beta|1\rangle$, through algebraic manipulation we can see the following:

$$[\alpha|0\rangle + \beta|1\rangle]\frac{|0\rangle U|0\rangle + |1\rangle U|1\rangle}{\sqrt{2}}$$

$$\Rightarrow \frac{1}{2}\big[|\Phi^+\rangle(U|d\rangle) + |\Phi^-\rangle(U\sigma_z|d\rangle) + |\Psi^+\rangle(U\sigma_x|d\rangle) + i|\Psi^-\rangle(U\sigma_y|d\rangle)\big]$$

Now, by performing Bell measurements on the first two qubits, we can discern the state of the unmeasured qubit. With probability 1/4 we see that the unitary has been correctly applied on the data qubit! The other three obtained cases cannot be used. For example, if the measurement corresponds to $U\sigma_X|d\rangle$, the circuit has implemented the unitary $U\sigma_X$ instead of U, thus "failing".

This can be seen as a direct consequence of the quantum teleportation protocol:

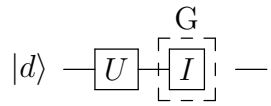


As seen in the first figure, this is just the quantum teleportation circuit, but with the additional modification of applying the unitary gate at the end of the unmeasured qubit. Since we already know the correspondence without the unitary...

Measurement outcome	**Expression**
00	$\alpha\,\|0\rangle + \beta\,\|1\rangle$
01	$\alpha\,\|1\rangle + \beta\,\|0\rangle$
10	$\alpha\,\|0\rangle - \beta\,\|1\rangle$
11	$\alpha\,\|1\rangle - \beta\,\|0\rangle$

... it becomes straightforward to determine the output after the application of the unitary.
We can now shift around the unitary applied on the third qubit since rest of the operations (incl. the measurements) only concern the first two qubits.

Just to make it clear, we must here reiterate the objective of [2], which is to send a state into the gate array such that the unitary corresponding to the state is then applied onto the data qubit.
Therefore, trivial implementations such as the one below do not count:



G here is simply the identity gate.
Nevertheless, one is still allowed to apply the arbitrary unitary onto any state which is then fed into the system, since only the definition of a fixed circuit needs to be satisfied.
Unfortunately the probability of success is given by 2^{-2m} in its generalized case, so it does not scale well.

0.3 Link to our original objective

Now that these workarounds have been shown to be impossible, this leaves us with the only option of inserting the unknown gate as a variable directly into the circuit. (We say this with the exception of the probabilistic implementation case. The authors seem to only be concerned with the deterministic outcome of the no-programming theorem.)
From this itself, we can provide an informal argument as to why a universal circuit is impossible:
Let us say that we are given U and $e^{i\phi}U$. They are essentially the same operator except for the global phase. Such an operator can be plugged in anywhere, and it would not make a difference except for changing the global phase of the qubit.
For controlled-U, the global phase now plays a measurable role.
$C - \mathbb{I} = \mathbb{I} \otimes \mathbb{I}, C - (-\mathbb{I}) = CZ$
Thus, the circuit will now have to quantify the global phase, a non-measurable quantity.
We need to show that the initial problem holds for control-$e^{iu}U$ as well, since we generally neglect global phase. There are cases where such phase dependencies occur.
Eg. from the paper under study:

> *Note also that if one's goal in implementing the control-U is to measure the energy of a Hamiltonian such that $U = e^{iHt}$ 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.* [3]

The proof of impossibility is as follows:

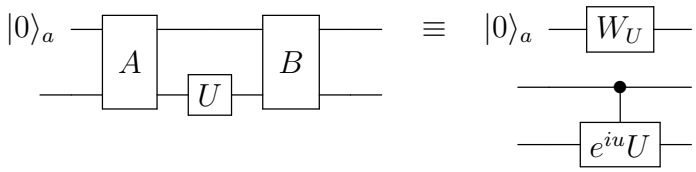


Figure from paper. First line is taken to be ancilla/"a"-dimensional quantum system.
We try to find unitaries A and B to implement a controlled-U such that the equality holds for any possible U.
Control-U gate: $\mathbb{I}_d \oplus U$. For a qubit system, this means that the control-U gate is controlled by $log_2 d$ qubits.

Let the total system be $a + j$ dimensional. The following equality must be proven:

$$B(\mathbb{I}_a \otimes \mathbb{I}_2 \otimes U)A|0\rangle_a|\psi\rangle_j = W_U|0\rangle_a(\mathbb{I}_d \oplus e^{iu}U)|\psi\rangle_j$$

Additional points:

- Let $W_U|0\rangle_a = |U^*\rangle_a$, to simplify notation.
- We must also take the tensor product with a two-dimensional Hilbert space, as it ensures that the resultant will have *some* subspace to use as control.
- For the proof here, we assume only one qubit as the control gate. Result can be generalised.

Let us assume that the equality holds for all unitary gates. Since every unitary gate can be decomposed into a linear combination of Pauli gates, let us consider the cases where U is the X gate, Z gate, and for the gate $G = \alpha X + \beta Z$ (normalized).
Then

$$B[\mathbb{I}_a \otimes \mathbb{I}_2 \otimes G]A(|0\rangle_a|\psi\rangle_j) = W_G|0\rangle_a \left(\mathbb{I}_2 \oplus e^{ig}G\right)|\psi\rangle_j$$

$$\Rightarrow B[\mathbb{I}_a \otimes \mathbb{I}_2 \otimes (\alpha X + \beta Z)]A(|0\rangle_a|\psi\rangle_j) = W_G|0\rangle_a \left(\mathbb{I}_2 \oplus e^{ig}G\right)|\psi\rangle_j$$

$$\Rightarrow \alpha W_X|0\rangle_a \left(\mathbb{I}_2 \oplus e^{ix}X\right)|\psi\rangle_j + \beta W_Z|0\rangle_a \left(\mathbb{I}_2 \oplus e^{iz}Z\right)|\psi\rangle_j = W_G|0\rangle_a \left(\mathbb{I}_2 \oplus e^{ig}G\right)|\psi\rangle_j$$

Taking the inner product with $|G^*\rangle_a$ and tracing out the j-dimensional subspace:

$$\alpha\langle G^*|X\rangle_a + \beta\langle G^*|Z\rangle_a = 1$$

Similarly, inner product with $|G^*\rangle_a|\psi\rangle_j$ gives:

$$\alpha\langle G^*|X\rangle_a e^{ix}\langle\psi|X|\psi\rangle_j + \beta\langle G^*|Z\rangle_a e^{iz}\langle\psi|Z|\psi\rangle_j = e^{ig}\langle\psi|\alpha X + \beta Z|\psi\rangle_j$$

Since X and Z are orthogonal, it is necessary that $\langle G^*|X\rangle = e^{i(g-x)}$ and $\langle G^*|Z\rangle = e^{i(g-z)}$.
If we substitute this into the equation obtained after the partial trace:

$$e^{i(g-x)}(\alpha + \beta e^{i(x-z)}) = 1$$

Taking the modulus squared of the equation shows that $cos(x-z) = 0$. Repeating this with gates $\alpha X + \beta Y$ and $\alpha Y + \beta Z$ gives:

$$cos(x-z) = cos(x-y) = cos(y-z) = 0$$

No such set of $\{x, y, z\}$ exists. **Thus, the transformation is not possible. No such circuit can be constructed.**

0.4 Surprisingly easy to circumvent in practical implementations

The now-proven theorem only holds when U belongs to the universal set of unitary gates. If even one eigenvector of U is known, then we can construct a circuit that performs its control [4].

0.4.1 The implementation

Zhou et al. [4] provide a clever method of circumventing the no-go theorem proved above. This is achieved by trivially extending the Hilbert space of the unknown unitary's input, such that there is a subspace over which the unitary acts, and a subspace over which it doesn't.
We can then define control-SWAP gates that conditionally move the target qubit state into the operating subspace of the unknown unitary gate, after which the necessary operation takes place.

Zhou et al. [4] state two methods of extension:

- Increasing the dimension of the target register: The target register now (instead of being a set of qubits) consists of a set of qudits, each qudit being a four-level system with logical states $|0\rangle, |1\rangle, |2\rangle$ and $|3\rangle$. The action of each X_α gate is to swap the states in the manner below:

$$X_\alpha|0\rangle = |2\rangle, X_\alpha|1\rangle = |3\rangle, X_\alpha|2\rangle = |0\rangle, X_\alpha|3\rangle = |1\rangle$$

$|2\rangle$ and $|3\rangle$, for the rest it acts as $\mathbb{I}$.

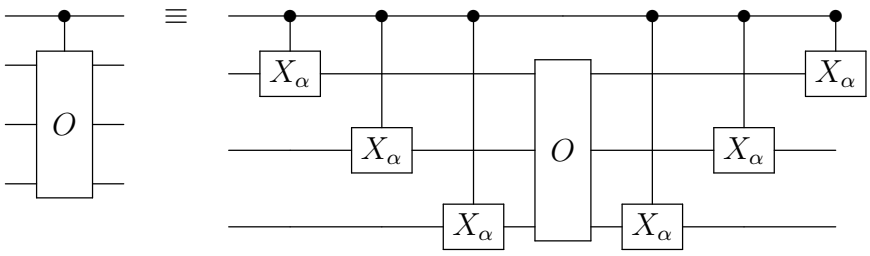


Figure 3: Example shown for a unitary acting on 3 qudits.

- Increasing the number of qubits: Each original qubit that was being acted upon by the unitary is now accompanied by an ancillary qubit. The circuit conditionally shifts the states into and out of the circuit.

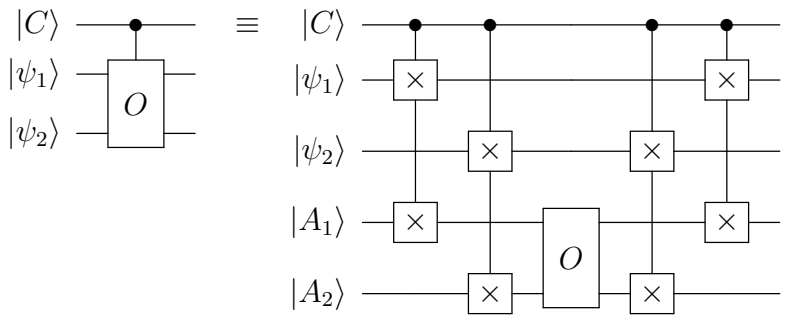


Figure 4: Example shown for a unitary acting on 2 qubits. $\boxed{\times}$ denotes SWAP gate. $|A_1\rangle$ and $|A_2\rangle$ play the role of ancillary qubits.

The authors (Zhou et al. [4]) state that the first implementation is more suitable for the present usage, as it uses smaller separate qubits, and the existing technologies are sufficient to scale the system for larger input unitaries. Araújo et al. [3] use the first implementation in their paper, and also provide a photonic implementation of circumvention:

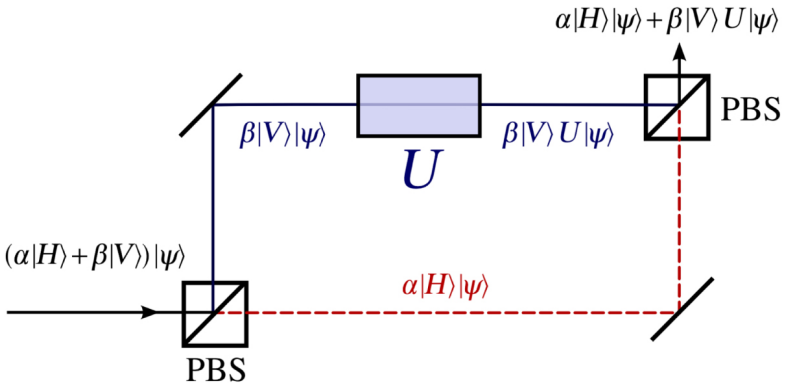


Figure 5: (Araújo et al.) *Interferometer that controls a qudit blackbox U. Here the control qubit is the polarization of the photon, and U acts on some additional degree of freedom of the same photon. The PBSs are polarizing beam splitters. A photon with polarization $|H\rangle$ takes the lower path (in red), while one with polarization $|V\rangle$ takes the upper path (blue).*

The phase shift operation is an example of an operation that does not affect the polarization of the photon.

This can be scaled to multi-qubit unitaries as well:

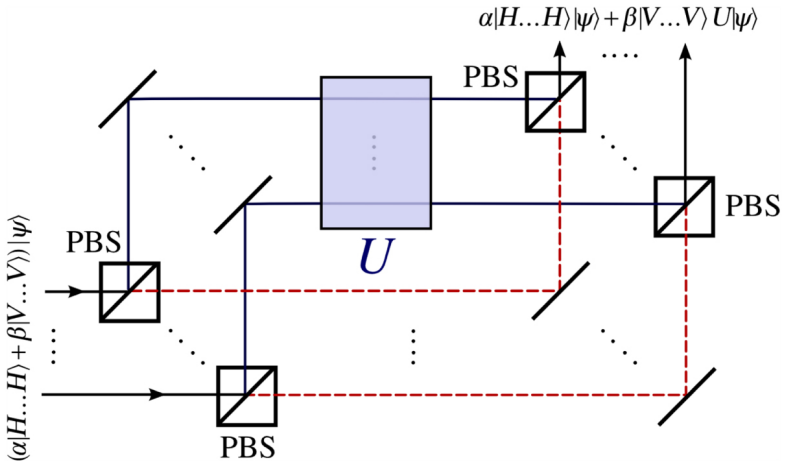


Figure 6: Scalable implementation. The control state is encoded in terms of the polarization of n photons as the state $\alpha|H\ldots H\rangle + \beta|V\ldots V\rangle$.

These implementations circumvent the no-go theorem as:

$$U_{\text{physical}} = \begin{bmatrix} \mathbb{I}_d & 0 \\ 0 & U \end{bmatrix}$$

0.5 Conclusions

The authors argue that since the no-go theorem can be circumvented by any possible physical implementation, the quantum circuit model is incomplete in the sense that such a circumvention must be covered "naturally" by the model if it is to represent quantum physics in its entirety.

Bibliography

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press, 2010.

[2] Nielsen, M. A., and Isaac L. Chuang. "Programmable Quantum Gate Arrays." Physical Review Letters 79, no. 2 (July 14, 1997): 321–24.

[3] Araújo, Mateus, Adrien Feix, Fabio Costa, and Časlav Brukner. 2014. "Quantum Circuits Cannot Control Unknown Operations." New Journal of Physics, no. 9 (September): 093026.

[4] Zhou, Xiao-Qi, 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, no. 1 (August 2, 2011): 413.