Quantum circuits cannot control unknown operations- Mateus Araújo et al

New Journal of Physics 16 (2014) 093026

Arnav Metrani MS21254

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
   - 4.0.1 Given any U, I can decompose it...
   - 4.0.2 We can store U and call it conditionally...
5. No-programming theorem
   - 5.1 Premise
   - 5.2 Proof
   - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

Revised abstract

tl;dr

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.

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
   - 4.0.1 Given any U, I can decompose it...
   - 4.0.2 We can store U and call it conditionally...
5. No-programming theorem
   - 5.1 Premise
   - 5.2 Proof
   - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

What is the objective?

Can you construct a fixed quantum circuit, such that if I provide you with any arbitrary unitary gate, then inserting the unitary gate into the circuit (or taking it in an an input) will cause the circuit to now function as a controlled-U gate?

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?

   4.0.1 Given any U, I can decompose it...

   4.0.2 We can store U and call it conditionally...

5. No-programming theorem

   5.1 Premise

   5.2 Proof

   5.3 What about probabilistic universal programmable quantum arrays?

6. What next?
7. Final proof
8. Conclusion

Informal argument

Let us say that we are given U and $e^{i\phi}U$. These 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.

Informal argument

Let us say that we are given U and $e^{i\phi}U$. These 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.
$C - \mathbb{I} = \mathbb{I} \otimes \mathbb{I}$, $C - (-\mathbb{I}) = CZ$

Informal argument

Let us say that we are given U and $e^{i\phi}U$. These 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.

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
    - 4.0.1 Given any U, I can decompose it…
    - 4.0.2 We can store U and call it conditionally…
5. No-programming theorem
    - 5.1 Premise
    - 5.2 Proof
    - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

Given any U, I can decompose it...

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.

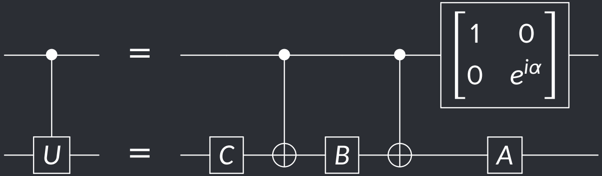


Figure: Circuit implementing the controlled-U operation for single qubit U. α, A, B and C satisfy $U = \exp(i\alpha)AXBXC$, $ABC = \mathbb{I}$.

We can store U and call it conditionally...

Classically, yes. We could store U (its description) as a bitstring in memory, and call it as required, based on the trigger.
One would believe that 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 no-programming theorem prevents this. [2]

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
    - 4.0.1 Given any U, I can decompose it…
    - 4.0.2 We can store U and call it conditionally…
5. No-programming theorem
    - 5.1 Premise
    - 5.2 Proof
    - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

No-programming theorem

Given an m-qubit data register $|d\rangle$ and an n-qubit program register which maps to to U $|P_U\rangle$, let us assume the existence of a fixed circuit (whose operations are defined by G) such that:

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

No-programming theorem

What if the output program state depends on the data state?

Not possible.

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:

$G[\,|d_1\rangle \otimes |P_U\rangle\,] \rightarrow U|d_1\rangle \otimes |P'_{U_1}\rangle$

$G[\,|d_2\rangle \otimes |P_U\rangle\,] \rightarrow U|d_2\rangle \otimes |P'_{U_2}\rangle$

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 and extra state $|d_3\rangle$ that is non-ortho to both, and using transitivity.

No-programming theorem

It still seems possible to do however, since the unitary matrix acting on m qubits is a $2^m \times 2^m$ matrix, so roughly 2^{2m} real numbers are required to describe them, while the number of real numbers required to describe a $2m$ qubit state is $2^{2m+1} - 1$.

No-programming theorem

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

Proof

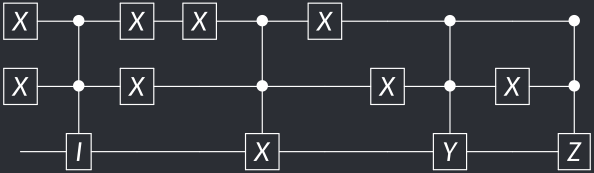
We show that for every distinct unitary operation that the fixed circuit wishes to implement, the dimension of the program register must be increased by 1. We show this by proving that distinct unitaries must correspond to orthogonal states.
∞ distinct unitary gates, ∞ dimensional system, ∞ qubits.
Impossible to implement, for every time you fix the circuit, you need to expand its input.

Proof

A program register $|P\rangle$ of dimension "n" can deterministically implement "n" distinct unitary operations (ignoring global phase) on the data register via control gates.

Proof

A program register $|P\rangle$ of dimension "n" can deterministically implement "n" distinct unitary operations (ignoring global phase) on the data register via control gates. Eg. for $n = 2$:



(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.)

Proof

Assume the 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.

Proof

Assume the 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.

Let us assume this is not the case

Proof

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:

Proof

$\langle Q|P\rangle = \langle Q'|P'\rangle\langle d|U_Q^\dagger U_P|d\rangle$
Assume $\langle Q'|P'\rangle \neq 0$.
Then $\frac{\langle Q|P\rangle}{\langle Q'|P'\rangle} = \langle d|U_Q^\dagger U_P|d\rangle$
LHS is not dependent on $|d\rangle$ (as seen from 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 our initial assumption $\langle Q'|P'\rangle \neq 0$ is wrong.
Thus, from first equation, if $\langle Q'|P'\rangle = 0$, then $\langle Q|P\rangle = 0$. Rest follows.

What about probabilistic universal programmable quantum arrays?

Theorem DOES NOT hold. Out of scope for this talk.

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
   - 4.0.1 Given any U, I can decompose it...
   - 4.0.2 We can store U and call it conditionally...
5. No-programming theorem
   - 5.1 Premise
   - 5.2 Proof
   - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

What next?

This leaves us with the option of only plugging in the arbitrary unitary gate as a variable into the fixed quantum circuit. So let us do that.

Additionally, let us now show that the initial problem holds for control-$e^{iu}U$ as well, since we generally neglect global phase overall. Additionally, there are cases where such dependencies occur.

What next?

From the paper itself:

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.

Next approach

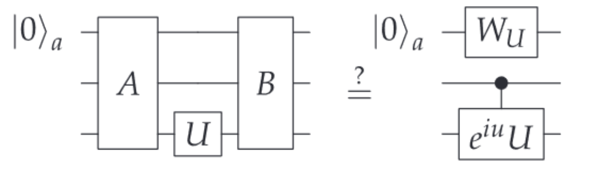


Figure: Figure from paper. First line is taken to be ancilla/a-dimensional quantum system.

We try to find unitaries A and B to implement a controlled U gate given the unknown U gate.

Control-U gate: $\mathbb{I}_d \oplus U$. For a qubit system it means that the control-U gate is controlled by $\log_2 d$ qubits.

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
   - 4.0.1 Given any U, I can decompose it...
   - 4.0.2 We can store U and call it conditionally...
5. No-programming theorem
   - 5.1 Premise
   - 5.2 Proof
   - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. Conclusion

Final proof

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 $W_U|0\rangle_a = |U^*\rangle_a$
- We must take tensor product with a two-dimensional Hilbert space as well as it ensures that the resultant will have *some* subspace to use as control.

Final proof

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

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

Here we assume only one qubit control gate. Result can be generalised.

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

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

Final proof

Taking inner product with $|G^*\rangle_a$ and taking 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:

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

Final proof

Since X and Z are orthogonal, we get the following: $\langle G^* | X \rangle = e^{i(g-x)}$ and $\langle G^* | Z \rangle = e^{i(g-z)}$
More manipulation gives $cos(x - z) = 0$
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 $\{x, y, z\}$ exist. **Thus, the transformation is not possible.**

Outline for the talk

1. Revised abstract
2. Objective
3. Informal argument
4. Possible workarounds?
   - 4.0.1 Given any U, I can decompose it...
   - 4.0.2 We can store U and call it conditionally...
5. No-programming theorem
   - 5.1 Premise
   - 5.2 Proof
   - 5.3 What about probabilistic universal programmable quantum arrays?
6. What next?
7. Final proof
8. **Conclusion**

Conclusion

Is this the end?

No, the authors then go one to show we can circumvent this if one eigenvector of U and its eigenvalue are known. Similarly if the unitaries are orthogonal.

Furthermore, physical implementations have already occurred. [3] We can exploit the first point for "physical" implementations by simply extending the Hilbert space.

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

The circuit formalism must be modified to account for this.

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] 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.