Exercise 1. *No-go theorem I: the no-programming theorem*

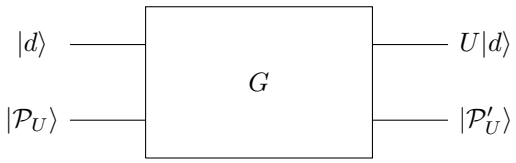
In the lecture we have seen the most famous example of a quantum no-go theorem: the no-cloning theorem. However, there are more theorems of this type showing that there are certain tasks that are possible in a classical setting but cannot be achieved for general quantum systems. In this exercise we will prove that it is impossible to build a programmable quantum gate array*, i.e., to construct fixed circuits that take as input a quantum state specifying a quantum program and a data register to which the unitary U corresponding to the quantum program is applied.*

The input given to the programmable quantum gate array may have the form

$$|d\rangle \otimes |\mathcal{P}_U\rangle$$

where $|d\rangle$ is the m-qubit data register and $|\mathcal{P}_U\rangle$ is a state of the n-qubit program register. The total dynamics of the programmable gate array is given by a unitary operator G

$$|d\rangle \otimes |\mathcal{P}_U\rangle \to G[|d\rangle \otimes |\mathcal{P}_U\rangle] = (U|d\rangle) \otimes |\mathcal{P}'_U\rangle.$$



(a) Show that $|\mathcal{P}'_U\rangle$ must be independent of the input state $|d\rangle$.

(b) Suppose that distinct unitary operators $U_1, U_2, \ldots, U_N$ are implemented.

(i) Show that if the expression $\langle d|U_i^\dagger U_j|d\rangle$ is independent of $|d\rangle$ then $U_i^\dagger U_j = \gamma \cdot \mathrm{id}$ must hold.

(ii) Use the result (i) to show that the corresponding programs $|\mathcal{P}_{U_1}\rangle, |\mathcal{P}_{U_2}\rangle, \ldots, |\mathcal{P}_{U_N}\rangle$ must be mutually orthogonal.

(iii) Discuss why this implies that there cannot exist a programmable quantum gate array that works for arbitrary inputs U.

(c) The result above shows that no deterministic *universal quantum gate array exists. We will see now that the task is possible in a* probabilistic *fashion. For simplicity we only consider the case $m = 1$. Show that*

$$|\mathcal{P}_U\rangle = (\mathrm{id} \otimes U)|\Phi^+\rangle_{12}$$

can be used to successfully implement the desired transformation with probability $1/4$.

Hint. Consider a measurement of the data register and the first subsystem of the program register w.r.t. the Bell basis.

Solution.

(a) Suppose

$$|d_1\rangle \otimes |\mathcal{P}_U\rangle = (U|d_1\rangle) \otimes |\mathcal{P}'_1\rangle.$$
$$|d_2\rangle \otimes |\mathcal{P}_U\rangle = (U|d_2\rangle) \otimes |\mathcal{P}'_2\rangle.$$

Now take the inner product of these two equations yields $\langle \mathcal{P}'_1|\mathcal{P}'_2\rangle = 1$ if $\langle d_1|d_2\rangle \neq 0$ and thus $|\mathcal{P}'_1\rangle = |\mathcal{P}'_2\rangle$.

(i) $U_i^\dagger U_j$ is still unitary and therefore it can be diagonalised. From the condition it follows that all the eigenvalues are identical. Therefore we have $\langle d|U_i^\dagger U_j|d\rangle = V(\lambda \cdot \mathrm{id})V^\dagger = \lambda \cdot \mathrm{id}$.

(ii) Suppose $|\mathcal{P}_i\rangle$ and $|\mathcal{P}_j\rangle$ are programs which implement two distinct unitary operators U_i and U_j (up to a global phase). Then for arbitrary input $|d\rangle$ we have

$$G[|d\rangle \otimes |\mathcal{P}_i\rangle] = (U_i|d\rangle) \otimes |\mathcal{P}_i'\rangle$$

$$G[|d\rangle \otimes |\mathcal{P}_j\rangle] = (U_j|d\rangle) \otimes |\mathcal{P}_j'\rangle.$$

Now we take the inner product of these equastions

$$\langle \mathcal{P}_i|\mathcal{P}_j\rangle = \left\langle \mathcal{P}_i'|\mathcal{P}_j'\right\rangle \langle d|U_i^\dagger U_j|d\rangle. \tag{S.1}$$

If $\left\langle \mathcal{P}_i'|\mathcal{P}_j'\right\rangle \neq 0$, then

$$\frac{\langle \mathcal{P}_i|\mathcal{P}_j\rangle}{\left\langle \mathcal{P}_i'|\mathcal{P}_j'\right\rangle} = \langle d|U_i^\dagger U_j|d\rangle.$$

The *lhs* is independent of the inputs state $|d\rangle$ and therefore the *rhs* must be independent as well. Using the result from (i) it follows that $U_i^\dagger U_j = \lambda \cdot \mathrm{id}$. Therefore we have $U_j = \lambda \cdot U_i$, i.e., U_j and U_i are identical up to a global phase. But this is in contradiction with our initial assumption and thus it follows that $\left\langle \mathcal{P}_i'|\mathcal{P}_j'\right\rangle = 0$. From Equation (S.1) we then get $\langle \mathcal{P}_i|\mathcal{P}_j\rangle = 0$. Therefore, in order to implement N distinct unitaries we need at least N orthogonal program states, i.e., the state space has to be N dimensional.

(iii) The number of possible unitary operations on m qubits is infinite and we have just seen that every unitary operation requires an extra Hilbert space dimension. Therefore, a universal gate array would require an infinite number of qubits (an N dimensional Hilbert space contains $\log N$ qubits) in the program register.

(b) We have

$$|\mathcal{P}_U\rangle = (\mathrm{id} \otimes U)|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle U|0\rangle + |1\rangle U|1\rangle).$$

For an input $|d\rangle = a|0\rangle + b|1\rangle$ we can write

$$(a|0\rangle + b|1\rangle)\left(\frac{1}{\sqrt{2}}(|0\rangle U|0\rangle + |1\rangle U|1\rangle)\right) =$$

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

Now if the result from the measurement w.r.t the Bell basis corresponds to $|\Phi^+\rangle$, the the post-measurement state of the second qubit of the program register will be $U|d\rangle$ as desired. The probability of this outcome is equal to $1/4$.

A detailed discussion can be found in PhysRevLett.79.321.

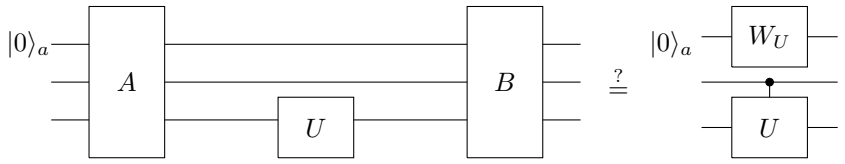
Exercise 2. ***No-go theorem II: unknown operations cannot be controlled in quantum circuits***

The quantum analogue of the "if"-statement in classical computer programs is the control of a unitary operation U depending on the value of a control 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 C is the control qubit and $|\psi\rangle$ is the initial state of the target system.

In this exercise we will show that there is no quantum circuit that can implement the controlled U gate, given as input a single copy of the unknown $d \times d$ gate U. Thus, the question is whether there exist unitaries A and B such that the following circuit identity is satisfied.

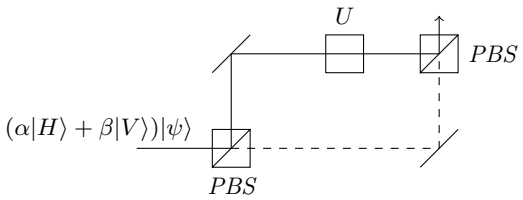


(a) Show that the above identidy cannot be satisfied. In order to see this note that on the* lhs *substituting U with $e^{i\phi}U$ does not produce any physical difference, but the same substitution on the* rhs *produces a relative phase. Therefore it is only meaningful to ask whether a circuit can implement the control-U modulo this global phase. The matrix representation of the control-U is given by $\mathrm{id}_d \oplus U$. Defining $|U\rangle_a := W_U|0\rangle_a$ the question is whether the identity*

$$B(\mathrm{id}_a \otimes \mathrm{id}_2 \otimes U)A|0\rangle_a = |U\rangle_A(\mathrm{id}_d \oplus e^{iu}U)$$

holds for some arbitrary phase factor e^{iu}. Show now that this equality cannot be satisfied for the qubit unitaries X, Z, $\alpha X + \beta Z$, $\alpha X + \beta Y$ and $\alpha Y + \beta Z$ simultaneously (α and β are real numbers such that $\alpha^2 + \beta^2 = 1$).

(b) Unlike for the no-cloning theorem, this no-go theorem does not prevent quantum control of unknown operations from being performed in practice. Explain how the circuit below implements a controlled unitary transformation.



Here $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states of a photon and the PBSs are polarizing beam splitters.

(c) How does this interferometric implementation circumvent the no-go theorem we have just proved?

Solution.

(a) Note that the *lhs* corresponds to the most general transformation that a quantum circuit can effect on U.

Note that substituting U with $e^{i\phi}U$ in the *lhs* results in

$$B(\mathrm{id}_a \otimes \mathrm{id}_2 \otimes e^{i\phi}U)A|0\rangle_a = e^{i\phi}B(\mathrm{id}_a \otimes \mathrm{id}_2 \otimes U)A|0\rangle_a$$

whereas in the *rhs* we get

$$|U\rangle_A(\mathrm{id}_d \oplus e^{iu}U).$$

Now it holds that two operations U and V can be physically distinguished if $\exists\rho$ such that $U\rho U^\dagger \neq V\rho V^\dagger$. If $U \neq e^{i\phi}V$ such a ρ exists. This can be seen as follows. We can rewrite the condition as $\rho \neq U^{-1}V\rho(U^{-1}V)^\dagger$. Because $(U^{-1}V)$ is still unitary it can be diagonalised $(U^{-1}V) = WDW^\dagger$ and our assumption that $(U^{-1}V) \neq e^{i\phi}\mathrm{id}$ implies that $D = diag(e^{i\phi_1}, e^{i\phi_2}, \ldots, e^{i\phi_d})$ such that $\phi_i \neq \phi_j$ for at least one pair (i, j). Without loss of generality let it be ϕ_1 and ϕ_2. Chose now

$$\rho = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & \ldots & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & \ldots & 0 \\ 0 & & \ldots & & 0 \\ \vdots & & \ldots & & \vdots \\ 0 & & \ldots & & 0 \end{pmatrix}$$

For this choice of ρ we have that $\rho \neq D\rho D^\dagger$ (in an eigenbasis of $(U^{-1}V)$) which transforms back into our original condition.

Now assume by contradiction that

$$B(\mathrm{id}_a \otimes \mathrm{id}_2 \otimes U)A|0\rangle_a = |U\rangle_a(\mathrm{id}_d \oplus e^{iu}U) \tag{S.2}$$

is true for X, Z and $H = \alpha X + \beta Z$.
For H we get from (S.2) that

$$B(\mathrm{id}_a \otimes \mathrm{id}_2 \otimes (\alpha X + \beta Z))A|0\rangle_a = |H\rangle_a(\mathrm{id}_d \oplus e^{ih}H).$$

Expanding the *lhs* and applying (S.2) again we get

$$\alpha|X\rangle_a(\mathrm{id}_d \oplus e^{ix}X) + \beta|Z\rangle_a(\mathrm{id}_d \oplus e^{iz}Z) + = |H\rangle_a(\mathrm{id}_d \oplus e^{ih}H).$$

Now we take the inner product with $|H\rangle_a$ (by multiplication with $\langle H|_a$ from the left) and find

$$\alpha\,\langle H|X\rangle_a\,(\mathrm{id}_d \oplus e^{ix}X) + \beta\,\langle H|Z\rangle_a\,(\mathrm{id}_d \oplus e^{iz}Z) = (\mathrm{id}_d \oplus e^{ih}H)$$

and hence

$$\begin{aligned}\alpha\,\langle H|X\rangle_a\,e^{ix}X + \beta\,\langle H|Z\rangle_a\,e^{iz}Z &= e^{ih}H \\ &= e^{ih}(\alpha X + \beta Z).\end{aligned}$$

Now we multiply this equation with X and take the trace ($\mathrm{tr}(XZ) = 0$ and $\mathrm{tr}(X^2) = \mathrm{tr}(\mathrm{id}) = 2$) yielding

$$\alpha\,\langle H|X\rangle_a\,e^{ix} = e^{ih} \Rightarrow \langle H|X\rangle_a = e^{i(h-x)}$$

and doing the same with Z we get

$$\langle H|Z\rangle_a = e^{i(h-z)}.$$

From the definition of $|H\rangle_a = \alpha X|0\rangle_1 + \beta Z|0\rangle_a$ we get by taking the inner product with itself

$$\alpha \langle H|X\rangle_a + \beta \langle H|Z\rangle_a = 1.$$

Plugging in that $\langle H|X\rangle_a = e^{i(h-x)}$ and $\langle H|Z\rangle_a = e^{i(h-z)}$ we find

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

Taking the modulus squared yields

$$1 = |\alpha|^2 + |\beta|^2 + \alpha\beta e^{i(x-z)} + \alpha\beta e^{-i(x-z)}$$

and therefore

$$0 = \cos(x - z).$$

Now we repeat the same thing for $H = \alpha X + \beta Y$ and $H = \alpha Y + \beta Z$ to find

$$0 = \cos(x - z) \text{ and } 0 = \cos(x - y) \text{ and } 0 = \cos(y - z).$$

This equations cannot be satisfied for any angles x, y and z, which shows that one cannot control an unknown unitary in the quantum circuit model.

(b) The interferometer applies the transformation

$$(\alpha|H\rangle + \beta|V\rangle)|\psi\rangle \mapsto \alpha|H\rangle|\psi\rangle + \beta|V\rangle U|\psi\rangle$$

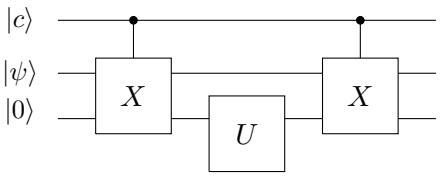
for any unitary U.

(c) We show the following

(i) If one of the eigenvectors of U is known then the implementation of the controlled U is possible.

(ii) In the interferometric implementation we know eigenvectors of the *physical* unitary.

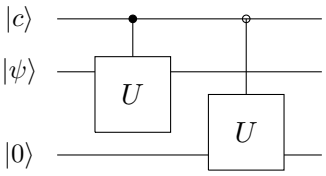
(i) Consider the following circuit



Because it maps

$$(\alpha|0\rangle + \beta|1\rangle)|\psi\rangle|0\rangle \to \alpha|0\rangle|\psi\rangle U|0\rangle + \beta|1\rangle U|\psi\rangle|0\rangle$$

it corresponds to the circuit



Here $\circ$ is a controlled operation of 0.

Now this looks similar to the circuit corresponding to the controlled-U operation and would be identical to it (with $W_u = \mathrm{id}$) if instead of the second unitary we would have an identity operation. If we know an eigenstate $|v\rangle$ of the unitary U this is indeed possible, because then, we can simply input $|v\rangle$ in the last wire instead of $|0\rangle$.

(ii) In the case of the interferometer the physical unitary does not only act on the space of the qubit but also on the space of the photon modes. W.r.t. the basis $\{|a0\rangle, |a1\rangle, |b0\rangle, |b1\rangle\}$ the total unitary operation is given by

$$U_{physical} = \begin{pmatrix} U & 0 \\ 0 & \mathrm{id}_2 \end{pmatrix}$$

and therefore acts trivially on a two dimensional subspace. The corresponding eigenvectors are $|b0\rangle, |b1\rangle$ and therefore known for all unitaries U.

A detailed discussion can be found in arxiv 1309.7976.