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

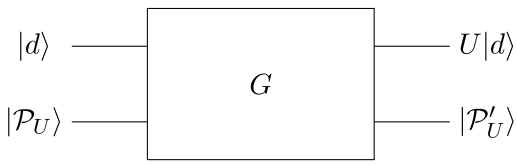
In the lecture we have seen the most famous example of a quantum no-go theorem: the no-cloning theorem. However, there are more theorems of this type showing that there are certain tasks that are possible in a classical setting but cannot be achieved for general quantum systems. In this exercise we will 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. *C*onsider a measurement of the data register and the first subsystem of the program register w.r.t. the Bell basis.

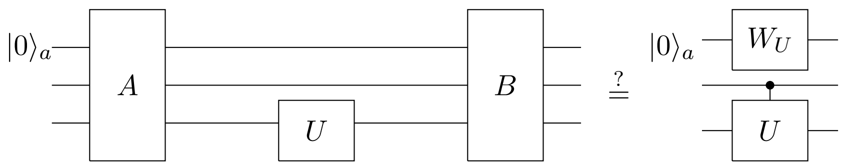
Exercise 2. ***No-go theorem II: unknown operations cannot be controlled in quantum circuits***

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.

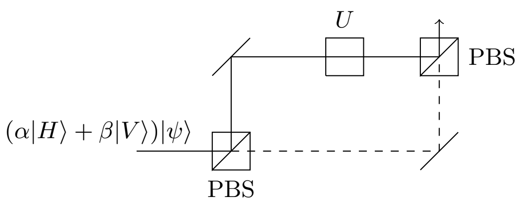


(a*) Show that the above identidy cannot be satisfied. In order to see this note that on the *lhs* substituting U with $e^{i\phi}U$ does not produce any physical difference, but the same substitution on the *rhs* produces a relative phase. Therefore it is only meaningful to ask whether a circuit can 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?