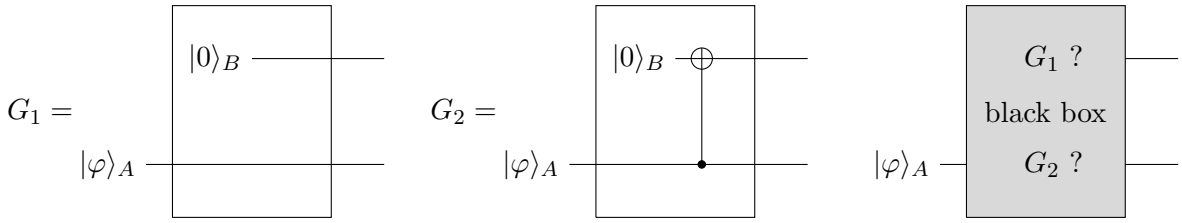
Exercise 1. ***A variant of the Elitzur-Vaidman bomb tester***

In the circuit model of classical and quantum computation one considers horizontal lines to indicate temporal evolution of bits and qubits, respectively, while boxes indicate gates that are applied to them. Consider the two gates G_1 and G_2 applied to an input $|\varphi\rangle$ on system A:



We use the braket notation for both the classical and the quantum case. In the classical case $|\varphi\rangle_A$ is the state of a bit and in the quantum case it is the state of a qubit. The gate G_1 applies the identity on system A and outputs the input on A together with $|0\rangle$ on B whereas G_2 applies a CNOT gate to $|\varphi\rangle_A \otimes |0\rangle_B$, where $|\varphi\rangle_A$ plays the role of the control (qu)bit. The (classical) truth table of a CNOT gate is:

control bit	target bit	output A	output B
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

In the quantum circuit model any gate can be written as a unitary matrix. If the first qubit is the control and the second the target qubit the unitary describing the CNOT operation reads

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Suppose now we are given a black box (depicted above) and are guaranteed to have either G_1 or G_2 in the box. In the following we assume that we can chose the input on system A but only the output on A is available to us, not the output on B.

(a) Write down the truth table of both gates G_1 and G_2 in the classical scenario and show that in this case it is impossible to distinguish the two (even if one can query the black box arbitrarily many times).

(b) If inputs and outputs of the black box can be quantum states the game changes. Choosing the right input qubit state $|\varphi\rangle$ one can exclude gate G_1 with probability $1/2$ in only one query if the black box implements G_2. Determine this input, calculate the output for both gates and explain why this allows us to distinguish them in certain cases. In what basis would you measure the output of A?

Suppose you want to know which gate is implemented in the black box but face the additional restriction that the output on B when measured in the $\{|0\rangle, |1\rangle\}$ basis must not be 1 (otherwise you blow up a bomb).

(c) In a first step, take the strict constraint that the probability to get outcome 1 on B must be zero in a measurement in the basis $\{|0\rangle, |1\rangle\}$, $\mathbb{P}[B = 1] \stackrel{!}{=} 0$. Prove that with this interpretation of the constraint quantum mechanics does not yield an advantage, i.e. it is impossible to distinguish G_1 from G_2 in the black box.

(d) Show how quantum mechanics allows us to achieve the above task by a procedure with N queries where the probability to get outcome 1 on B is $O(1/N)$, i.e. it can be made arbitrarily small.

Hint: Apply an iterative strategy using the single qubit gate

$$R_\varepsilon = \begin{pmatrix} \cos\varepsilon & -\sin\varepsilon \\ \sin\varepsilon & \cos\varepsilon \end{pmatrix}$$

in between two steps, where ε is a small real parameter depending on N (the number of iterations).