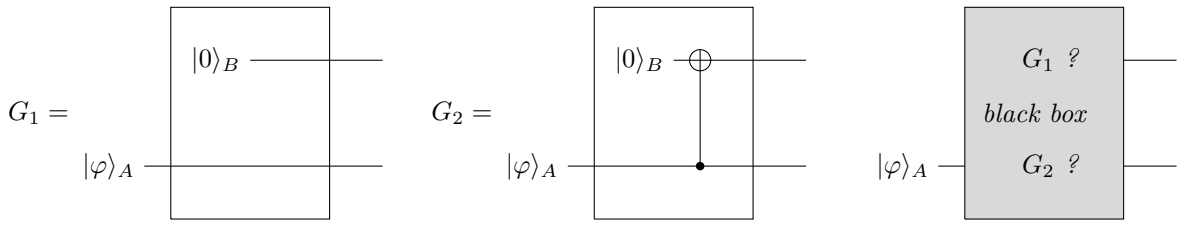
Exercise 1. *A variant of the Elitzur-Vaidman bomb tester*

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).*

Solution.

(a) The truth tables of classical gates characterize the gates completely and contain all possible input-output pairs. For the two gates G_1 and G_2 they are:

G_1 : input A	output A	output B
0	0	0
1	1	0

G_2 : input A	output A	output B
0	0	0
1	1	1

If access on the outputs is restricted to system A only it becomes obvious that it is impossible to distinguish the gates. They differ only on output B which is inaccessible by assumption.

(b) Colloquially speaking, the difference in the quantum case is that the truth table of input and output states in the computational basis $\{|0\rangle, |1\rangle\}$ is not all one can say about a gate. Instead of inserting $|0\rangle$ or $|1\rangle$ one can now input superpositions of these states too, e.g. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Suppose we insert $|\varphi\rangle = |-\rangle$, then the *global* output on AB is

$$|\rho^{(1)}\rangle_{AB} = |-0\rangle_{AB} \qquad \text{if } G_1 \text{ is implemented,} \tag{S.1}$$

$$|\rho^{(2)}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right) \qquad \text{if } G_2 \text{ is implemented,} \tag{S.2}$$

where we used the notation $|xy\rangle_{AB} = |x\rangle_A \otimes |y\rangle_B$ for $x, y \in \{0, 1, +, -, ...\}$. In the following we omit the indices of the systems A and B if it is clear from the context which system is meant. The output state $|\rho^{(2)}\rangle$ can also be written as $|\rho^{(2)}\rangle = \frac{1}{\sqrt{2}}(|-+\rangle + |+-\rangle)$ Hence, measuring the output on A in the $\{|-\rangle, |+\rangle\}$ basis we obtain probabilities

$$\mathbb{P}^{(1)}[A = -] = \mathrm{tr}\left[|-\rangle\langle -|_A \otimes \mathbb{1}_B \; \rho^{(1)}_{AB}\right] = 1, \quad \mathbb{P}^{(1)}[A = +] = 0, \tag{S.3}$$

$$\mathbb{P}^{(2)}[A = -] = \mathrm{tr}\left[|-\rangle\langle -|_A \otimes \mathbb{1}_B \; \rho^{(2)}_{AB}\right] = \frac{1}{2}, \quad \mathbb{P}^{(2)}[A = +] = \frac{1}{2}. \tag{S.4}$$

Here, $\rho^{(i)}_{AB} = |\rho^{(i)}\rangle\langle\rho^{(i)}|$ denotes the density matrices describing the respective quantum states. We conclude that if the black box implements G_1 then the outcome of the measurement must be $-$ always. But if it implements G_2 then with probability $1/2$ the outcome is $+$. Such an outcome enables us to conclude that the black box cannot implement G_1.

Notice that choosing $|\varphi\rangle = |-\rangle$ is just one out of many possibilities to solve this exercise.

(c) Before starting we note that since we deal with qubit in- and outputs the orthogonal subspace to any state is one-dimensional. For instance, the orthogonal subspace of $|1\rangle$ is $\text{span}(|0\rangle)$.

Clearly, if the black box implements gate G_1 the probability of getting outcome 1 in a measurement on B is zero. Therefore we consider only gate G_2 in this part of the exercise. We start with

$$0 \stackrel{!}{=} \mathbb{P}[B=1] = \text{tr}\left[\mathbb{1}_A \otimes |1\rangle\langle 1|_B \; \rho_{AB}^{(2)}\right]. \tag{S.5}$$

This is the same as saying that the state $\rho_{AB}^{(2)}$ is orthogonal to $|1\rangle_B$, which by the above statement implies that it has the form $\rho_{AB}^{(2)} = \rho_A^{(2)} \otimes |0\rangle\langle 0|_B$. We also know that the initial state on B was $|0\rangle$. Hence, by consulting the matrix of the CNOT gate we find

$$|00\rangle_{AB} \to |00\rangle_{AB}, \quad |10\rangle_{AB} \to |11\rangle_{AB}$$

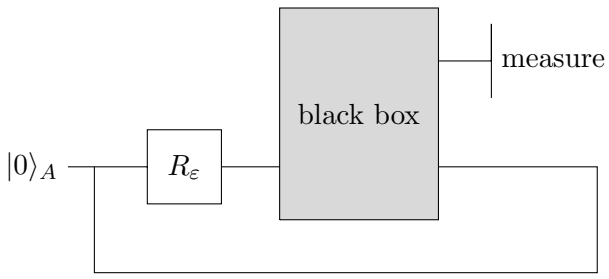
and the only input on A that gives an output of this form is $|0\rangle_A$. However, if this is the only allowed input then there cannot be an information gain about what gate is implemented because the outgoing states for both gates G_1 and G_2 are identical for the input $|0\rangle_A$.

(d) Consider the initial input $|0\rangle_A$ followed by the single qubit gate R_ε, where ε is yet to be determined. The intermediate state after inputting this to the black box is

$$(\cos\varepsilon\,|0\rangle_A + \sin\varepsilon\,|1\rangle_A) \otimes |0\rangle_B \qquad \text{if } G_1 \text{ is implemented,} \tag{S.6}$$

$$(\cos\varepsilon\,|00\rangle_{AB} + \sin\varepsilon\,|11\rangle_{AB}) \qquad \text{if } G_2 \text{ is implemented.} \tag{S.7}$$

If the black box implements G_1 there is no problem as the only possible outcome on B is 0. Furthermore, a measurement on B does not change the state on A at all because the two systems are in a product state. In the other case, when G_2 is implemented, the probability of getting outcome 1 is $\mathbb{P}[B=1] = \sin^2\varepsilon$. If this happens, then the procedure stops (because the bomb exploded and there is no black box anymore to worry about). However, if outcome 0 is measured, which happens with probability $\mathbb{P}[B=0] = \cos^2\varepsilon$, then the state on A collapses to $|0\rangle_A$ and we can continue by applying again R_ε etc.



Now let $\varepsilon = \frac{\pi}{2N}$ for some (large) N and repeat the above procedure N times. If the black box implements G_1 the final state on A after N rounds is $R_\varepsilon^N|0\rangle = R_{N\varepsilon}|0\rangle = R_{\frac{\pi}{2}}|0\rangle = |1\rangle$ and the bomb never exploded. However, if the black box implements G_2 and the outcome $B=1$ never occurred the final state on A is $|0\rangle$. The states $|0\rangle$ and $|1\rangle$ are perfectly distinguishable, i.e. orthogonal, and thus a measurement on A in the basis $\{|0\rangle, |1\rangle\}$ reveals with certainty which gate was used.

Now to the probability of failure. If the black box contains G_2 the probability to fail in a single run is $\mathbb{P}[B = 1] = \sin^2 \varepsilon$, as mentioned above. Thus in N runs:

$$\begin{aligned} \mathbb{P}[B = 1 \text{ once or more}] &= 1 - \mathbb{P}[B = 0 \text{ always}] = 1 - (1 - \sin^2 \varepsilon)^N \\ &\approx 1 - (1 - \varepsilon^2)^N \approx N\varepsilon^2 = \left(\frac{\pi}{2}\right)^2 \cdot \frac{1}{N} \\ &= O\left(\frac{1}{N}\right), \end{aligned} \tag{S.8}$$

where we used Taylor expansion for small ε twice. We conclude that the above procedure achieves the distinction of G_1 and G_2 in N rounds while the probability of getting outcome 1 in a measurement on B is $O(1/N)$. This means it can be made arbitrarily small by increasing the number of rounds.