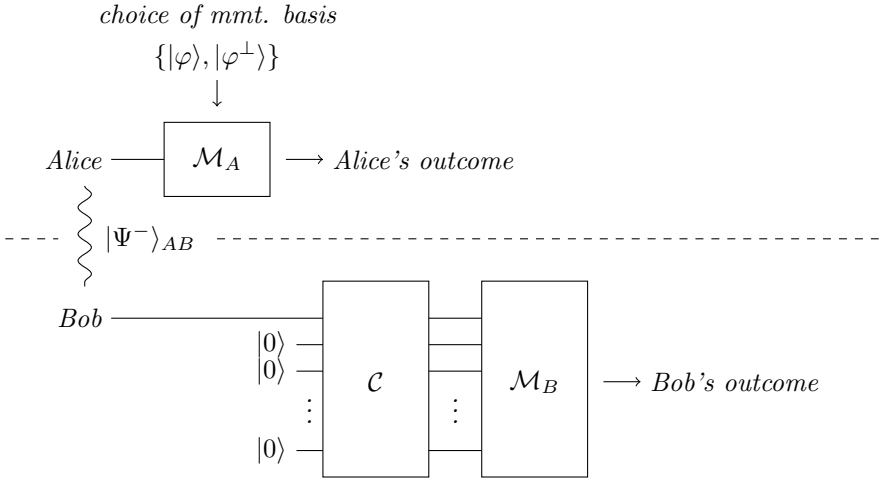
Exercise 1. *Cloning implies signalling*

We have seen in the lecture that no unitary operation (actually: no completely positive trace preserving map) can clone a quantum state. Because in quantum mechanics the evolution of a closed system is unitary, this proves that quantum states cannot be cloned. In this exercise we will see that quantum cloning is incompatible with no-signalling which is believed to be a fundamental principle. This provides us with an argument for the impossibility of cloning that does not rely on any assumption regarding the evolution of quantum systems.

A n-fold quantum cloning machine implements the operation

$$\mathcal{C} : |\psi\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle \otimes \cdots \otimes |\psi\rangle$$

for all possible inputs $|\psi\rangle$, i.e. it produces n copies of an arbitrary quantum state. Consider Alice and Bob, two agents who are spatially separated and share a Bell pair $|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$. The no-signalling principle implies that, no matter what Alice does to her part of the Bell state, she cannot influence the measurement statistics on Bob's side. In the following we show that if Bob has a quantum cloning machine then he can detect what measurement Alice carried out on her side. Hence Alice could signal without sending an information carrier to Bob.



(a) *Suppose Alice measures in the basis $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\varphi^\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. What is the state on Bob's side conditioned on Alice's outcome after her measurement?*

(b) *Alice can do one out of two measurements, either in the $\{|0\rangle, |1\rangle\}$ basis or in the $\{|+\rangle, |-\rangle\}$ basis. With the help of the cloning machine, explain how Bob can find out about Alice's measurement choice with high probability for large n.*

Hint. *Bob can perform a measurement on the output of the cloning machine. What measurement would tell him with high probability the measurement choice of Alice?*

(c) *With the protocol established in (b) Alice can signal one bit, encoded in her choice of measurement, to Bob under the assumption that they shared a maximally entangled state and that Bob has access to a quantum cloning machine. What goes wrong with the procedure if they instead shared n copies of a maximally entangled state, $|\Psi^-\rangle_{AB}^{\otimes n}$, but without the cloning machine?*

(d) *In fact, the number of bits Alice can signal to Bob making use of a Bell pair and the cloning machine is much larger than one. How can the protocol from (b) be extended to allow Alice to signal an unlimited amount of bits to Bob?*

Solution.

(a) Alice measures in the (orthonormal) basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$. Suppose the outcome is $|\varphi\rangle_A$, then the post measurement state is

$$\frac{|\varphi\rangle\langle\varphi|_A \otimes \mathbb{1}_B |\Psi^-\rangle_{AB}}{\sqrt{\langle\Psi^-| |\varphi\rangle\langle\varphi|_A \otimes \mathbb{1}_B |\Psi^-\rangle}}, \tag{S.1}$$

where the term in the denominator is for normalization. This can be simplified:

$$\begin{aligned} |\varphi\rangle\langle\varphi|_A \otimes \mathbb{1}_B |\Psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}\big(\alpha|0\rangle_A + \beta|1\rangle_A\big)\big(\alpha^*\langle 0|_A + \beta^*\langle 1|_A\big)\big(|01\rangle_{AB} - |10\rangle_{AB}\big) \\ &= \frac{1}{\sqrt{2}}|\varphi\rangle_A \otimes \big(\alpha^*|1\rangle_B - \beta^*|0\rangle_B\big). \end{aligned}$$

Hence the (normalized) post measurement state if the outcome was $|\varphi\rangle_A$ is

$$-|\varphi\rangle_A \otimes |\varphi^\perp\rangle_B. \tag{S.2}$$

Likewise one can see that if Alice's outcome was $|\varphi^\perp\rangle_A$, then the state after the measurement is

$$|\varphi^\perp\rangle_A \otimes |\varphi\rangle_B. \tag{S.3}$$

We carried out these calculations for the most general measurement basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ and conclude that whenever Alice measures with outcome $|\varphi\rangle_A$, then the state on Bob's side is the orthogonal state to $|\varphi\rangle$, which we denoted $|\varphi^\perp\rangle$. Notice that the global phase (-1) in Eq. S.2 can be neglected as global phases are not physically relevant.

(b) Suppose Alice wants to communicate one bit to Bob instantaneously, i.e. she wants to signal one bit to Bob. She encodes the bit in her measurement choice. Measuring in the basis $\{|0\rangle, |1\rangle\}$ corresponds to a bit value of 0 and measuring in the basis $\{|+\rangle, |-\rangle\}$ corresponds to the value 1.

Bob knows that Alice measures in one of those bases (because that is what they agreed on in advance). He makes use of that knowledge by cloning his qubit n times using $\mathcal{C}$ and measuring half of the clones in the $\{|0\rangle, |1\rangle\}$ basis and the other half in the $\{|+\rangle, |-\rangle\}$ basis. If Alice measured in $\{|0\rangle, |1\rangle\}$ then Bob's clones will all be either $|1\rangle$ (if Alice's outcome was 0) or $|0\rangle$ (if Alice obtained outcome 1). Hence the first half of the measured clones will all give the same outcome whereas the second half will produce random outputs. On the other hand, if Alice measured $\{|+\rangle, |-\rangle\}$ the outcomes of the first half of Bob's measurements will be random and the second half will all be the same (either 0, corresponding to $+$, or 1, corresponding to $-$).

To sum up, Alice can influence the measurement statistics of Bob by choosing her measurement basis appropriately but without sending information carriers to Bob. This is signalling.

Now to the probability with which Bob cannot tell the measurement choice of Alice. This happens when the uniformly distributed half of the measurement outcomes are all the same (either 0 or 1). The probability for this to happen is

$$\mathbb{P}[\text{fail}] = 2\left(\frac{1}{2}\right)^{n/2}, \tag{S.4}$$

which vanishes exponentially fast as n grows. Therefore Bob can achieve to decode Alice's bit arbitrarily well by increasing the number of clones.

Notice that the actual measurement outcome of Alice is unimportant in this protocol.

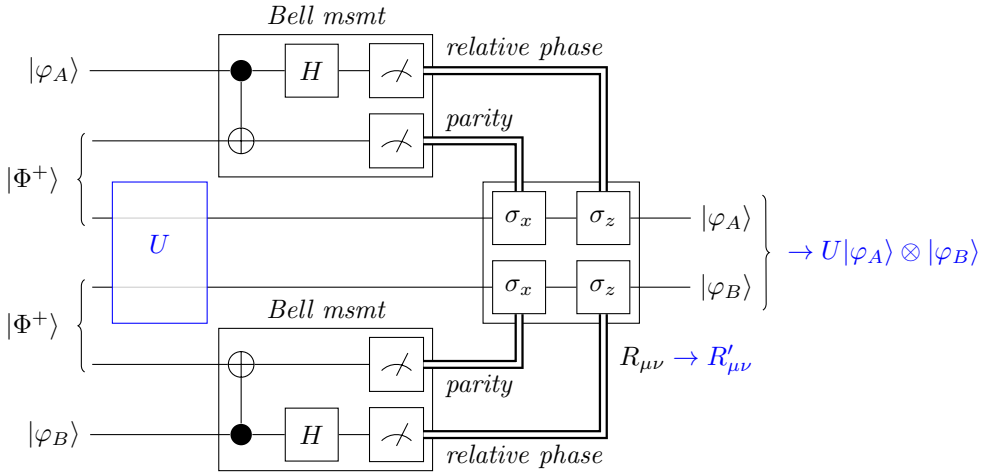
(c) Suppose Bob was not in possession of a cloning machine but instead Alice and Bob share n copies of the maximally entangled state $|\Psi^-\rangle$. One might think that this enables them to signal using the protocol from (b) but this is not the case. Now that Alice has n qubits it may make sense to say that she should measure all of them in one of the bases from above, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Depending on her choice Bob's qubits would then be in one of the states $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, respectively. However, not all of Bob's qubits would be in the same state as they are no longer clones but different post measurement states of the same measurement.

For instance, if Alice chose to measure in the basis $\{|0\rangle, |1\rangle\}$ and Bob would apply the same strategy as in (b) then all of his measurement outcomes would be random because now the outcomes on Alice's side do matter. Before they did not as Bob knew that all his qubits are in one and the same state. In essence, it is this promise/knowledge that enables signalling.

(d) There is no reason why Alice should restrict herself to choose one out of two bases only. Instead, she could choose from as many different measurement bases as desired. In this case, Bob adjusts his measurements of the clones such that he is able to distinguish all possible measurement bases. This is always possible because using the cloning machine (possibly recursively before measuring) he can produce as many clones as he needs to decode Alice's measurement basis.

Exercise 2. *Teleportation through a two-qubit gate*

As shown in the lecture, by a modification of the standard teleportation scheme, one can apply a gate U during the teleporation process. This can be done even for multi-qubit gates. For two qubits, it looks as follows:



Without the U gate, this would simply be ordinary teleportation of two qubits in parallel. In this case, the rotations $R_{\mu\nu} = \sigma_\mu \otimes \sigma_\nu$ that have to be applied to the output qubits depend on the outcome of the Bell measurements as usual:

$$|\Phi^+\rangle \to \sigma_\mu/\sigma_\nu = 1\,, \quad |\Phi^-\rangle \to \sigma_\mu/\sigma_\nu = \sigma_x\,, \quad |\Psi^+\rangle \to \sigma_\mu/\sigma_\nu = \sigma_y\,, \quad |\Psi^-\rangle \to \sigma_\mu/\sigma_\nu = \sigma_z\,.$$

Simply by applying the gate U to the teleportation target beforehand would not give us the desired output $U|\varphi_A\rangle \otimes |\varphi_B\rangle$. Instead the set of output rotations $R_{\mu\nu}$ has to be modified as well.

(a) *For a general U, find the set of output rotations $R'_{\mu\nu}$ such that we get the desired output.*

(b) *What could be the advantages and disadvantages of such a scheme, compared to direct application of U.*

(c) *Find $R'_{\mu\nu}$ for $U = \mathrm{CNOT}$.*
Hint: *It might be useful to write* $\mathrm{CNOT} = [|\uparrow\rangle\langle\uparrow| \otimes 1 + |\downarrow\rangle\langle\downarrow| \otimes \sigma_x]$ *and then perform the conjugation on control and target qubits separately.*

Solution.

(a) Knowing that $R_{\mu\nu}|\mathrm{in}\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$ (without U applied), one can see that the modified rotation is given by conjugation with $U^\dagger$:

$$R'_{\mu\nu}\, U|\mathrm{in}\rangle = U R_{\mu\nu} U^\dagger U|\mathrm{in}\rangle = U|\varphi_A\rangle \otimes |\varphi_B\rangle \tag{S.5}$$

(b) Applying U to a known input is possibly easier than applying U to a general state. Furthermore, one can verify correct preparation of the auxillaries $(1 \otimes U \otimes 1)\, |\Phi^+\rangle \otimes |\Phi^+\rangle$ ahead of time, not risking the possibly 'expensive' input qubits $|\varphi\rangle_A$ and $|\varphi\rangle_B$.

However, the conjugated rotation gate $R'_{\mu\nu} = U R_{\mu\nu} U^\dagger$ is in general more difficult to implement than $R_{\mu\nu}$, but it turns out it's still easier than U for many important gates.

Another advantage comes in conjunction with fault tolerant application of gates on stabiliser codes, which gets simplified by this scheme.

(c) If we write $R_{\mu\nu} = \sigma_\mu \otimes \sigma_\nu$, then we find

$$\begin{aligned} R'_{\mu\nu} = {} & |\uparrow\rangle\langle\uparrow|\sigma_\mu|\uparrow\rangle\langle\uparrow| \otimes 1\sigma_\nu 1 + |\uparrow\rangle\langle\uparrow|\sigma_\mu|\downarrow\rangle\langle\downarrow| \otimes 1\sigma_\nu\sigma_x \\ & + |\downarrow\rangle\langle\downarrow|\sigma_\mu|\uparrow\rangle\langle\uparrow| \otimes \sigma_x\sigma_\nu 1 + |\downarrow\rangle\langle\downarrow|\sigma_\mu|\downarrow\rangle\langle\downarrow| \otimes \sigma_x\sigma_\nu\sigma_x. \end{aligned} \tag{S.6}$$

With this expansion, we can analyse each term on a per-qubit basis.

Remember the properties of the Pauli matrices

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = -i\sigma_x\sigma_y\sigma_z = 1. \tag{S.7}$$

For the control qubit, we find either $|\uparrow\rangle\langle\uparrow|$ or $|\downarrow\rangle\langle\downarrow|$ next to the σ_μ.

	σ_μ	$\lvert\uparrow\rangle\langle\uparrow\rvert\sigma_\mu\lvert\uparrow\rangle\langle\uparrow\rvert$	$\lvert\uparrow\rangle\langle\uparrow\rvert\sigma_\mu\lvert\downarrow\rangle\langle\downarrow\rvert$	$\lvert\downarrow\rangle\langle\downarrow\rvert\sigma_\mu\lvert\downarrow\rangle\langle\downarrow\rvert$
$\lvert\Phi^+\rangle_c \to$	1	$\lvert\uparrow\rangle\langle\uparrow\rvert$	0	$\lvert\downarrow\rangle\langle\downarrow\rvert$
$\lvert\Phi^-\rangle_c \to$	σ_x	0	σ_+	0
$\lvert\Psi^+\rangle_c \to$	σ_y	0	$-i\sigma_+$	0
$\lvert\Psi^-\rangle_c \to$	σ_z	$\lvert\uparrow\rangle\langle\uparrow\rvert$	0	$-\lvert\downarrow\rangle\langle\downarrow\rvert$

For the target qubit, we either find 1 or σ_x next to the σ_ν.

	σ_ν	$1\cdot\sigma_\nu\cdot 1$	$1\cdot\sigma_\nu\cdot\sigma_x$	$\sigma_x\cdot\sigma_\nu\cdot\sigma_x$
$\lvert\Phi^+\rangle_t \to$	1	1	σ_x	1
$\lvert\Phi^-\rangle_t \to$	σ_x	σ_x	1	σ_x
$\lvert\Psi^+\rangle_t \to$	σ_y	σ_y	$-i\sigma_z$	$-\sigma_y$
$\lvert\Psi^-\rangle_t \to$	σ_z	σ_z	$i\sigma_y$	$-\sigma_z$

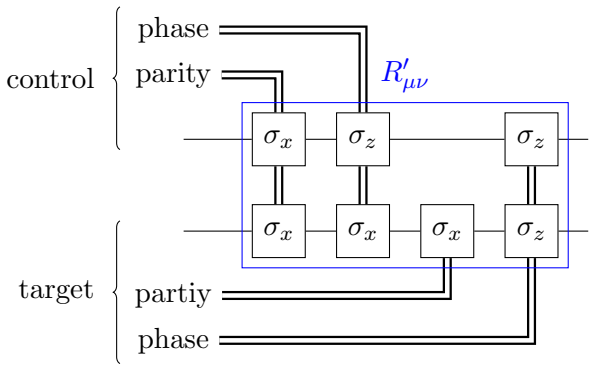
Using those results as a basis, it is straight forward to calculate the entries of $R'_{\mu\nu}$. For example, we find

$$\begin{aligned}
R'_{zx} &= |\uparrow\rangle\langle\uparrow| \otimes \sigma_x - |\downarrow\rangle\langle\downarrow| \otimes \sigma_x && = \sigma_z \otimes \sigma_x \\
R'_{zy} &= |\uparrow\rangle\langle\uparrow| \otimes \sigma_y + |\downarrow\rangle\langle\downarrow| \otimes \sigma_y && = 1 \otimes \sigma_y \\
R'_{xx} &= \sigma_+ \otimes 1 + \sigma_- \otimes 1 && = \sigma_x \otimes 1 \\
R'_{xz} &= i\sigma_+ \otimes \sigma_y - i\sigma_- \otimes \sigma_y && = -\sigma_y \otimes \sigma_y
\end{aligned}$$

The complete set of gates that has to be applied (global phases are of course irrelevant) is then

	$\|\Phi^+\rangle_t$	$\|\Phi^-\rangle_t$	$\|\Psi^+\rangle_t$	$\|\Psi^-\rangle_t$
$\|\Phi^+\rangle_c$	$1 \otimes 1$	$1 \otimes \sigma_x$	$\sigma_z \otimes \sigma_y$	$\sigma_z \otimes \sigma_z$
$\|\Phi^-\rangle_c$	$\sigma_x \otimes \sigma_x$	$\sigma_x \otimes 1$	$\sigma_y \otimes \sigma_z$	$-\sigma_y \otimes \sigma_y$
$\|\Psi^+\rangle_c$	$\sigma_y \otimes \sigma_x$	$\sigma_y \otimes 1$	$-\sigma_x \otimes \sigma_z$	$\sigma_x \otimes \sigma_y$
$\|\Psi^-\rangle_c$	$\sigma_z \otimes 1$	$\sigma_z \otimes \sigma_x$	$1 \otimes \sigma_y$	$1 \otimes \sigma_z$

In fact, that even translates quite nicely into single classical bit controlled gates, as illustrated in this circuit:



For CNOT, $R'_{\mu\nu}$ consists solely of single qubit rotations. This is true for any unitary U from the Clifford group (defined as exactly those operators that transform Paulis into Paulis under conjugation), which contains for example H, P (single qubit) and CNOT (two qubit).

The Cliffords are not universal, thus some operators will involve more complicated $R'_{\mu\nu}$. But in the case of e.g. $\mathrm{diag}(1, 1, 1, i)$ or Toffoli, $R'_{\mu\nu}$ will be in the Clifford group, thus these can be implemented using a two-level nested application of teleportation through gates.