4.2 No-cloning theorem

For different computational reasons, one would like to create an independent and identical copy of an arbitrary state with a unitary operation. Nevertheless, the following theorem prevents it.

Theorem 4.1 (No-cloning).
Consider two quantum systems $\mathcal{A}$ and $\mathcal{B}$ with corresponding Hilbert spaces of the same dimensions $\mathbb{H}_{\mathcal{A}}$ and $\mathbb{H}_{\mathcal{B}}$. Then, it is not possible to construct a unitary operation $\hat{U}$ acting on $\mathbb{H}_{\mathcal{A}} \otimes \mathbb{H}_{\mathcal{B}}$ that copies an arbitrary state of $\mathcal{A}$ over an initial, reference state of $\mathcal{B}$. Namely, $\nexists \hat{U}$ such that

$$\hat{U} |\psi\rangle |e\rangle = |\psi\rangle |\psi\rangle , \tag{4.25}$$

where $|\psi\rangle$ is an arbitrary state and $|e\rangle$ is a reference state.

Proof. A simple proof goes as follows. Suppose there exists $\hat{U}$ such that described in Eq. (4.25). Then, one considers the scalar product between the state $|\psi, e\rangle = |\psi\rangle |e\rangle$ and $|\phi, e\rangle = |\phi\rangle |e\rangle$, where $|\phi\rangle$ is a second arbitrary state. This gives

$$\langle \phi, e | \psi, e \rangle = \langle \phi | \psi \rangle \langle e | e \rangle . \tag{4.26}$$

Exploiting the unitarity of $\hat{U}$, we have

$$\langle \phi, e | \psi, e \rangle = \langle \phi, e | \hat{U}^\dagger \hat{U} | \psi, e \rangle \tag{4.27}$$

Now, we apply Eq. (4.25) to both these states:

$$\langle \phi, e | \hat{U}^\dagger \hat{U} | \psi, e \rangle = \langle \phi, \phi | \psi, \psi \rangle = \langle \phi | \psi \rangle^2 . \tag{4.28}$$

By putting together the last three expressions we find

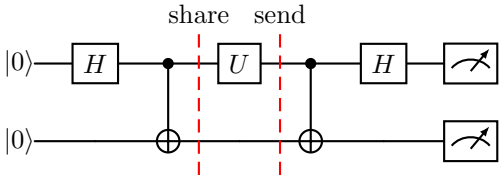
$$\langle \phi | \psi \rangle \langle e | e \rangle = \langle \phi | \psi \rangle^2 , \tag{4.29}$$

which holds true only if $\langle \phi | \psi \rangle = 0$ or $|\phi\rangle = e^{i\alpha(\phi,\psi)} |\psi\rangle$ with $\alpha(\phi, \psi)$ being a phase possibly depending on the two input states. In both cases, one does not allow for full arbitrariness, thus proving the no-cloning theorem.

Importantly for the quantum computation field, the no-cloning theorem prevents the employment of classical error correction techniques on quantum states. One needs to employ quantum error corrections, which will be subject of Chapter 7, that effectively circumvent the no-cloning theorem.

4.3 Dense coding

An interesting quantum algorithm is that of dense coding. Suppose Alice has two classical bits x and y that wants to communicate (securely) to Bob, and wants to do it only via a single qubit. The following protocol allows for it. It assumes to have two qubits on which six operations are performed:



(4.30)

The first operation is to prepare an initial entangled state

$$|0\rangle|0\rangle \xrightarrow{\hat{H}\otimes\hat{\mathbb{1}}} \tfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle \xrightarrow{CNOT} \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle) = |\psi_+\rangle\,. \tag{4.31}$$

The second operation is to share the state among Alice (qubit 0) and Bob (qubit 1). Then, the third operation is the encoding: Alice encodes the state of (x, y) in the operation performed with the gate $\hat{U}$:

x, y	$\hat{U}$
$0, 0$	$\hat{\mathbb{1}} \otimes \hat{\mathbb{1}}$
$0, 1$	$\hat{\sigma}_x \otimes \hat{\mathbb{1}}$
$1, 0$	$\hat{\sigma}_z \otimes \hat{\mathbb{1}}$
$1, 1$	$i\hat{\sigma}_y \otimes \hat{\mathbb{1}}$

This leads to

$$|\psi_+\rangle \xrightarrow{\hat{U}\otimes\hat{\mathbb{1}}} \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle) = |\psi_+\rangle\,, & \text{if } (x,y)=(0,0), \\ \frac{1}{\sqrt{2}}(|1\rangle|0\rangle+|0\rangle|1\rangle) = |\phi_+\rangle\,, & \text{if } (x,y)=(0,1), \\ \frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle) = |\psi_-\rangle\,, & \text{if } (x,y)=(1,0), \\ \frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle) = |\phi_-\rangle\,, & \text{if } (x,y)=(1,1), \end{cases} \tag{4.32}$$

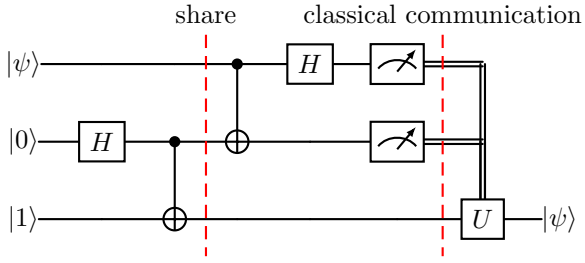
where $|\psi_\pm\rangle$ and $|\phi_\pm\rangle$ are the four Bell states (fully entangled state, being a basis of the common Hilbert space). The fourth operation consists in Alice sending the qubit 0 to Bob. Any operation performed on the two qubits by Bob is now fully local. The fifth operation is the decoding. Bob applies the last two operations (CNOT and $\hat{H}\otimes\hat{\mathbb{1}}$) which together form the inverse operation of the encoding:

$$\begin{aligned} |\psi_+\rangle &\to |0\rangle|0\rangle\,, \\ |\phi_+\rangle &\to |0\rangle|1\rangle\,, \\ |\psi_-\rangle &\to |1\rangle|0\rangle\,, \\ |\phi_-\rangle &\to |1\rangle|1\rangle\,. \end{aligned} \tag{4.33}$$

The last operation is to Bob to measure the state of both qubits, which will identify which bits Alice encoded in her qubit.

4.4 Quantum teleportation

An application of the dense coding protocol is the quantum teleportation, that allows for sending a generic state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ from Alice to Bob without knowing a priory the state. The protocol is based on the use of three qubits and six operations:



(4.34)

The first operation is to prepare an entangled state between qubit 1 and 2 (similarly as in the dense coding protocol):

$$|\psi 01\rangle \xrightarrow{\hat{\mathbb{1}}\otimes\hat{H}\otimes\hat{\mathbb{1}}} |\psi\rangle\tfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|1\rangle \xrightarrow{\hat{\mathbb{1}}\otimes CNOT} |\psi\rangle\tfrac{1}{\sqrt{2}}(|01\rangle+|10\rangle) = |\psi\rangle|\phi_+\rangle\,. \tag{4.35}$$

Then, the second operation is to shared the qubits among Alice (qubit 0 and 1) and Bob (qubit 2). The third operation consists in applying a decoding operation (see dense coding) to the first two qubits. Namely, the decoding operation acts as in Eq. (4.33). Thus, owning that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, one obtains

$$\begin{aligned} |\psi\rangle|\phi_+\rangle &\xrightarrow{CNOT\otimes\hat{\mathbb{1}}} \tfrac{1}{\sqrt{2}}\left[\alpha|0\rangle(|01\rangle+|10\rangle)+\beta|1\rangle(|11\rangle+|00\rangle)\right] \\ &\xrightarrow{\hat{H}\otimes\hat{\mathbb{1}}\otimes\hat{\mathbb{1}}} \tfrac{1}{2}\left[|00\rangle(\alpha|1\rangle+\beta|0\rangle)+|01\rangle(\alpha|0\rangle+\beta|1\rangle)+|10\rangle(\alpha|1\rangle-\beta|0\rangle)+|11\rangle(\alpha|0\rangle-\beta|1\rangle)\right]. \end{aligned} \tag{4.36}$$

The fourth operation consists in Alice measuring her qubits. There are 4 possible couples, and thus four possible collapses (according to the measurement postulate of quantum mechanics). These are $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ with probability $1/4$ each. The fundamental point of the protocol is that the collapse of the state of the first 2 qubit implies that of the last qubit, being in Bob's hands. In particular, if Alice measures the couple $(0,0)$, then qubit 2 collapses in $\alpha|1\rangle + \beta|0\rangle$; and similarly for the other three measurement outcomes. The fifth operation is the classical communication of the outcomes of the measurement to Bob. Consequently, the sixth operation is a unitary operation $\hat{U}$ on qubit 2 that depends on the outcomes (q_0 and q_1) of the measurement:

q_0	q_1	$\lvert q_2\rangle$	$\hat{U}$
0	0	$\alpha\lvert1\rangle+\beta\lvert0\rangle$	$\hat{\sigma}_x$
0	1	$\alpha\lvert0\rangle+\beta\lvert1\rangle$	$\hat{\mathbb{1}}$
1	0	$\alpha\lvert1\rangle-\beta\lvert0\rangle$	$i\hat{\sigma}_y$
1	1	$\alpha\lvert0\rangle-\beta\lvert1\rangle$	$\hat{\sigma}_z$

(4.37)

where $|q_2\rangle$ is the state on which qubit 2 has collapsed after the measurement. By applying the unitary we obtain

$$\begin{aligned} \alpha|1\rangle+\beta|0\rangle &\xrightarrow{\hat{\sigma}_x} |\psi\rangle, \\ \alpha|0\rangle+\beta|1\rangle &\xrightarrow{\hat{\mathbb{1}}} |\psi\rangle, \\ \alpha|1\rangle-\beta|0\rangle &\xrightarrow{i\hat{\sigma}_y} |\psi\rangle, \\ \alpha|0\rangle-\beta|1\rangle &\xrightarrow{\hat{\sigma}_z} |\psi\rangle. \end{aligned} \tag{4.38}$$

In such a way, Bob retrieves the state $|\psi\rangle$ without that neither Bob or Alice had measure it.

We notice that there is a strong difference with the case studied in the no cloning theorem. Here, one needs to measure two qubits to perform the protocol: this a fundamentally different procedure with respect to a unitary operation.