# An introduction to quantum information and computation

A.y. 2023/24 – Leonardo Mazza – leonardo.mazza@universite-paris-saclay.fr

## Lecture 2: Two qubits.

### 1) The Hilbert space of two qubits.

We have seen that a qubit is a quantum 2-level system. It is defined throug 2 orthonormal states, $\{|0\rangle, |1\rangle\}$, which constitute a basis, often called computational basis. The Hilbert space for 1 qubit, $\mathcal{H}_1$, is the linear space generated by this basis: $\mathcal{H}_1 = \text{Span}\{|0\rangle, |1\rangle\}$.

For two qubits, we have already seen during the lectures of quantum mechanics I that the Hilbert space is the tensor product of two Hilbert spaces for one qubit: $\mathcal{H}_2 \doteq \mathcal{H}_1 \otimes \mathcal{H}_1$. In practice, the best and easiest thing is to think at the canonical basis of $\mathcal{H}_2$. For 2 qubits, there are four states that I surely need to consider

$$|00\rangle \qquad |01\rangle \qquad |10\rangle \qquad |11\rangle$$

and because of the principle of q. mechanics according to which a linear combination of physical states is also a physical state, I obtain the most generic 2-qubits state:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$\text{with } \alpha, \beta, \gamma, \delta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

This leads to a standard vector representation of $|\psi\rangle$:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

The Hilbert space $\mathcal{H}_2$ has dimension $4 = 2 \times 2$.

$$\dim \mathcal{H}_2 = \dim \mathcal{H}_1 \times \dim \mathcal{H}_1$$

Be careful: $4 = 2+2$ but the correct general rule is $4 = 2 \times 2$ !

The orthonormal basis:

$$\{ |00\rangle, \; |01\rangle, \; |10\rangle, \; |11\rangle \}$$

is called "canonical" or "tensor-product basis".

It is customary to interpret each of the vectors of the basis as a tensor product of the vectors; for instance:

$$|00\rangle = |0\rangle \otimes |0\rangle$$

This has a natural matrix interpretation:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

For two generic vectors:

$$|v\rangle \otimes |u\rangle = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \otimes \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = \begin{pmatrix} v_0 \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \\ v_1 \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} v_0 u_0 \\ v_0 u_1 \\ v_1 u_0 \\ v_1 u_1 \end{pmatrix}$$

## 2) Quantum gates for two qubits.

When we discuss q-gates $U$ for a 2-qubit system, we need to distinguish two cases:

A) the case when they act on only one of the two qubits;

B) the case when they act on two qubits jointly.

In both cases, however, there is an important point to keep in mind: $U$ should be a unitary operator.

CASE A: The action on a single qubit.

Consider the single-qubit gate $U$, and let us act with this on the first qubit (remember, it is customary to enumerate the qubits from right to left):

$$|\psi_1\rangle \otimes |\psi_0\rangle \longrightarrow |\psi_1\rangle \otimes \left( U_1 |\psi_0\rangle \right) = |\psi_1\rangle \otimes |\psi_0'\rangle.$$

How to write this as a 2-qubit operation? Simple! just observe that we did not do anything to the second qubit.

$$\left(\mathbb{1} \otimes U_1\right) |\psi_1\rangle \otimes |\psi_0\rangle = \left(\mathbb{1} |\psi_0\rangle\right) \otimes \left(U_1 |\psi_0\rangle\right) = |\psi_1\rangle \otimes |\psi_0'\rangle$$

We can give to $\mathbb{1} \otimes U_1$ a $4\times 4$ matrix representation. If we take for instance $\mathbb{1} \otimes \sigma_z$:

$$\mathbb{1} \otimes \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & 0\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ 0\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & 1\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

Exercise: Check its action on the vectors $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

Obviously, if the single-qubit gate acts on the second qubit, we will use $U_1 \otimes \mathbb{1}$.

CASE B: The joint action on two qubits.

Take for instance a two-qubit quantum gate, $U_1$ and $U_1'$

$$U_2 = U_1 \otimes U_1'$$

acts jointly on two qubits:

$$U_2 |\psi_1\rangle \otimes |\psi_0\rangle = U_1|\psi_1\rangle \otimes U_1'|\psi_0\rangle = |\psi_1'\rangle \otimes |\psi_0'\rangle$$

An example: $U_2 = \sigma_z \otimes \sigma_z$. The action on the standard basis is rather simple:

$$\begin{cases} \sigma_z \otimes \sigma_z |00\rangle = +|00\rangle \\ \sigma_z \otimes \sigma_z |01\rangle = -|01\rangle \\ \sigma_z \otimes \sigma_z |10\rangle = -|10\rangle \\ \sigma_z \otimes \sigma_z |11\rangle = +|11\rangle \end{cases}$$

Note that there are 2-qubit gates that cannot be written as $U_1 \otimes U_1'$. Example: the CNOT, or controlled NOT

$$\begin{cases} U_{CNOT} |00\rangle = |00\rangle \\ U_{CNOT} |01\rangle = |01\rangle \\ U_{CNOT} |10\rangle = |11\rangle \\ U_{CNOT} |11\rangle = |10\rangle \end{cases}$$

NOT operation on the first qubit depending on the state of the second qubit.

$$U_{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x .$$

Matrix representation: $U_{CNOT} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$.

We can similarly define the C-PHASE gate:

$$U_{C-\varphi} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes P_\varphi = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{i\varphi} \end{pmatrix}.$$

Exercise: Show that $U_2 = U_1 \otimes U_1'$ is a unitary operator.

## 3) The no-cloning theorem.

The no-cloning theorem states that it is impossible to make a copy of an unknown quantum state using a 2-qbit quantum gate.

Idea: Given the initial state $|\psi\rangle \otimes |0\rangle$ we look for a two-qubit quantum gate $U_{copy}$ such that:

$$U_{copy} \, |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle .$$

It has been proven in the '60s and then rediscovered in the '80s that $U_{copy}$ does not exist. (Wootters and Zurek 1982, Dieck 1982).

Important: $U_{copy}$ should be unitary, otherwise it is not a quantum gate.

PROOF: take two generic 1qbit states, $|\psi\rangle$ and $|\phi\rangle$; and construct the 2-qubit states $|\psi\rangle\otimes|0\rangle$ and $|\phi\rangle\otimes|0\rangle$.

The scalar product of these states is:

$$① \quad \left(\langle\psi|\otimes\langle 0|\right)\left(|\phi\rangle\otimes|0\rangle\right) = \langle\psi|\phi\rangle \otimes \langle 0|0\rangle = \langle\psi|\phi\rangle$$

$$② \quad \left(\langle\psi|\otimes\langle 0|\right)\left(|\phi\rangle\otimes|0\rangle\right) = \left(\langle\psi|\otimes\langle 0|\right) U^{\dagger}_{copy} \, U_{copy} \left(|\phi\rangle\otimes|0\rangle\right)$$

$$= \left(\langle\psi|\otimes\langle\psi|\right)\left(|\phi\rangle\otimes|\phi\rangle\right)$$

$$= \left(\langle\psi|\phi\rangle\right)^2 .$$

Hence: $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$, which implies $\langle\psi|\phi\rangle = 0, 1$.

But $|\psi\rangle$ and $|\phi\rangle$ where generic, hence in general $\langle\psi|\phi\rangle \neq 0, 1$. We got an absurd. $U_{copy}$ does not exist.

Important: specific states can be copied. For a given $|\psi\rangle$ there is a unitary $U_{copy, |\psi\rangle}$ such that

$$U_{copy,|\psi\rangle} \, |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$$

But if you consider $|\phi\rangle \neq |\psi\rangle$ we get

$$U_{copy,|\psi\rangle} \, |\phi\rangle \otimes |0\rangle \neq |\phi\rangle \otimes |\phi\rangle .$$

Remark: this is not the case in classical computing. You can produce the back-up of your hard-disk!

Obviously, the no-cloning theorem has fundamental consequences in the context of secure communication, because it makes impossible for a eavesdropper (a spy) to copy the quantum state that is communicated between Alice and Bob.

The same "game" can be played for single-qubit observables, using the Hermitian observable:

$$\mathbb{1} \otimes A_1 \quad \text{or} \quad A_1 \otimes \mathbb{1} .$$

## 4) Two-qubit measurements.

At this stage, one could believe that 2-qubit physics is just a simple generalisation of the 1-qubit computation, and that is carried out in a similar fashion:

| | | | |
|---|---|---|---|
| • INITIALIZATION | $\|0\rangle$ | or | $\|00\rangle$ |
| • EXECUTION OF THE QUANTUM GATES (the quantum circuit) | $U_1\|0\rangle$ | or | $U_2\|00\rangle$ |

In both cases the gates are unitary operation that amount at rotations in the Hilbert space.

| | | | |
|---|---|---|---|
| • MEASUREMENT Perform a measurement in the $\sigma_z$ basis and get with a certain probability. | $\{0,1\}$ | or | $\{00, 01, 10, 11\}$ |

What we are going to discuss is that the 2-qubit situation is qualitatively richer than the 1-qubit one because it is possible to measure just one of the qubits...

Let us begin with a simple example, considering the state:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

What happens if we measure just one of the qubits? For instance, the first one (remember to count qubits from right to left.
Let me rewrite:

$$|\psi\rangle = (\alpha|0\rangle + \gamma|1\rangle) \otimes |0\rangle + (\beta|0\rangle + \delta|1\rangle) \otimes |1\rangle$$

We now measure $\sigma_z$ for the second qubit. Two eigenvalues and eigenvectors are possible:

$\{+1, |0\rangle\}$ and $\{-1, |1\rangle\}$.

What happens to the second qubit?

CASE $+1 \longrightarrow$ $$|\psi\rangle = \frac{1}{\sqrt{|\alpha|^2+|\gamma|^2}}\left(\alpha|0\rangle+\gamma|1\rangle\right)\otimes|0\rangle$$
$$= \frac{1}{\sqrt{|\alpha|^2+|\gamma|^2}}\left(\alpha|00\rangle+\gamma|10\rangle\right)$$

CASE $-1 \longrightarrow$ $$|\psi\rangle = \frac{1}{\sqrt{|\beta|^2+|\delta|^2}}\left(\beta|0\rangle+\delta|1\rangle\right)\otimes|1\rangle$$
$$= \frac{1}{\sqrt{|\beta|^2+|\delta|^2}}\left(\beta|01\rangle+\delta|11\rangle\right)$$

We are in front of a phenomenon of partial collapse that is crucial in quantum computing.

When is partial collapse interesting? When the state before collapse is entangle, that is, not separable.

SEPARABLE two qubit state: A state $|\psi\rangle$ that can be written in the form $|\psi\rangle = |\psi_2\rangle\otimes|\psi_1\rangle$.

ENTANGLED two qubit state: A state that is not separable.

Interesting fact: For $\mathcal{H}_2$, the Hilbert space of 2 qubits, we can present a basis of separable states but also a basis of entangled states.

Basis of separable states:

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

called the computational basis or tensor-product basis.

Basis of entangled states:

$$\left\{\frac{|00\rangle+|11\rangle}{\sqrt{2}}, \frac{|00\rangle-|11\rangle}{\sqrt{2}}, \frac{|01\rangle+|10\rangle}{\sqrt{2}}, \frac{|01\rangle-|10\rangle}{\sqrt{2}}\right\}$$

called Bell basis.

Fact: given a state $|\Psi\rangle$, if we measure $\sigma_z$ on one of the qubits, the state after the measurement is a separable state. This means that the partial collapse of the wavefunction produces a separable state.

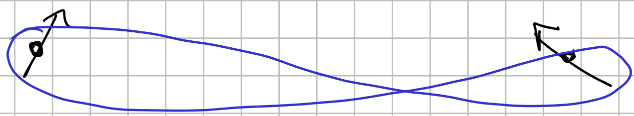
This has important implications if the state $|\Psi\rangle$ was entangled. A local action (local here means "on just one qubit) has a non-local effect (it changes a property of the global two-qubit state as a whole).

## 5) Quantum dense coding.

We now use the possibility of creating 2-qubit entangled states to do things that are impossible in classical physics.

IDEA

Alice (A) and Bob (B)



share a 2-qubit state $|\Psi\rangle$.

One qubit is with Alice and one qubit is with Bob.

A and B can communicate with classical means (a telephone) and can manipulate or measure their qubit at will. No joint action on the qubit is possible.

Goal: Bob wants to communicate to Alice two bits of information. which is a message like 00 or 01, or 10 or 11.

CLASSICAL PROCEDURE. Bob decides the message, for instance "10", takes two bits, prepares them in the 10 state and sends them to Alice.

QUANTUM PROCEDURE. Let us make very clear that also in this case it is necessary to use 2 qubits. It is not possible to send a message like "10" with a single qubit. We now show that in the quantum case this can be done in a novel and unusual way. This procedure is called quantum dense coding.

Step 1. Alice and Bob prepare one Bell state, for instance

$$|B_0\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

and share it: Alice has the first qubit, Bob has the second.

Step 2. Alice can operate a single-qubit gate on the first qubit (first from right to left) and can create any of the four Bell states:

- $\mathbb{1}_0 |B_0\rangle = |B_0\rangle$
- $\sigma_{z,0} |B_0\rangle = \frac{1}{\sqrt{2}}\left(-|01\rangle - |10\rangle\right) = -\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$
- $\sigma_{x,0} |B_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$
- $\sigma_{y,0} |B_0\rangle = \frac{1}{\sqrt{2}}\left(-i|00\rangle - i|11\rangle\right) = -i\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

This result is extraordinary! It means that Alice, acting only on her qubit, can explore the entire 4-dimensional Hilbert space. This would not be possible in the classical context: from the 2-bit configuration "11" she can only create the configuration "10". She cannot explore the full space of messages, such as "00" or "01". The same is true for an initial 2-qubit state that is separable. For instance, from $|11\rangle$ she can only create states of the form $\alpha|11\rangle + \beta|10\rangle$.

Alice associate a message to any of the four Bell states:

"00" $\longleftrightarrow -\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ "10" $\longleftrightarrow -\frac{i}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$

"01" $\longleftrightarrow \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$ "11" $\longleftrightarrow \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$

Depending on the message that she wants to send, she creates the corresponding Bell state.
For instance, in order to transmit the message "10" she applies $\sigma_x$ to her qubit and creates

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

Step 3 Alice sends her qubit to Bob.

Step 4 Bob decodes the information withe the following quantum circuit

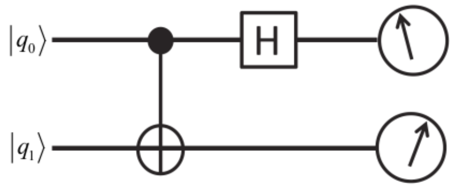



Figure 4.8: Bell-basis measurement circuit comprising a Bell state decoder with a CNOT and Hadamard gate followed by measurement in the computational basis. This circuit permits measurement of which Bell state a pair of qubits is in by mapping the states to the standard basis of eigenstates of $\sigma_0^z$ and $\sigma_1^z$.

We are using here the standard graphical representation of the CNOT

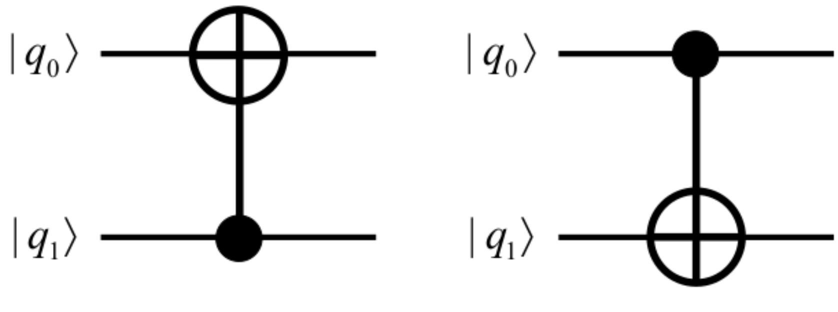



Figure 4.2: Quantum circuit representation of the $\mathrm{CNOT}_1$ operation (left panel) and the $\mathrm{CNOT}_0$ operation (right panel). The filled circle denotes the control qubit (in the left panel, $q_1$) and the symbol $\oplus$ denotes the target qubit (in the left panel, $q_0$) for the gate. The right panel shows the gate with control and target interchanged. In quantum circuit notation the order in which gates are applied ('time') runs from left to right. If the circuit has $\mathrm{GATE}_1$ followed by $\mathrm{GATE}_2$, reading from left to right, this corresponds to the (right-to-left) sequence of matrix operations $\mathrm{GATE}_2\ \mathrm{GATE}_1|\mathrm{INPUT\ STATE}\rangle$. For the $\widetilde{\mathrm{CNOT}}$ gate the control is shown as an open, rather than filled, circle. This denotes the operation being activated by the control being in 0 rather than 1.

After the application of the decoding circuit, Bob obtains:

| Message encoded by Alice | | State prepared by Alice with a single-qubit operation | | State decoded by Bob with the the decoding circuit |
|---|---|---|---|---|
| "00" | $\longleftrightarrow$ | $-\frac{1}{\sqrt{2}}\left(\lvert 00\rangle + \lvert 11\rangle\right)$ | $\longleftrightarrow$ | $-i\lvert 00\rangle$ |
| "01" | $\longleftrightarrow$ | $\frac{1}{\sqrt{2}}\left(\lvert 00\rangle - \lvert 11\rangle\right)$ | $\longleftrightarrow$ | $+\lvert 01\rangle$ |
| "10" | $\longleftrightarrow$ | $-\frac{i}{\sqrt{2}}\left(\lvert 01\rangle + \lvert 10\rangle\right)$ | $\longleftrightarrow$ | $-\lvert 10\rangle$ |
| "11" | $\longleftrightarrow$ | $\frac{1}{\sqrt{2}}\left(\lvert 01\rangle - \lvert 10\rangle\right)$ | $\longleftrightarrow$ | $-\lvert 11\rangle$ |

<u>Step 5</u>: Bob measures $\sigma_z$ on the two qubit he has. He gets the message encoded by Alice. Note that the phases appearing in the third column do not play any role when it comes to measuring the state of the qubits.

What is remarkable about the quantum dense coding?
Many things parallel the classical case: need of using two qubits, need of sending both qubits to Bob etc.
Two actions on the qubits are necessary in order to encode the info: the preparation of the Bell state and the actual encoding by Alice. What is truly remarkable is that the first action have been performed before choosing the message to send. Only one action needs to be performed after the message to send has been chosen.

## 6) The no-cloning theorem and superluminal communication.

Let us now show that the no-cloning theorem has a fundamental importance for the consistency of quantum theory with the relativity principle, which implies the impossibility of sending superluminal messages, namely to communicate at a speed that is faster than the speed of light.