TUTORIAL 1

1 Homework 1

1. A system X is either in the state $v_0 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ or $v_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$. We want to know which is the case. Describe a sequence of operations that determine which is the case.

2. Show that $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ is not a product state, ie. not of the form $v \otimes v'$ for some qubits v, v'. Such a state is said *entangled*.

2 Quantum Random Access Code

We want to encode 2 bits in a single qubit in such a way that we should be able to recover the information about the first bit only or the second bit only with a good probability of success. Formally:

Definition 2.1 (QRAC)**.** *A* quantum random access code *(QRAC) with success probability p is an encoding $f : \{0,1\}^2 \to \mathbb{C}^2$ (maps a pair of bits (x_1, x_2) into a quantum state $|f(x_1, x_2)\rangle$) and two unitaries U_1 and U_2 (U_i is the transformation we apply on the qubit $|f(x_1, x_2)\rangle$ to retrieve bit i) such that for all x_1, x_2:*

$$\mathbb{P}(\textit{Measure output } = x_1 | U_1 \textit{ was applied}) = |\langle x_1 | U_1 | f(x_1, x_2)\rangle|^2 \geq p$$
$$\mathbb{P}(\textit{Measure output } = x_2 | U_2 \textit{ was applied}) = |\langle x_2 | U_2 | f(x_1, x_2)\rangle|^2 \geq p$$

1. A classical random access code depicts the situation where you restrict yourself to encodings $f : \{0,1\}^2 \to \{0,1\}$, ie. encoding two bits into one bit. Then we aim to design a (probabilistic) strategy that, given $f(x_1, x_2)$, recover the information of either x_1 only or x_2 only. Show that such strategies cannot succeed with probability greater than 0.5.

2. How can you geometrically interpret a real unitary acting on real qubits?

3. Exhibit a quantum random access code with $p > 0.5$. What is the best you can achieve?
Hint : Plot the space of real qubits, and try to dispatch them the furthest appart, in such a way that two distinct unitaries can distinghuish them efficiently

3 No-cloning Theorem

1. Construct a circuit that "clones" any vector of the standard basis, ie that on input $|b\rangle \otimes |0\rangle$ for $b \in \{0,1\}$, outputs $|b\rangle \otimes |b\rangle$.

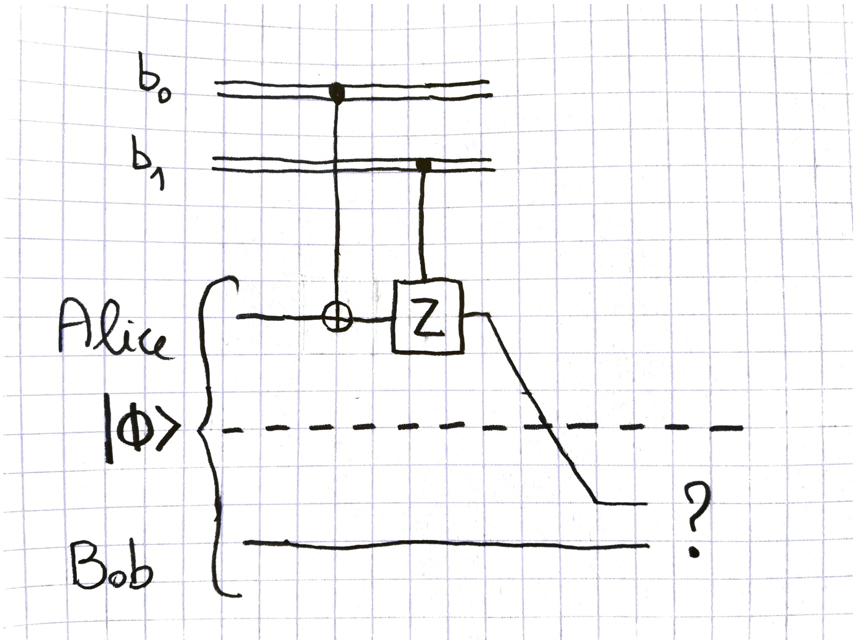
2. Apply your previous circuit to the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$, have you cloned the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

3. Prove the No-Cloning Theorem: there is no circuit that can clone any qubits, ie there is no 4×4 unitary matrix U such that for any $|\varphi\rangle \in \mathbb{C}^2$, $U \cdot |\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$.
Hint: suppose that such a U exists and proceed by contradiction. Remember that $U^\dagger U = I$ and try to rewrite $\langle\psi|\varphi\rangle$ differently.

4 Super-dense Coding

In this exercise, we will have two actors, Alice and Bob. Alice has two classical bits of information $(b_0, b_1) \in \{0,1\}^2$ and she want to send them to Bob.

1. What is the minimum number of classical bits that Alice has to send to Bob in order to communicate him (b_0, b_1)?
2. Now suppose that Alice and Bob share an entangled **EPR pair** (or **Bell pair**), that is to say there is a quantum state $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ such that the first qubit is owned by Alice (she can only perform operations of the form $U \otimes I$ on $|\phi\rangle$) and the second qubit is owned by Bob.
   Alice is going to perform operations on her qubit and send it to Bob. If $b_0 = 1$, she applies NOT $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (bit flip, also called X) and then if $b_1 = 1$ she applies $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (phase flip), she send her part of the qubit back to Bob.
   Explain how Bob can recover the values of b_0 and b_1 using $|\phi\rangle$.


b_0
b_1
Alice
Z
$|\Phi\rangle$
?
Bob