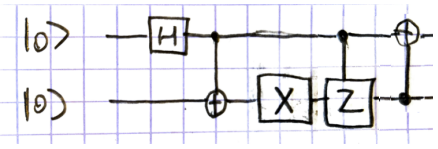
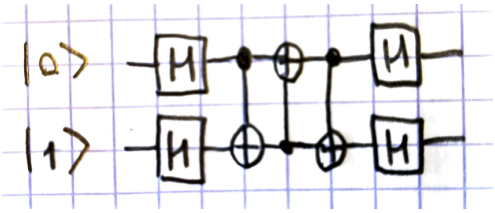
TUTORIAL 9

1 Some Small Calculations

1. Give the probability of each outcome when you measure $|\varphi\rangle$ in basis $\mathcal{B}$:
   (a) $|\varphi\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ and $\mathcal{B} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
   (b) $|\varphi\rangle = \frac{|00\rangle+(1-i)|10\rangle-|11\rangle}{2}$ and $\mathcal{B} = \left(|00\rangle, |01\rangle, \frac{|10\rangle+|11\rangle}{\sqrt{2}}, \frac{|10\rangle-|11\rangle}{\sqrt{2}}\right)$.
2. Compute the probability of measuring 1 on the first qubit of the following circuits:
   (a)
   

   (b)
   

3. Using a circuit computing $U_f^{\oplus} : |x\rangle|a\rangle|0\rangle \mapsto |x\rangle|a \oplus f(x)\rangle|0\rangle$, build a circuit that computes $Z_f : |x\rangle|0\rangle \mapsto (-1)^{f(x)}|x\rangle|0\rangle$.

2 Simon's Problem Generalized

Consider a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there exists a vector subspace V of $\{0,1\}^n$ (seen as a vector space over $\mathbb{F}_2$) such that:

$$\forall x, y \in \{0,1\}^n,\ f(y) = f(x) \Leftrightarrow \exists v \in V, x = y + v\ .$$

1. Recall Simon's algorithm circuit and compute its final state.
2. With $V = \text{span}(b_1, \ldots, b_c)$, prove the following equality:
$$\sum_{v \in V} (-1)^{v \cdot y} = \prod_{i=1}^{c} \left(1 + (-1)^{b_i \cdot y}\right)\ .$$
3. Show that one run of Simon's algorithm outputs $x \in \{0,1\}^n$ such that x is orthogonal to V ($\forall y \in V, x \cdot y = 0 \mod 2$).
   Hint: Measure first the n first qubits: it won't change the result of the measurement on the n last qubits, but the analysis will be easier.

Remark. The usual version of Simon's Problem is when $V = \{0, a\}$ for some $a \in \{0,1\}^n$. □

3 Superdense 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. (informal) 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 $|\phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ 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 $b_1 = 1$, she applies X (bit flip) and then if $b_0 = 1$ she applies Z (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 $|\phi\rangle$.