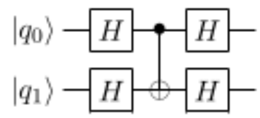
TUTORIAL 2

1 Homework 2

1. Simplify the following circuit:



2. Consider a function $f : \{0,1\}^n \to \{0,1\}$ such that either
   - f is constant.
   - f is balanced: $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$.

   Given a gate $U_f : |a \in \{0,1\}^n\rangle|b \in \{0,1\}\rangle \mapsto |a\rangle|b \oplus f(a)\rangle$, desing a quantum algorithm which output 1 is f is balanced and 0 if f is constant, using only 1 query to U_f.

   What is the classical query complexity? What if we allow some error probability?

2 Warm-up Calculations

2.1 Measurements and Probabilities

For all $|\varphi\rangle$ and $\mathcal{B}$, justify that $|\varphi\rangle$ is a state, $\mathcal{B}$ a basis, then measure $|\varphi\rangle$ in $\mathcal{B}$ and give the probability of each outcome:

1. $|\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\mathcal{B} = (|0\rangle, |1\rangle)$.
2. $|\varphi\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$, $\mathcal{B} = (|0\rangle, |1\rangle)$.
3. $|\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\mathcal{B} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
4. $|\varphi\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$, $\mathcal{B} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
5. $|\varphi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $\mathcal{B} = (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$.
6. $|\varphi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $\mathcal{B} = \left(i|00\rangle, |01\rangle, -|10\rangle, e^{i\frac{\pi}{4}}|11\rangle\right)$.
7. $|\varphi\rangle = \frac{|00\rangle+(1+i)|01\rangle+|11\rangle}{2}$, $\mathcal{B} = (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$.
8. $|\varphi\rangle = \frac{|00\rangle+(1+i)|01\rangle+|11\rangle}{2}$, $\mathcal{B} = \left(|00\rangle, |01\rangle, \frac{|10\rangle+|11\rangle}{\sqrt{2}}, \frac{|10\rangle-i|11\rangle}{\sqrt{2}}\right)$.

2.2 Partial Measurements

Let $|\varphi\rangle, |\psi\rangle$ two normalized quantum states, let $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\varphi\rangle + |1\rangle|\psi\rangle)$, suppose we apply H to the first qubit, then measure that qubit in the computational basis. Give the probability of measurement 1 as a function of $|\varphi\rangle$ and $|\psi\rangle$.

2.3 Gates

1. Construct a SWAP-gate, that is to say a quantum circuit U such that for any $a, b \in \{0, 1\}$ is such that $U \cdot |a\rangle|b\rangle \mapsto |b\rangle|a\rangle$, using CNOT gates.
   Hint: how do you swap two digits using only XOR gate in the classical case?

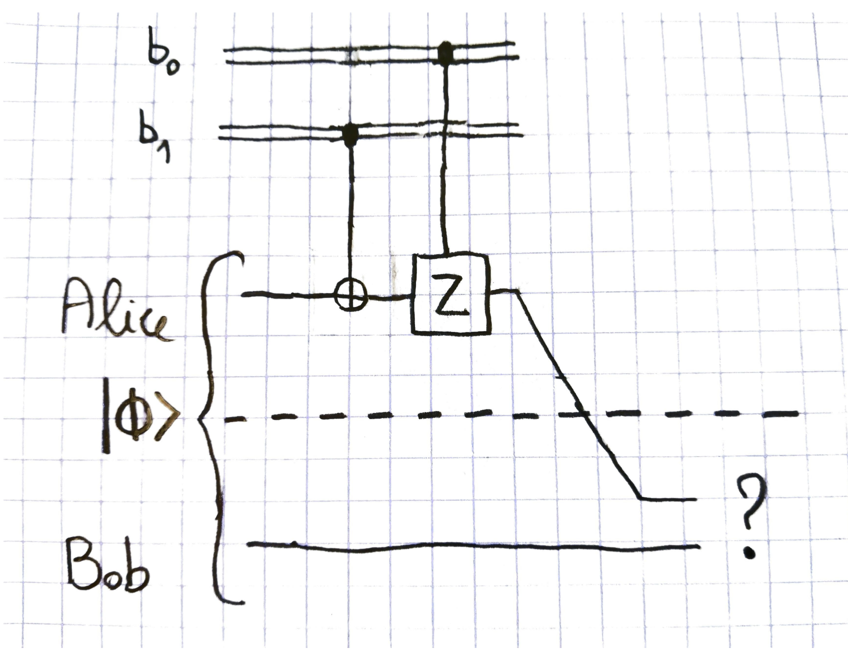
2. Suppose you are given access to a **bit-query**-oracle for a function $f : \{0, 1\}^n \to \{0, 1\}$, that is to say a gate U_f such that $\forall a \in \{0, 1\}^n, \forall b \in \{0, 1\}, U_f|a\rangle|b\rangle = |a\rangle|b \oplus f(a)\rangle$.
   Construct a circuit giving acces to a **phase-query**-oracle, that is to say construct a circuit U'_f such that for any $(a, b) \in \{0, 1\}^n \times \{0, 1\}$, $U'_f \cdot |a\rangle|b\rangle = (-1)^{b \cdot f(a)}|a\rangle|b\rangle$.

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)?

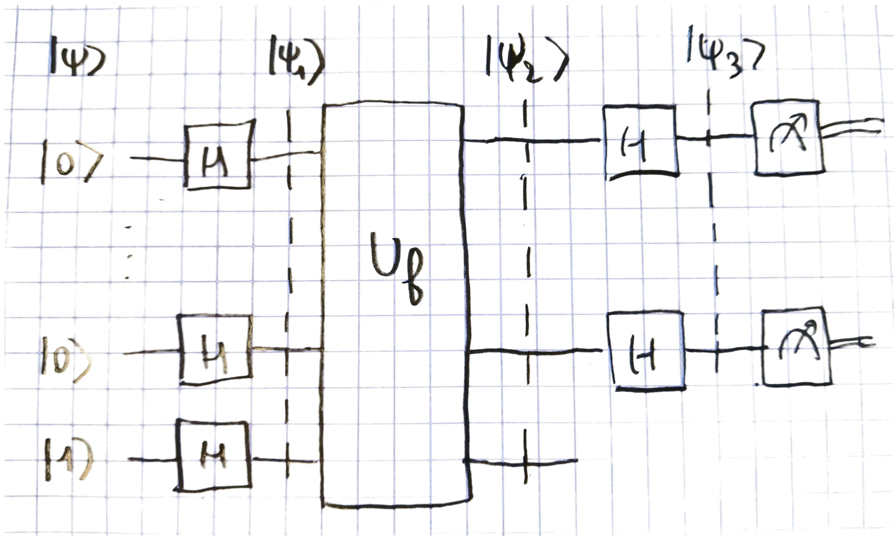
2. Now suppose that Alice and Bob share an entangled **EPR pair** (or **Bell pair**), that is to say there is a quantum state $|\phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ such that the first qubit is owned by Alice (she can only perform operations of the form $U \otimes I$ on $|\phi\rangle$) 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 $|\phi\rangle$.



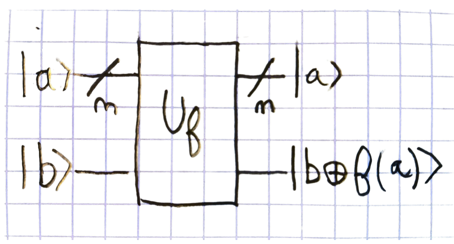
4 Bernstein-Vazirani Problem

The *Bernstein-Vazirani* problem is the following: given a function $f : \{0,1\}^n \to \{0,1\}$ which is of the form $f(x) = a \cdot x := \sum_{i=1}^{n} a_i \cdot x_i \text{ MOD } 2$ for some unknown $a \in \{0,1\}^n$, the objective is to retrieve the value of a.

Consider the following circuit:



with the gate U_f defined in the following way:



1. Compute the values of $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$ (where $|\psi_3\rangle$ is the state corresponding to the first n qubits).
2. How efficiently, in terms of quantum query complexity, can we solve the Bernstein-Vaziran problem?