# TUTORIAL 3

## 1 Homework 3

1. Let $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Given a basis $\mathcal{B} := (|b_0\rangle, |b_1\rangle)$, we measure $|\Phi\rangle$ in $\mathcal{B} \otimes \mathcal{B}$. If the outcome of the measure on the first qubit is $|b_0\rangle$, is the outcome of the measure on the second qubit always $|b_0\rangle$ (and vice-versa) ?
2. Now let $|\Phi'\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Show that if the outcome of the measure on the first qubit is $|b_0\rangle$, then the outcome of the measure on the second qubit is $|b_1\rangle$ (and vice-versa).

## 2 Some Properties of Circuits

### 2.1 Do Circuits Commute?

1. Propose two different gates $A, B$ acting on 2-qubits states such that applying $A$ then $B$ is the same as applying $B$, then $A$.
2. Propose two different gates $A, B$ acting on 2-qubits states such that applying $A$ then $B$ is **not** the same as applying $B$, then $A$.

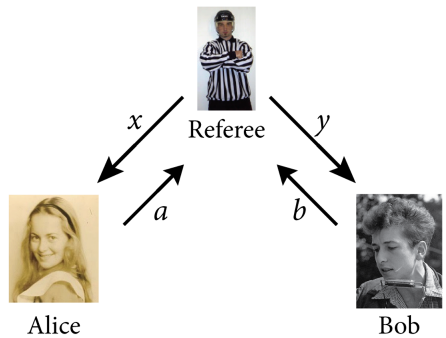
### 2.2 Are Circuits Ambiguous?

1. Let $|\phi\rangle$ be a 2-qubits state. A gate $A$ is applied to the first qubit, and then a gate $B$ is applied to the second qubit. Show that the gate $B$ could have been applied before the gate $A$.
2. Let $|\phi\rangle$ be a 2-qubits state. Check that measuring the first qubit, then the second one gives the same result as measuring the second qubit, then the first.
3. Let $|\phi\rangle$ be a $n+1$-qubits state. A gate $U$ is applied to the first $n$ qubits, and then the last qubit is measured. Show that measuring the last qubit and then applying the gate $U$ on the first $n$ qubits gives the same result.

## 3 The CHSH Game

The CHSH game (named after John Clauser, Michael Horne, Abner Shimony, and Richard Holt) was introduced to disprove local hidden-variable theories trying to explain the correlations that can result from entanglement. The goal here is to retrieve this result.

The game works in the following way: two players, Alice and Bob, receive respectively two bits $x$ and $y$ from a referee. They send him back two bits $a$ and $b$ and win the game if $a \oplus b = x \wedge y$. However Alice and Bob cannot communicate with each other during the process. They can only agree on a strategy beforehand.




$$a \oplus b \stackrel{?}{=} x \wedge y.$$

We will consider the case where the referee send uniformly $X$ and $Y$. The goal for Alice and Bob is to maximize the probability of winning, ie. $\mathbb{P}(A \oplus B = X \wedge Y)$. The value of the game is the maximum over all possible strategies of the probability of winning.

1. What is a classical deterministic strategy for Alice and Bob? Show that no classical deterministic strategy can have a probability of success greater than $\frac{3}{4}$. What is the classical value of the CHSH game?

2. Suppose now that Alice and Bob share some hidden-variable, ie. some common shared randomness. This is modelised as a random variable $K \in [n]$, and now Alice and Bob can have a common strategy depending on $K$.

   (a) Give a formula to express the value of that game, where you can also choose freely the random variable $K$ and $n$.

   (b) What is the hidden-variable value of the CHSH game?

3. Suppose now that Alice and Bob share some EPR pair $|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Alice (resp. Bob) can make local measurements depending on $x$ (resp. $y$) on the first qubit (resp. second qubit). Find the best quantum strategy possible. Conclude.
   *Hint: If Alice measures her qubit in the real basis* $(|a_0\rangle, |a_1\rangle)$, *what is the remaining state of Bob? Then plot Bob's qubit in order to find the best strategy.*

## 4 Quantum 1-Machine

You have a device that outputs only $|0\rangle$. You can use this device several times, and measure in any basis. How many calls to the device do you need to get a $|1\rangle$?

## 5 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:

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

Show that one run of Simon's algorithm output $x \in \{0,1\}^n$ such that $x$ is orthogonal to $V$ ($\forall y \in V, x \cdot y = 0 \text{ MOD } 2$).

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