1 Partial Measurements

1. For all $|\varphi\rangle$ and $B$, measure $|\varphi\rangle$ in $B$ and determine the post-measurement states and their respective probabilities.

   (a) $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and $B = \{I \otimes |+\rangle\langle+|, I \otimes |-\rangle\langle-|\}$.

   (b) $|\varphi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$, and $B = \{I \otimes |+\rangle\langle+|, I \otimes |-\rangle\langle-|\}$.

   (c) $|\varphi\rangle = 2^{-n/2} \sum_{a \in \{0,1\}^n} |a\rangle |a \text{ MOD } 2\rangle$, and $B = $ measure the second register in the computational basis.

   (d) $|\varphi\rangle = 2^{-n/2} \sum_{a \in \{0,1\}^n} |a\rangle |a \text{ MOD } 4\rangle$, and $B = $ measure the second register in the computational basis.

2. 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 Bernstein-Vazirani Problem

The Bernstein-Vazirani problem is the following: given a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ 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:

![Circuit Diagram]

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?

3 **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 3.1 (QRAC).** A quantum random access code (QRAC) with success probability $p$ is an encoding $f : \{0, 1\}^2 \rightarrow \mathbb{C}^2$ (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 $x_1, x_2$:

$$
\Pr(\text{Measure output } = x_1 | U_1 \text{ was applied}) = |\langle x_1 | U_1 | f(x_1, x_2) \rangle|^2 \geq p
$$

$$
\Pr(\text{Measure output } = x_2 | U_2 \text{ was applied}) = |\langle x_2 | U_2 | f(x_1, x_2) \rangle|^2 \geq p
$$

1. A classical random access code depicts the situation where you restrict yourself to encodings $f : \{0, 1\}^2 \rightarrow \{0, 1\}$, i.e. 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 apart, in such a way that two distinct unitaries can distinguish them efficiently