Exercise 1. ***Unambiguous state discrimination.***

If we have a set of n orthogonal states $\{|\psi_i\rangle\}_{i=1,\ldots,n}$, we can always define a set of projective measurement operators that distinguishes them perfectly: Define measurement operators

$$M_i = |\psi_i\rangle\langle\psi_i| \tag{1}$$

for each state in the set and add one operator

$$M_0 = \mathbb{I} - \sum_{i=1}^{n} M_i. \tag{2}$$

to ensure that the operators sum up to the identity.

(a) Show that the probability of getting outcome i when measuring the state $|\psi_i\rangle$ is 1.

Can we still perfectly distinguish the states if they are not orthogonal? Consider the set of two non-orthogonal states $\{|0\rangle, |+\rangle\}$. Suppose someone randomly selects one of the two states (with equal probability) and hands it to us. To determine which of the two states was given to us, we perform a projective measurement and use the outcome to guess whether the state was $|0\rangle$ or $|+\rangle$. We can try to minimise the probability of misidentifying $|0\rangle$ as $|+\rangle$, or vice versa.

(b) First, let us measure in the computational basis $\{|0\rangle, |1\rangle\}$. We identify the state as $|0\rangle$ if the outcome is 0, and as $|+\rangle$ if the outcome is 1. What are p, the probability of incorrectly identifying $|0\rangle$ (i.e., saying the state is $|0\rangle$ when actually $|+\rangle$ was given to us), and q, the probability of incorrectly identifying $|+\rangle$?

We now allow a general measurement, a POVM, instead of a projective measurement. Consider the POVM given by the following three elements:

$$M_0 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \tag{3}$$

$$M_1 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{4}$$

$$M_2 = \mathbb{I} - M_0 - M_1. \tag{5}$$

(c) Show that the set $\{M_0, M_1, M_2\}$ forms a valid POVM.

(d) The three possible outcomes of this measurement are 0, 1, and 2. What is the best strategy for assigning them to the states we want to distinguish? What does the third outcome correspond to? What are now the probabilities p and q of misidentifying $|0\rangle$ and $|+\rangle$, respectively?

(e) Using this measurement, what is the probability of guessing correctly which state is given to you?

Exercise 2. ***Secret sharing with entanglement.***

In this exercise, we will learn a scheme that allows three parties, Alice, Bob, and Charlie, to share a classical secret using entangled quantum states. Suppose the three parties share a state of the form

$$|\psi_b\rangle_{ABC} = \frac{1}{\sqrt{2}} \Big(|000\rangle + (-1)^b |111\rangle \Big) \tag{6}$$

with $b \in \{0, 1\}$ being the secret bit they want to share.

(a) Alice would like to find the secret b by performing a local measurement on her qubit. Calculate her reduced density matrix from (6). Explain why this implies that she cannot find the secret on her own.

(b) Since Alice cannot find the secret on her own, she teams up with Bob. They would like to find b without Charlie being involved. Show that the reduced state of Alice and Bob is independent of b.

(c) Show that the same holds for the two-party combinations Alice-Charlie and Bob-Charlie and that therefore no two parties are able to find the secret without the third one being involved.

(d) Now imagine that for some reason (for example, a terrible snowstorm) Alice, Bob, and Charlie cannot leave their respective houses. However, the radio is still working, so they can use it to communicate classical information. Also, each of them has their respective qubit at home and can apply operations to it and perform measurements. They would like to find out the secret bit b. However, they want to do it in a way that guarantees that they succeed. Can you design a protocol (i.e., a series of operations, measurements, and classical communication for the three parties) that outputs the bit b with probability 1?

Hint. What happens if all three parties measure in the Hadamard basis?