Homework # 2. Physics 265, Spring 2024

Topic: *On Measurements, Projections, Entanglement and Multiple Qubits*

Due date: Thursday Feb 15, 2024. This problem set may be long. If so choose a subset of problems of about 7 to work on. You can also create and share your own problems or do problems from the previous problem set.

1. **On changing basis for a 2 qubit system**

   We defined

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

   Show how the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

   can be written in the basis $\{|{+}{+}\rangle, |{+}{-}\rangle\, |{-}{+}\rangle, |{-}{-}\rangle\}$.

2. **On partial measurement in a three-qubit system**

   A three qubit system is in the state

$$|\psi\rangle = \frac{1}{\sqrt{3}}\left(|000\rangle + i\,|010\rangle - |111\rangle\right)$$

   The first qubit is measured in the $\{|0\rangle, |1\rangle\}$ basis (for example using the Pauli Z gate).

   a) When measured, what is the probability that the first qubit is in the $|0\rangle$ state?

   b) If the first qubit is measured to be in the $|0\rangle$ state, what is the resulting quantum state vector afterward?

   c) Suppose one qubit is measured and then immediately afterwards another qubit is measured, with both measurements using a single qubit Z gate. The final state depends upon the values found in each measurement. Does the final state depend upon which order the two measurements were done?

3. **Mostly relevant for POVM measurements**

   $\mathbf{A}, \mathbf{B}, \mathbf{M}$ are operators in a Hilbert space.

   a) Show that $(\mathbf{AB})^\dagger = \mathbf{B}^\dagger\mathbf{A}^\dagger$

   b) Show that $\mathbf{MM}^\dagger$ is Hermitian.

   c) If $\mathbf{H}$ is Hermitian and $\mathbf{U}$ is unitary, show that $\mathbf{UHU}^\dagger$ is Hermitian.

   d) If $\mathbf{H}$ is Hermitian show that $\mathbf{U} = e^{i\mathbf{H}}$ is unitary.

   e) If $\mathbf{U}$ is unitary, show that it is possible to find a Hermitian operator $\mathbf{H}$ such that $\mathbf{U} = e^{i\mathbf{H}}$.

   Hints: Unitary and Hermitian matrices can be diagonalized.

4. **A Hadamard transformation on a Bell pair state**

   Starting with a Bell pair,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   perform a Hadamard on one of the qubits and then measure one of the qubits.

   Show that the probability of measuring a 0 or 1 during the measurement does not depend on which bit is measured or on which bit you operated on with the Hadamard operation.

5. **The Bell basis**

   The Bell basis is a set of 4 entangled states

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

   Write the following state in the Bell basis

$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$$

   Your answer should look like this:

$$a\left|\Phi^+\right\rangle + b\left|\Phi^-\right\rangle + c\left|\Psi^+\right\rangle + d\left|\Psi^-\right\rangle$$

   You need to find the complex numbers a, b, c, d.

6. **On entanglement**

   Give an example of a two-qubit state that is a superposition with respect to the standard basis but that is not entangled.

   The standard basis is $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. A superposition is a state vector $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ where at least 2 of the complex numbers a, b, c, d are not zero.

   A state that is **not** entangled can be written as a tensor product. In other words it can be written as $|\psi\rangle = |v\rangle \otimes |w\rangle$ where $|\psi\rangle$ is the 2 qubit state and $|v\rangle, |w\rangle$ are single qubit states.

7. **Subspace decomposition and designing measurements**

   Design a measurement on a three-qubit system that distinguishes between states in which the number of 1 bits is even, and those in which the number of 1 bits is odd, and gives no other information. Write your solution in bra/ket notation.

   You need to find a Hermitian operator for the measurement $\mathbf{M}$. Find a set of complete and orthogonal and Hermitian projection operators $\mathbf{P}_i$ such that $\mathbf{M} = \sum_\mathbf{i} \mathbf{m_i}\mathbf{P_i}$, where m_i are the possible measurement values.

   This is problem 4.10 from Rieffel & Polak.

8. **On entanglement and measurement**

   a) Show that if a measurement is performed on one of the bits of an unentangled state $|\psi\rangle$, the resulting 2 qubit state is unentangled.

   b) Can a measurement on an unentangled state $|\psi\rangle$ produce an entangled state? If so, give an example.

   Hint: make use of the Bell states and construct projection operators.

   c) Can an unentangled state be obtained by measuring a single qubit of an entangled state $|\phi\rangle$? If so, give an example.

   Based on Problem 4.17 of Rieffel & Polak.

9. **Interpretations of Quantum Mechanics**

   Which of the possible interpretations of quantum mechanics most appeal to you and why?

   Here are some possible topics for discussion: Discuss the advantages and disadvantages of one of the interpretations. Should there be a consensus in our community? Do the interpretations motivate new experiments or ways to resolve inconsistencies between theories in physics?

10. **On single qubit rotations**

a) Show that

$$(\hat{\mathbf{n}} \cdot \boldsymbol{\sigma})^2 = \mathbf{I}$$

where $\boldsymbol{\sigma} = (\boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y, \boldsymbol{\sigma}_z)$ and $\hat{\mathbf{n}} = (n_x, n_y, n_z)$ is a unit vector.

b) If an operator $\mathbf{A}$ satisfies $\mathbf{A}^2 = \mathbf{I}$ show that

$$e^{i\alpha \mathbf{A}} = \cos\alpha\ \mathbf{I} + i \sin\alpha\ \mathbf{A}$$

c) Show that any unitary transformation on a single qubit can be written as

$$S_{\hat{\mathbf{n}}}(\alpha) = e^{i\alpha \hat{\mathbf{n}}\cdot\boldsymbol{\sigma}}$$

where $\hat{\mathbf{n}}$ is a unit vector and α is an angle.

This gives a rotation on the Bloch sphere by angle α about axis $\hat{\mathbf{n}}$.

$$R_{\hat{\mathbf{n}}}(\alpha) = e^{-i\frac{\alpha}{2}\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}}$$

Any transformation can be written as

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}.$$

For U unitary we require $UU^\dagger = I$ which gives these conditions on the components of U

$$\begin{aligned} u_{00}u_{00}^* + u_{01}u_{01}^* &= 1 \\ u_{00}u_{10}^* + u_{01}u_{11}^* &= 0 \\ u_{10}u_{10}^* + u_{11}u_{11}^* &= 1. \end{aligned}$$

11. **On irrational rotations**

Consider the unitary transformation

$$\mathbf{U}(\beta) = \begin{pmatrix} e^{i\pi\beta} & 0 \\ 0 & e^{-i\pi\beta} \end{pmatrix}$$

with β a real number. This operation is a rotation about the z axis on the Bloch sphere.

We consider n consecutive iterations of operations of $\mathbf{U}$ on initial state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

I am choosing this initial state as it lies on the x axis on the Bloch sphere.

a) Show that

$$\langle\psi|\,\mathbf{U}^{\mathbf{n}}(\beta)\,|\psi\rangle = \cos(\pi\mathbf{n}\beta)$$

b) Show that for $n > 0$ and β irrational

$$|\,\langle\psi|\,\mathbf{U}^{\mathbf{n}}(\beta)\,|\psi\rangle\,|$$

cannot be zero or 1.

This implies that each iteration gives a new state.

We consider the set of iterations $\{\mathbf{U}^j(\beta)\,|\psi\rangle\}$ for $j \in \{1, 2, ..., n\}$.

c) With β irrational, how many iterations n does it take before one of the iterations $\mathbf{U}^j(\beta)\,|\psi\rangle$ is very close to the original state $|\psi\rangle$?

If $|\psi\rangle$ is close to $\mathbf{U}^j(\beta)\,|\psi\rangle$ then $\langle\psi|\,\mathbf{U}^{\mathbf{j}}(\beta)\,|\psi\rangle \sim \mathbf{1}$.

Given ϵ, a small positive number, we would like to find n large such that there is a positive integer $j \le n$ for which

$$1 - |\,\langle\psi|\,\mathbf{U}^{\mathbf{j}}(\beta)\,|\psi\rangle\,|^{\mathbf{2}} < \epsilon. \tag{1}$$

How large does n have to be satisfy to ensure that one of the iterations satisfies this inequality?

This is like a *recurrence time* for a dynamical system.

Hint: Use *Dirichlet's theorem on Diophantine approximation.* The theorem: For any real numbers α, N with $N \ge 1$, there exists integers p, q such that $1 \le q \le N$ and

$$|q\alpha - p| < \frac{1}{N} \tag{2}$$

You need to choose $\frac{1}{N}$ from ϵ and set α based on β (possibly by multiplying by 2π). The resulting limit on q gives you n.

I find that it is much hard to estimate the number of iterations it takes to approach a particular state, rather than to return to near the original one. This exercise is related to the idea that a few single qubit gates that include an irrational rotation, can be used to construct any unitary transformation of a qubit. Remarkably the number of gates required for the Solovay Kitaev theorem is logarithmic in $1/\epsilon$ whereas here with a single gate, I find a power law dependence of the recurrence time on $1/\epsilon$.

12. **More on the Bell basis**

Consider a two-qubit system. The Bell basis is comprised of

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

For any Bell basis state

$$|\Phi\rangle \in \{\left|\Phi^+\right\rangle, \left|\Phi^-\right\rangle, \left|\Psi^+\right\rangle, \left|\Psi^-\right\rangle\},$$

and any $\mathbf{V}$ a Pauli matrix

$$\mathbf{V} \in \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$$

the following is true:

$$\mathbf{V}_1 |\Phi\rangle = \pm \mathbf{V}_2 |\Phi\rangle .$$

Here the index of $\mathbf{V}$ denotes which qubit the Pauli matrix operates on. This relation is helpful for understanding quantum teleportation protocols.

If two states $|a\rangle, |b\rangle$ are equivalent up to a global phase then $\langle a|b\rangle = e^{i\delta}$ for some angle δ.

Find a unitary operation $\mathbf{U}$ on a single qubit and a Bell basis vector $|\Phi\rangle$ such that $\mathbf{U}_1 |\Phi\rangle$ cannot be written as a global phase times $\mathbf{U}_2 |\Phi\rangle$.

13. **On consecutive measurements**

Consider a single qubit system is in state $|\psi\rangle = a|0\rangle + b|1\rangle$.

The Pauli matrices we refer to as X, Y, Z gates. Note that $ZX = -iY$.

Suppose a Pauli Z gate is used to make a measurement and then a Pauli X gate is used to make a measurement.

a) What are the possible final states and what is the probability for each of them?

b) What are the possible different sets of measured values and what is the probability of set of measurements?

c) What if instead you measure with X first and then Z. What are the possible different sets of measured values and their probabilities?

d) What if instead of doing 2 measurements, you only measure with Y. What are the possible final states and what are their probabilities?

14. **On Quantum Teleportation**

A procedure for quantum teleportation of a qubit in state $|\psi\rangle$ from Alice to Bob when Alice and Bob share a Bell pair state is shown in Figure 1.

Instead of sharing the initial state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the second and third qubits, Alice and Bob share the state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Alice and Bob can still teleport the first qubit. Alice opts to keep her procedures the same.

How should Bob vary what he does in response to Alice's measurements to ensure that the first qubit is teleported intact into Bob's (the third one)?

Draw a quantum circuit to illustrate your modified teleportation protocol.

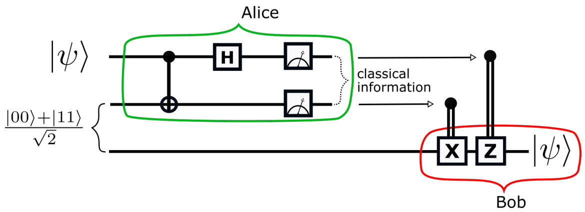

Figure 1: A recipe for teleporting a qubit $|\psi\rangle$ using two additional entangled qubits, a CNOT, a Hadamard operation and two measurements. Alice and Bob share an entangled state. The transmitter (Alice) applies the CNOT and the Hadamard and makes the two measurements. The transmitter then tells the receiver the results of the two measurements. The receiver (Bob) applies a transformation on the third qubit that is based on the measurements of the first two qubits. The receiver then holds the third qubit which has become identical to $|\psi\rangle$, the original state of the first qubit.

15. Problem 3.15 by Rieffel and Polak This problem analyzes the effectiveness of some simple attacks an eavesdropper Eve could make on Ekert's entangled state based quantum key distribution protocol. This is in the book *Quantum Computing, A gentle Introduction*. You could also choose to work on other problems from this book!

16. **The Chau02 Quantum Key Distribution Protocol**

    The Chau02 Quantum Key Distribution protocol is a variant of the BB84 protocol.

    Alice randomly chooses 0 or 1. Then she randomly choose a basis from one of the following bases $\{|0\rangle, |1\rangle\}$, or $\{|+\rangle, |-\rangle\}$ or $\{|i\rangle, |-i\rangle\}$. If Alice chose a 0 she sends to Bob $|0\rangle$ or $|+\rangle$ or $|i\rangle$, depending upon her chosen basis.

    Otherwise she sends to Bob $|1\rangle$ or $|-\rangle$ or $|-i\rangle$, depending upon her chosen basis.

    Bob randomly chooses one of these bases for measurement.

    Afterwards Alice and Bob share which bases they used and discard all bits in which their bits were not the same. The remaining bits are their shared key.

    a) What fraction of Bob's measurements are eventually discarded?

    Suppose Eve intercepts Alice's sent qubit, makes a measurement in one of the three bases and then sends the result to Bob.

    b) What fraction of Alice and Bob's generated key would be incorrect due to Eve's interference?

17. **A mutually unbiased basis via the discrete Fourier transform**

    Let $\mathcal{H}$ is a finite complex vector space of dimension N. We define a basis for $\mathcal{H}$ with $|j\rangle$ and $j \in [0, 1....., N-1]$. We can define a Fourier basis with

$$\left|\tilde{k}\right\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} |j\rangle \tag{3}$$

    with $\omega = e^{2\pi i/N}$ and $k \in [0, 1....., N-1]$.

    Show that the two bases $\{|j\rangle\}$ and $\{\left|\tilde{k}\right\rangle\}$ are mutually unbiased.

    In other words show that measurement in the $\{|j\rangle\}$ basis of a basis state $\left|\tilde{k}\right\rangle$ in the other basis gives no information about which basis state is measured.

18. **A new or different problem**

    Propose and solve a different problem!