Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2019	MATH3391-WE01

Title:

Quantum Information III

Time Allowed:	3 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	No	Models Permitted: Use of electronic calculators is forbidden.
Visiting Students may use dictionaries: No		

Instructions to Candidates:	Credit will be given for: the best **FOUR** answers from Section A and the best **THREE** answers from Section B. Questions in Section B carry **TWICE** as many marks as those in Section A.

Revision:	

ED01/2019

SECTION A

1. The density matrix ρ for a single qubit can be described in terms of the Bloch sphere as

$$\rho = \frac{1}{2}\left(I + \mathbf{r}\cdot\boldsymbol{\sigma}\right)$$

where the Bloch vector $\mathbf{r}$ is a position vector in three dimensions, I is the 2×2 identity matrix and

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\ ,\ \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\ ,\ \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(a) For a constant $\lambda \in \mathbb{C}$ we define $U \equiv \exp(i\lambda\sigma_3)$. Show that

$$U = I\cos\lambda + i\sigma_3\sin\lambda$$

and find the necessary condition on λ so that U is a unitary matrix.

(b) Under a time evolution $\rho \to \tilde{\rho} = U\rho U^\dagger$ where U is the unitary matrix from part (a). Calculate the Bloch vector $\tilde{\mathbf{r}}$ of $\tilde{\rho}$ in terms of the initial Bloch vector $\mathbf{r}$ and explain the geometric interpretation (in the Bloch sphere picture) of this time-evolution, stating explicitly the dependence on λ.

2. (a) Find a unitary operator $\hat{U}$ which acts as

$$\hat{U}\left(|n\rangle \otimes |0\rangle\right) = |n\rangle \otimes |n\rangle\ \ ,\ n \in \{0,1\}$$

on the standard orthonormal basis states of a 2-qubit system.

You can write the operator in Dirac notation or using standard matrix notation.

(b) State the no-cloning theorem and explain clearly why, although the operator $\hat{U}$ in part (a) clones the states $|n\rangle$, this does not contradict the no-cloning theorem.

(c) Give an example of a pure state which $\hat{U}$ does not clone, and show explicitly that it does not clone that state.

3. In this question orthonormal basis states $|0\rangle$ and $|1\rangle$ of a single qubit Hilbert space are represented by column vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ respectively. Also, we interchangeably use notation $|x\rangle \otimes |y\rangle = |xy\rangle$ etc.

   Consider a system of 3 qubits. The first is held by Alice in the state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

   for some $a, b \in \mathbb{C}$. Alice also holds the second qubit which is entangled with the third qubit which Bob holds. The second and third qubits are in the state

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\,|00\rangle - \frac{1}{\sqrt{2}}\,|11\rangle \ .$$

   Any tensor products of two or all of the qubits are written in the order 1st, 2nd, 3rd left to right.

   (a) Show that if Alice acts on her qubits with the (unitary) operator

$$|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

   the state of the system becomes

$$\frac{a}{\sqrt{2}}\,|000\rangle + \frac{c}{\sqrt{2}}\,|011\rangle + \frac{d}{\sqrt{2}}\,|110\rangle - \frac{b}{\sqrt{2}}\,|101\rangle$$

   giving the explicit expressions for c and d in terms of a and b.

   (b) Alice then acts on the first qubit with the (unitary) operator/matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

   before measuring each of her qubits using the observable

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

   What is the state of the qubit held by Bob if the results of Alice's measurements were $(1, -1)$, i.e. 1 for the first qubit and -1 for the second?

   (c) Alice can tell Bob the result of her two measurements using classical communication. Once Bob knows that Alice's measurement results were $(1, -1)$, which unitary operator can Bob use to transform his state to the state $|\psi\rangle$ even though neither Alice nor Bob know the values of a and b?

4. Give a universal gate set for reversible classical computation. Using this gate set, draw circuit diagrams corresponding to

    (a) A function of two bits such that $f(01) = 1$ and $f(x) = 0$ otherwise.

    (b) A function of three bits such that $f(011) = 1$ and $f(x) = 0$ otherwise.

5. Consider the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle - |x_0 \oplus a\rangle)$ in an n-qubit system, where $\oplus$ denotes bitwise addition.

    (a) Calculate $H^{\otimes n}|\psi\rangle$, where H is the Hadamard operator.

    (b) Suppose we would like to learn the value a, and x_0 is a random value of no interest to us. Explain what information a measurement in the computational basis on the state $H^{\otimes n}|\psi\rangle$ gives us about a. How many such measurements are typically required to determine a?

6. Given a unitary operator U_f representing a function $f(x)$ with $f(a) = 1$ and $f(x) = 0$ for $x \neq a$, construct an operation which will reflect a state $|\psi\rangle$ in the plane orthogonal to $|a\rangle$ (that is, which keeps the component of $|\psi\rangle$ orthogonal to $|a\rangle$ unchanged, and reverses the sign of the component along $|a\rangle$).

    Explain how this operation is used in Grover's algorithm to find the value of a.

SECTION B

7. The four Bell states are

$$\beta_{xy} = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |y\rangle + (-1)^x |1\rangle \otimes |\overline{y}\rangle \right)$$

where $x, y \in \{0, 1\}$, $\overline{0} \equiv 1$ and $\overline{1} \equiv 0$. In this question you may assume without proof that the four Bell states are orthonormal and that any two Bell states are related by a unitary transformation of the form $\hat{U} \otimes \hat{I}$.

In this question Alice wants to send a message with absolute security to Bob. They can communicate classically but suspect that Eve can listen in on such communications.

(a) Alice and Bob each have one qubit of a known Bell state. Explain in detail how Alice can send a single message "yes" or "no" to Bob using LOCC only, in such a way that Eve cannot learn which message is sent.

(b) Again Alice and Bob each have one qubit of a known Bell state. If Alice is allowed to send one qubit to Bob, explain how she can transmit two bits of information to Bob without using any classical communication.

(c) If Eve is able to intercept any qubits sent to Bob, explain why she cannot learn anything about Alice's message in part (b).

(d) Eve decides to simply block any qubits sent to Bob. Alice and Bob can communicate but assume Eve can listen in on their communications so cannot risk sending any sensitive information via classical communication. Unfortunately Alice still needs to send two bits of information to Bob but they no longer share any entangled states. Fortunately they both share some Bell states with Charlie whom they trust (so they don't mind if Charlie discovers the message). Using the above results, describe how Charlie can help Alice transmit her two bits of information to Bob using the least number of Bell pairs, without Charlie sending any qubits to Alice.

8. (a) Consider a bipartite system with an orthonormal basis $\{|\alpha_n\rangle\}$ for $\mathcal{H}_A$, the Hilbert space of system A, and similarly $\{|\beta_i\rangle\}$ for $\mathcal{H}_B$. Here $n \in \{1, 2, \ldots, \dim \mathcal{H}_A\}$ and $i \in \{1, 2, \ldots, \dim \mathcal{H}_B\}$.

Give an orthonormal basis for $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, give an expression for a general pure state $|\Psi\rangle \in \mathcal{H}$ and show that $|\Psi\rangle$ can always be written in the form

$$|\Psi\rangle = \sum_n |\alpha_n\rangle \otimes |\phi_n\rangle \ .$$

(b) Let $\hat{M}$ be an observable in system A with eigenstates $|\alpha_n\rangle$ and a non-degenerate spectrum. Measuring M in system A can also be viewed as a measurement in the full bipartite system. State what observable (operator) this corresponds to in the bipartite system. Show that after such a measurement the state of the full system will be separable, no matter what the initial pure state $|\Psi\rangle$ is.

(c) Now consider the case where $\dim \mathcal{H}_A = 3$ but the spectrum of $\hat{M}$ has degeneracy. Specifically $|\alpha_1\rangle$ and $|\alpha_3\rangle$ have eigenvalue λ_1 while $|\alpha_2\rangle$ has eigenvalue $\lambda_2 \neq \lambda_1$.

Suppose also that

$$|\phi_1\rangle = \frac{1}{2}|1\rangle \ , \ |\phi_2\rangle = \frac{\sqrt{3}}{4}(|1\rangle + |2\rangle) \ , \ |\phi_3\rangle = \frac{\sqrt{3}}{4}(|1\rangle - |3\rangle)$$

where the three states $|n\rangle$ are orthonormal.

i. What are the possible outcomes and final states in the full system if M is measured in system A?

ii. Calculate $\mathrm{Tr}(\hat{\rho}_A^2)$ (for each possible outcome) after the measurement of M, where $\hat{\rho}_A$ is the reduced density operator in system A.

iii. Without explicit calculation, what can you say about the value of $\mathrm{Tr}(\hat{\rho}_A^2)$ before the measurement in comparison to the value of this quantity after the measurement?

9. Consider

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

   (a) Write this as the product of unitaries U_i which each act non-trivially on a two-dimensional subspace of the Hilbert space.

   (b) Write the operators U_i which do not act on a subspace corresponding to a single qubit as products of ones that do.

   (c) Draw a quantum circuit corresponding to U, using only NOT, H, Z and CNOT, controlled-H and controlled-Z.

   (d) For an n-qubit system, how many operators U_i which each act non-trivially on a two-dimensional subspace are required to realise a general unitary U? What does this tell us about the complexity of a general unitary U?

10. We want to construct a 5 qubit code allowing for recovery from arbitrary single qubit errors.

   (a) Consider the operators in a 5 qubit Hilbert space

$$M_0 = Z_1 X_2 X_3 Z_4, \quad M_1 = Z_2 X_3 X_4 Z_0, \quad M_2 = Z_3 X_4 X_0 Z_1,$$

$$M_3 = Z_4 X_0 X_1 Z_2, \quad M_4 = Z_0 X_1 X_2 Z_3.$$

   Show that

$$|\bar{0}\rangle = \frac{1}{4}(I + M_0)(I + M_1)(I + M_2)(I + M_3)|00000\rangle,$$

$$|\bar{1}\rangle = \frac{1}{4}(I + M_0)(I + M_1)(I + M_2)(I + M_3)|11111\rangle$$

   are eigenstates of all the M_i for $i = 0, \ldots, 3$ with eigenvalue $+1$.

   (b) Find the eigenvalues for the subspaces obtained after the single qubit errors X_0, Y_0 or Z_0.

   (c) Show that $|\bar{0}\rangle$, $|\bar{1}\rangle$ form a code subspace for arbitrary single qubit errors, and that M_i $i = 0, \ldots 3$ are suitable error syndromes.

   (d) Define a fault tolerant operation on the logical qubit. Show that $\bar{X} = X_0 X_1 X_2 X_3 X_4$ realizes Pauli X on the logical qubit. Is it fault tolerant?