A14687W1

SECOND PUBLIC EXAMINATION

Honour School of Mathematics Part C: Paper C7.4
Honour School of Mathematics and Computer Science Part C: Paper C7.4
Honour School of Mathematical and Theoretical Physics Part C: Paper C7.4
Master of Science in Mathematical Sciences: Paper C7.4
Master of Science in Mathematical and Theoretical Physics: Paper C7.4

Introduction to Quantum Information

TRINITY TERM 2022

Monday 06 June, 14:30pm to 16:15pm

You may submit answers to as many questions as you wish but only the best two will count for the total mark. All questions are worth 25 marks.
Candidates may bring a summary sheet into this exam consisting of (both sides of) one sheet of A4 paper containing material prepared in accordance with the guidance given by the Mathematical Institute.

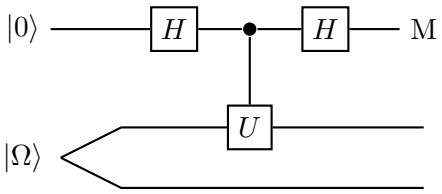
You should ensure that you observe the following points:

- start a new answer booklet for each question which you attempt.
- indicate on the front page of the answer booklet which question you have attempted in that booklet.
- cross out all rough working and any working you do not want to be marked. If you have used separate answer booklets for rough work please cross through the front of each such booklet and attach these answer booklets at the back of your work.
- hand in your answers in numerical order.

If you do not attempt any questions, you should still hand in an answer booklet with the front sheet completed.

Do not turn this page until you are told that you may do so.

1. Consider the following quantum circuit composed of two Hadamard gates, one controlled-U operation, and the measurement M in the standard basis.



The top horizontal line represents a qubit, initially in state $|0\rangle$, and the two bottom lines represent two qubits prepared in the Bell state

$$|\Omega\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle \right).$$

(a) [6 marks] Step through the execution of this circuit, writing down the quantum states of the three qubits after each computational step. Show that the final state $|\Psi\rangle$ at the output can be written as

$$|\Psi\rangle = |0\rangle\,\frac{1}{2}\Big(|\Omega\rangle + (U \otimes \mathbb{1})\,|\Omega\rangle \Big) + |1\rangle\,\frac{1}{2}\Big(|\Omega\rangle - (U \otimes \mathbb{1})\,|\Omega\rangle \Big).$$

(b) [7 marks] Show that the probability of obtaining outcome 0 in the M measurement is

$$\Pr(0) = \frac{1}{2}\left[1 + \frac{1}{2}\,\mathrm{Re}\,(\mathrm{tr}\,U) \right].$$

(c) [6 marks] You are promised that U is chosen uniformly at random to be either the Hadamard or the identity gate. Your task is to determine which gate was chosen.

(i) Suppose you run the circuit once and you register outcome 0. Is this outcome conclusive? If your answer is "yes", explain why. If your answer is "no", is U more likely to be the Hadamard or the identity gate?

(ii) Instead, suppose you registered the outcome 1. What can you say in this case?

(d) [6 marks] Suppose U is an unknown unitary in $SU(2)$, and that you can run the circuit as many times as you wish. How would you estimate the eigenvalues of U?

[*Recall that* $SU(2)$ *consists of the* (2×2) *unitary matrices with determinant equal to* 1.]

2. The norm of an operator $A \in \mathcal{B}(\mathcal{H})$, denoted by $\|A\|$, is the maximum length of the vector $A|v\rangle$ over all choices of normalised $|v\rangle \in \mathcal{H}$. This norm is *unitarily invariant* (i.e. $\|UAV\| = \|A\|$ for any unitaries U and V) and *submultiplicative* (i.e. $\|AB\| \leqslant \|A\|\|B\|$).

   Throughout this question, you may use, without proof, the following fact: If A is normal (i.e. if $A^\dagger A = AA^\dagger$), then $\|A\|$ is equal to the largest absolute value of the eigenvalues of A.

   (a) [3 marks] Justify briefly the following statements (exact derivations are not required):
   (i) $\|A^\dagger\| = \|A\|$ for any normal A.
   (ii) $\|U\| = 1$ if U is unitary.
   (iii) $\|\Pi\| = 1$ if $\Pi \neq 0$ is an orthogonal projector.

   (b) [3 marks] Show that, for any operators A and B,

$$|\langle\psi| A^\dagger B |\psi\rangle| \leqslant \|A\|\|B\|.$$

[*You may use, without proof, the Cauchy-Schwarz inequality:* $|\langle a|b\rangle|^2 \leqslant \langle a|a\rangle \langle b|b\rangle$.]

Let U and V be unitary operators acting on the same Hilbert space. Think of U as the target unitary operator that we wish to implement, and V as the unitary operator that we can actually implement in practice. We say that V *approximates* U *with precision* ϵ if

$$\|U - V\| \leqslant \epsilon.$$

   (c) [5 marks] Suppose that a quantum system initially in the state $|\Psi\rangle$ evolves according to U (respectively V). Let Π be a projector associated with a specific outcome of some measurement that can be performed on the system after the evolution, and let P_U (respectively P_V) be the probability of obtaining the corresponding measurement outcome if the operation U (respectively V) was performed. Show that

$$|P_U - P_V| = |\langle\Psi| U^\dagger \Pi U |\Psi\rangle - \langle\Psi| V^\dagger \Pi V |\Psi\rangle| \leqslant 2\|U - V\|.$$

   [*Hint: Notice that*

$$|\langle\Psi| U^\dagger \Pi U |\Psi\rangle - \langle\Psi| V^\dagger \Pi V |\Psi\rangle| = |\langle\Psi| U^\dagger \Pi (U - V) |\Psi\rangle + \langle\Psi| (U^\dagger - V^\dagger) \Pi V |\Psi\rangle|.\ ]$$

   (d) [6 marks] For unitary gates U_1, V_1, U_2, V_2 show that, if $\|U_1 - V_1\| \leqslant \epsilon_1$ and $\|U_2 - V_2\| \leqslant \epsilon_2$, then

$$\|U_2 U_1 - V_2 V_1\| \leqslant \epsilon_1 + \epsilon_2.$$

   (e) [4 marks] Deduce that, if $\|U_i - V_i\| \leqslant \epsilon$ for $i = 1, \ldots, n$, then

$$\|U_n \ldots U_1 - V_n \ldots V_1\| \leqslant n\epsilon.$$

   (f) [4 marks] Suppose we wish to implement a quantum circuit containing d gates, U_1 through U_d, but we are only able to approximate each U_i by some V_i. We require that the probabilities of different outcomes obtained from the approximate circuit be within a tolerance δ of the correct probabilities. What is the required precision of approximation for each gate?

3. Any density matrix of a single qubit can be parameterised by the three real components of the Bloch vector $\vec{s} = (s_x, s_y, s_z)$ and written as

$$\rho = \frac{1}{2}\left(\mathbb{1} + s_x X + s_y Y + s_z Z\right)$$

where $X \equiv \sigma_x = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, $Y \equiv \sigma_y = \left[\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right]$, and $Z \equiv \sigma_z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ are the Pauli matrices.

(a) [4 marks] One of the Pauli operators, $\mathbb{1}$, X, Y or Z, was chosen uniformly at random and applied to a qubit in state ρ, but you do not know which particular operator was chosen. Show, using the Bloch vector parametrisation or otherwise, that *from your perspective* the qubit is now prepared in the maximally mixed state

$$\rho \longmapsto \frac{1}{4}\mathbb{1}\rho\mathbb{1} + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z = \frac{1}{2}\mathbb{1}.$$

(b) [5 marks] Alice has n qubits, each of them in state ρ. For each $1 \leqslant k \leqslant n$, she chooses two key bits $a_k, b_k \in \{0, 1\}$ uniformly at random, which are then used to "encrypt" the kth qubit through the following operation:

$$\rho \longmapsto X^{a_k} Z^{b_k}\, \rho\, Z^{b_k} X^{a_k}.$$

The qubits are then passed to Bob, who does not know any of the key bits a_k, b_k. Show that *from Bob's perspective* the outcomes of any complete projective measurement on the qubits are all equally likely.

(c) [5 marks] Alice picks key bits $a, b \in \{0, 1\}$ uniformly at random and doesn't tell anybody what they are. She uses them to encrypt a qubit:

$$\rho \longmapsto X^a Z^b \rho Z^b X^a.$$

She then passes the qubit to Bob, who applies the Hadamard gate H to the encrypted state as follows,

$$X^a Z^b \rho Z^b X^a \longmapsto H X^a Z^b \rho Z^b X^a H,$$

and returns the qubit back to Alice. Before returning the qubit, can Bob obtain any information about the state ρ? Show that Alice can decrypt the returned qubit and obtain the desired state $H\rho H$. What is the decrypting operation?

Recall that a unitary C is said to be a *Clifford gate* if, for any tensor product P of Pauli operators, $CPC^\dagger$ is (up to a phase factor) another tensor product of Pauli operators. Examples of Clifford gates include the Hadamard and the controlled-NOT gate.

(d) [3 marks] Show that compositions of Clifford gates are again Clifford gates.

Alice has n qubits in some initial state $\rho^{\otimes n}$ that she wants to operate on, but she has limited quantum capabilities: *Alice can only implement the Pauli gates.* Bob is able to implement *any* unitary gate, and so can perform Alice's desired computation, but *Alice does not want to reveal any information about the state ρ.*

(e) [4 marks] Suppose Alice wants to apply a sequence of multi-qubit Clifford gates C_1, C_2, …, C_m to her n qubits. Explain how Alice can delegate quantum computation to Bob so that Bob cannot learn anything about the state ρ, but Alice, upon receiving the modified qubits from Bob, can retrieve the desired result of computation.

(f) [4 marks] If the computation that Alice wants to perform is described by a unitary gate which is *not* a Clifford gate, can she still use the same method to delegate the computation to Bob?