Part II

Quantum Information and Computing

Year

2023
2022
2021
2020
2019
2018

Paper 1, Section I
10D Quantum Information and Computation

(a) Assume that you are given a device that is able to clone arbitrary quantum states. Consider two states $|\phi\rangle, |\psi\rangle$ with $|\phi\rangle \neq |\psi\rangle$. Show how the given device can be used to distinguish between these states with arbitrarily high success probability. [You may use without proof any results from the course provided these are clearly stated.]

(b) Assume you are given a device that is able to distinguish the states $|\phi\rangle$ and $|\psi\rangle$ perfectly. Show how this can be used to clone these states. [You can assume that you are able to prepare any computational basis state and implement any unitary operator U.]

(c) Let $\{|\phi_0\rangle, |\phi_1\rangle\}$ and $\{|\psi_0\rangle, |\psi_1\rangle\}$ be two sets of states. Show that there exists a unitary operator U and states $|e_0\rangle$ and $|e_1\rangle$ such that

$$U|\phi_0\rangle|0\rangle = |\psi_0\rangle|e_0\rangle$$
$$U|\phi_1\rangle|0\rangle = |\psi_1\rangle|e_1\rangle$$

if and only if $|\langle\phi_0|\phi_1\rangle| \leqslant |\langle\psi_0|\psi_1\rangle|$.

[*Hint: You can use the fact that for sets of states* $\{|\xi_0\rangle, |\xi_1\rangle\}$ *and* $\{|\eta_0\rangle, |\eta_1\rangle\}$ *with* $\langle\xi_0|\xi_1\rangle = \langle\eta_0|\eta_1\rangle$ *there exists a unitary operator* U *such that* $U|\xi_0\rangle = |\eta_0\rangle$ *and* $U|\xi_1\rangle = |\eta_1\rangle$.]

Paper 2, Section I

10D Quantum Information and Computation

(a) Consider the Bell states

$$|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad \text{and} \quad |\Phi^-_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right). \tag{1}$$

Show that $\langle\Phi^+_{AB}|\, Q \otimes I\, |\Phi^+_{AB}\rangle = \langle\Phi^-_{AB}|\, Q \otimes I\, |\Phi^-_{AB}\rangle$ for any positive semidefinite linear operator Q acting on qubit A.

(b) Suppose you are now given a quantum state which can either be $|\Phi^+_{AB}\rangle$ or $|\Phi^-_{AB}\rangle$ with equal probability.

(i) If you have access to both qubits A and B, can you determine which of the two states you have by doing a measurement on both qubits?

(ii) If you can only access qubit A, can you determine which of the two states you have by doing a measurement on it alone?

(iii) Suppose instead that qubit A is with Alice and qubit B is with Bob. Alice and Bob are at distant locations. They are allowed to do local measurements on the qubits in their possession and can communicate classically with each other. Can they determine the joint state of the two qubits?

(c) Suppose Alice uses the *quantum dense coding protocol* and a third party, Charlie, intercepts the qubit that Alice sends to Bob. Can Charlie infer which of the four bit strings 00, 01, 10 and 11 Alice is trying to send? Justify your answer.

Paper 3, Section I
10D Quantum Information and Computation

(a) Given two positive integers N and a which are coprime to each other (with $1 < a < N$), define the *order* of $a \bmod N$.

(b) For such a pair of integers (a, N), the *modular exponential function* $f : \mathbb{Z} \to \mathbb{Z}_N$, is defined as $f : k \mapsto a^k \bmod N$, where $\mathbb{Z}_N := \{0, 1, \ldots, N-1\}$. Prove that f is a periodic function and determine its period (clearly stating any theorem that you use).

(c) Suppose that we would like to factorise $N = 33$ and we pick $a = 10$. Following the argument presented in the lecture for Shor's algorithm, show how the order of $a \bmod N$ can be used to factorise N. Find the order of $a \bmod N$ by hand and hence factorise N.

(d) Recall that Shor's algorithm for factoring an integer N involves an application of the quantum Fourier transform on m qubits and a subsequent measurement of these m qubits which yields an integer c, where $0 \leqslant c < 2^m$. Suppose we want to factor the number $N = 21$; we pick $a = 8$, $m = 9$ and get the measurement result $c = 256$. Show how you can find the order of $a \bmod N$ from this measurement result. [You should clearly state any results that you use from the lectures.]

Paper 4, Section I

10D Quantum Information and Computation

[In this question you do not need to draw any circuits and you can assume that Alice can perform a measurement on two qubits in the Bell basis.]

(a) Suppose that Alice and Bob share the quantum state

$$|\psi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

and can communicate classically. Alice wants to send an arbitrary qubit state to Bob. State the steps that Alice and Bob need to execute to achieve this goal.

(b) Suppose Alice, Bob and Charlie share the following state of three qubits:

$$|\Psi_{ABC}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right),$$

where the qubits A, B and C are with Alice, Bob and Charlie, respectively. Moreover, Alice has the qubit state $|\alpha\rangle = a\,|0\rangle + b\,|1\rangle$, with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. She now performs the Bell measurement on the two qubits in her possession. Depending on the measurement outcome, she asks Bob and Charlie to perform the necessary correction operations on their individual qubits, as is done in the standard teleportation protocol. Show that the final *joint* state of Bob and Charlie at the end of this protocol is either the state $|\varphi_1\rangle := a\,|00\rangle + b\,|11\rangle$ or the state $|\varphi_2\rangle := a\,|00\rangle - b\,|11\rangle$. Show that these states are entangled if and only if $a \neq 0$ and $b \neq 0$.

Paper 2, Section II

15D Quantum Information and Computation

(a) Let $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$ and let QFT_N denote the quantum Fourier transform mod N. What is the action of QFT_N on $|x\rangle$, where $x \in \mathbb{Z}_N$?

(b) Show that $\mathrm{QFT}_N^2 |x\rangle = |-x\rangle$. Hence show that $\mathrm{QFT}_N^4 = \mathbb{I}$. What can you conclude about the eigenvalues of QFT_N?

(c) Let $f : \mathbb{Z}_{16} \to \mathbb{Z}_4$ be a periodic function such that $f(0) = 2$, $f(1) = 1$, $f(2) = 3$, $f(3) = 0$ and $f(x) = f(x-4)$ for all $x \in \mathbb{Z}_{16}$ (so that $f(4) = 2$ etc.).

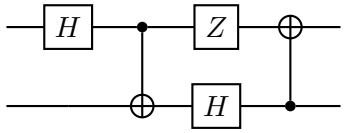
We want to determine the periodicity of the function f using the quantum Fourier transform. The periodicity determination algorithm acts on two registers and involves two measurements – one being a measurement of the second register and one being a measurement of the first register. Work through all the steps of the periodicity determination algorithm, assuming that the outcome of the first measurement is 1 and the outcome of the second measurement is 12. Does the algorithm succeed?

(d) Now consider the same setup as in part (c) but assume that the outcome of the second measurement is 8. Does the algorithm succeed?

Paper 3, Section II

15D Quantum Information and Computation

Consider the following quantum circuit C:

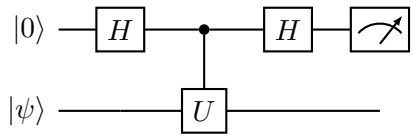


(a) Suppose the state $|0\rangle|0\rangle$ is sent through the circuit. What is the state at the output? Suppose each of the two qubits are measured in the computational basis. What is the distribution of measurement outcomes?

(b) Let V denote the unitary operator corresponding to the circuit C. Draw the quantum circuit corresponding to the inverse operator V^{-1}.

(c) The SWAP gate for two qubits is defined as $\mathrm{SWAP}\,|x\rangle|y\rangle = |y\rangle|x\rangle$, where $x, y \in \{0, 1\}$. Show that the SWAP gate can be implemented as a combination of CNOT gates and draw the corresponding quantum circuit.

(d) Let U be a unitary operator with eigenstate $|\psi\rangle$ such that $U|\psi\rangle = e^{i\theta}|\psi\rangle$. Consider the following quantum circuit:



Write down the final state at the end of the algorithm. What is the probability that the outcome 1 is observed when the first register is measured in the computational basis? Suppose we are promised that either $U|\psi\rangle = |\psi\rangle$ or $U|\psi\rangle = -|\psi\rangle$, but we have no other information about U and $|\psi\rangle$. Show that the above circuit can be used to determine which of these is the case with certainty.

Paper 1, Section I
10D Quantum Information and Computation

Alice and Bob are separated in space and possess local quantum systems A and B respectively.

(a) State the *no-signalling theorem* for quantum states of the composite system AB.

(b) State and prove the *no-cloning theorem* (for unitary processes) for a set $\mathcal{S}$ of quantum states.

(c) Now let $\mathcal{S} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Starting with a suitable state for a 2-qubit composite system AB, show how the no-cloning theorem for the set $\mathcal{S}$ can be seen as a consequence of the no-signalling theorem for AB.

Paper 2, Section I
10D Quantum Information and Computation

(a) Suppose that Alice and Bob are distantly separated in space and they can communicate classically publicly. They also have available a noiseless quantum channel on which there is no eavesdropping. Describe the steps of the BB84 protocol that results in Alice and Bob sharing a secret key of expected length $n/2$. [Note that the steps of information reconciliation and privacy amplification will not be needed in this idealised situation.]

(b) Suppose now that an eavesdropper Eve taps into the quantum channel. Eve also possesses a supply of ancilla qubits each in state $|0\rangle_E$. For each passing qubit $|\psi\rangle_A$ sent by Alice, Eve intercepts it and applies a CX operation to it and one of her ancilla qubits $|0\rangle_E$ with Alice's qubit being the control i.e. Eve applies CX_{AE}. After this action Eve sends Alice's qubit on to Bob while retaining her ancilla qubit.

(i) Show that for two choices of Alice's sent qubits, the qubit received by Bob will be entangled with Eve's corresponding ancilla qubit.

(ii) Calculate the bit error rate for Alice and Bob's final key in part (a) that results from Eve's action.

Paper 3, Section I
10D Quantum Information and Computation

Let $\mathbf{x} = x_0 x_1 \ldots x_{N-1}$ be an N-bit string with $N = 2K$ being even. Let $\mathcal{H}_M$ denote a state space of dimension M with orthonormal basis $\{|\, k\rangle \,:\, k \in \mathbb{Z}_M\}$. A quantum oracle $O_{\mathbf{x}}$ for $\mathbf{x}$ is a unitary operation on $\mathcal{H}_N \otimes \mathcal{H}_2$ whose action is defined by $O_{\mathbf{x}} \,|\, i\rangle \,|\, y\rangle = |\, i\rangle \,|\, y \oplus x_i\rangle$, where $y \in \{0, 1\}$ and $\oplus$ denotes addition modulo 2.

Consider the following oracle problem, called Problem A:
Input: an oracle $O_{\mathbf{x}}$ for some N-bit string $\mathbf{x}$.
Promise: $\mathbf{x}$ is either a constant string, or a balanced string (the latter meaning that $\mathbf{x}$ contains exactly K 0's and K 1's).
Problem: decide if $\mathbf{x}$ is balanced.

(a) Suppose we have a universal set of quantum gates available and any desired unitary operation that is independent of $\mathbf{x}$ may be exactly implemented. Also, we may perform measurements in the basis $\{|\, i\rangle : i \in \mathbb{Z}_N\}$ of an N-dimensional register.

Show that Problem A can be solved with certainty by a quantum algorithm that makes only one query to the oracle $O_{\mathbf{x}}$. The algorithm should begin with each register initially in the state $|\, 0\rangle$ (in the appropriate state space).

(b) Suppose now that in addition to $O_{\mathbf{x}}$ and measurements in the basis $\{|\, i\rangle : i \in \mathbb{Z}_N\}$, we can implement only the Pauli Z gate on a qubit register and gates F and F^{-1} on an N-dimensional register, where F has the property that $F \,|\, 0\rangle = \frac{1}{\sqrt{N}} \sum_{i \in \mathbb{Z}_N} |\, i\rangle$.

By considering the action of Z on a qubit register $|\, y\rangle$, or otherwise, show that with the restricted set of operations, Problem A can be solved with certainty by a quantum algorithm that makes two queries to the oracle $O_{\mathbf{x}}$, and as before, with each register starting in the state $|\, 0\rangle$ (in the appropriate state space).

Paper 4, Section I
10D Quantum Information and Computation

(a) Let B_n denote the set of all n-bit strings and write $N = 2^n$. The *Grover iteration operator* on n qubits is given by

$$Q = -H_n I_0 H_n I_{x_0}.$$

Give a definition of the constituent operators H_n, I_0 and I_{x_0} and state a geometrical interpretation of the action of Q on the space of n qubits.

(b) The quantum oracle for the identity function $\mathcal{I} : B_n \to B_n$, $\mathcal{I}(x) = x$ is the unitary operation $U_{\mathcal{I}}$ on $2n$ qubits defined by $U_{\mathcal{I}}(|\,x\rangle\,|\,y\rangle) = |\,x\rangle\,|\,y \oplus \mathcal{I}(x)\rangle$ for all $x, y \in B_n$. Here $\oplus$ denotes the sum of n-bit strings bitwise mod 2 separately at each of the n positions in the string, *i.e.* the group operation in $(\mathbb{Z}_2)^n$.

Show how the action of $U_{\mathcal{I}}$ can be represented by a circuit of CX gates.

(c) Suppose we are given a quantum oracle for $\mathcal{I}$ but it is known to be faulty on one of its inputs. Instead of the full identity function it implements instead the function $f : B_n \to B_n$ given by

$$f(x) = \begin{cases} x & \text{for all } x \neq x_0 \\ x \oplus a & \text{for } x = x_0 \end{cases}$$

where $a \in B_n$ is the n-bit string $00\ldots01$ and where $x_0 \in B_n$ is unknown, *i.e.* the given quantum oracle actually implements U_f. By providing a suitable input state for a circuit involving U_f and further gates independent of f, show how I_{x_0} on n qubits may be implemented in terms of U_f.

(d) Hence or otherwise show that for sufficiently large N, x_0 may be determined with some constant probability greater than $\frac{1}{2}$ using $O(\sqrt{N})$ queries to the oracle U_f.

Paper 2, Section II
15D Quantum Information and Computation

(a) (i) Define the *Bell measurement* on two qubits.

(ii) In terms of the Bell measurement and the Bell state $|\phi^+\rangle$ give the steps of the quantum teleportation protocol. You need not give a derivation of the steps but you should clearly state all inputs and outputs of the protocol.

(iii) Suppose now that the $|\phi^+\rangle$ state used in the protocol is replaced by $|\xi\rangle = I \otimes U\,|\phi^+\rangle$, where U is any 1-qubit unitary and all steps of the protocol remain otherwise the same as in part (ii) above. State the outputs of this modified protocol and give a justification of your answer. [You may quote any statements from part (ii) above.]

(b) A *programmable 1-qubit gate* $\mathcal{G}$ is defined to be a device acting on two registers A and B, where A is a 1-qubit register called the input register and B is a K-qubit register (for some fixed $K \in \mathbb{N}$) called the program register. For any given state of AB the action of $\mathcal{G}$ is a fixed unitary operation G on the $K+1$ qubits, which is required to satisfy the following condition called (PROG):

For any 1-qubit unitary U there is a K-qubit state $|P_U\rangle$ such that for any 1-qubit state $|\alpha\rangle$ we have

$$|\alpha\rangle \otimes |P_U\rangle \longmapsto G(|\alpha\rangle \otimes |P_U\rangle) = (U|\alpha\rangle) \otimes \left|\tilde{P}_U\right\rangle.$$

Here $\left|\tilde{P}_U\right\rangle$ is some K-qubit state (which could generally depend on $|\alpha\rangle$ too). Thus $|P_U\rangle$ serves as a "program" for the application of U to any 1-qubit state $|\alpha\rangle$ via the fixed unitary action G.

(i) By considering suitable inner products or otherwise, show that if (PROG) holds then $\left|\tilde{P}_U\right\rangle$ must be independent of the state $|\alpha\rangle$.

(ii) Suppose that $|P_U\rangle$ and $|P_V\rangle$ implement 1-qubit unitaries U and V that have physically different actions i.e. $U \neq Ve^{i\theta}$ for any phase θ. Show that $|P_U\rangle$ and $|P_V\rangle$ must then be orthogonal if (PROG) holds. [*Hint: It may be helpful to show that for any unitary W, if $\langle\alpha|W|\alpha\rangle$ is independent of $|\alpha\rangle$ then W must be the identity gate (up to an overall phase).*]

(iii) Show that a programmable 1-qubit gate $\mathcal{G}$ satisfying (PROG) cannot exist.

(iv) Suppose now that (PROG) is extended to allow the action of $\mathcal{G}$ to involve quantum measurements as well as unitary operations and we require of the "program" $|P_U\rangle$ only that it succeeds in applying U to $|\alpha\rangle$ with at least some constant probability $0 < p < 1$ independent of U and $|\alpha\rangle$, *i.e.* the action of $\mathcal{G}$ on $|\alpha\rangle \otimes |P_U\rangle$ results in $U|\alpha\rangle$ in the first register with probability at least p for each U and $|\alpha\rangle$. Can such a probabilistic programmable 1-qubit gate exist? Give a reason for your answer.

Paper 3, Section II
15D Quantum Information and Computation

For any positive integer N, let QFT_N denote the quantum Fourier transform mod N.

(a) Consider an N-dimensional state space equipped with an orthonormal basis $\mathcal{B} = \{|\,k\rangle : k \in \mathbb{Z}_N\}$. You may assume that QFT_N, measurements in the basis $\mathcal{B}$, and the basic arithmetic operations of addition and multiplication modulo N may all be performed in time $O(\mathrm{poly}(\log N))$.

Consider the function $f : \mathbb{Z}_N \to \mathbb{Z}_N$ defined by $f(x) = a^x \mod N$, where we have fixed a choice of $a \in \mathbb{Z}_N$ with $a \neq 0$. It is promised that f is periodic with period r which divides N exactly, and f is one-to-one within each period.

Describe a quantum algorithm which runs in time $O(\mathrm{poly}(\log N))$ that will identify r with success probability at least $1/2$. The algorithm should start with each quantum register (of suitable dimension) being in state $|\,0\rangle$ and it should have the property that in any run, we also learn whether it has succeeded or not. For any step of your algorithm that is not one of the operations listed above, give a brief justification that it can be performed in time $O(\mathrm{poly}(\log N))$. [You may use without proof any results from classical number theory or classical probability theory but they must be stated clearly.]

(b) Consider an N-dimensional state space with orthonormal basis $\{|\,i\rangle : i \in \mathbb{Z}_N\}$. Let S be the operation defined by $S\,|\,i\rangle = |\,i+1\rangle$ for all $i \in \mathbb{Z}_N$ (and $+$ being addition modulo N). Show that the states $\mathrm{QFT}_N\,|\,k\rangle$ for $k \in \mathbb{Z}_N$ are eigenvectors of S.
Now let $N = 4$ and represent each basis state $|\,j\rangle$ with two qubits as $|\,x\rangle\,|\,y\rangle$ where the 2-bit string xy is j written in binary. Suppose we can implement only the gates QFT_4, its inverse and any 1-qubit phase gate $P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$. Show how S may be implemented on any input 2-qubit state and sketch the circuit for S.

Paper 1, Section I
10D Quantum Information and Computation

Alice wishes to communicate to Bob a 1-bit message $m = 0$ or $m = 1$ chosen by her with equal prior probabilities 1/2. For $m = 0$ (respectively $m = 1$) she sends Bob the quantum state $|a_0\rangle$ (respectively $|a_1\rangle$). On receiving the state, Bob applies quantum operations to it, to try to determine Alice's message. The Helstrom–Holevo theorem asserts that the probability P_S for Bob to correctly determine Alice's message is bounded by $P_S \leqslant \frac{1}{2}(1 + \sin\theta)$, where $\theta = \cos^{-1}|\langle a_0|a_1\rangle|$, and that this bound is achievable.

(a) Suppose that $|a_0\rangle = |0\rangle$ and $|a_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and that Bob measures the received state in the basis $\{|b_0\rangle, |b_1\rangle\}$, where $|b_0\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle$ and $|b_1\rangle = -\sin\beta\,|0\rangle + \cos\beta\,|1\rangle$, to produce his output 0 or 1, respectively. Calculate the probability P_S that Bob correctly determines Alice's message, and show that the maximum value of P_S over choices of $\beta \in (-\frac{\pi}{2}, \frac{\pi}{2}]$ achieves the Helstrom–Holevo bound.

(b) State the no-cloning theorem as it applies to unitary processes and a set of two non-orthogonal states $\{|c_0\rangle, |c_1\rangle\}$. Show that the Helstrom–Holevo theorem implies the validity of the no-cloning theorem in this situation.

Paper 2, Section I
10D Quantum Information and Computation

Let $\mathcal{B}_n$ denote the set of all n-bit strings and let $f : \mathcal{B}_n \to \mathcal{B}_1$ be a Boolean function which obeys either

(I) $f(x) = 0$ for all $x \in \mathcal{B}_n$, or
(II) $f(x) = 0$ for exactly half of all $x \in \mathcal{B}_n$.

Suppose we are given the n-qubit state

$$|\,\xi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathcal{B}_n} (-1)^{f(x)}\,|x\rangle\ .$$

Show how we may determine with certainty whether f is of case (I) or case (II).

Suppose now that Alice and Bob are separated in space. Alice possesses a quantum oracle for a Boolean function $f_A : \mathcal{B}_n \to \mathcal{B}_1$ and Bob similarly possess a quantum oracle for a Boolean function $f_B : \mathcal{B}_n \to \mathcal{B}_1$. These functions are arbitrary, except that either

(1) $f_A(x) = f_B(x)$ for all $x \in \mathcal{B}_n$, or
(2) $f_A(x) = f_B(x)$ for exactly half of all $x \in \mathcal{B}_n$.

Alice and Bob each have available a supply of qubits in state $|0\rangle$ and each can apply local quantum operations (including their own function oracle) to any qubits in their possession. Additionally, they can send qubits to each other.

Show how Bob may decide with certainty which case applies, after he has received n qubits from Alice. [*Hint: You may find it helpful to consider the function* $h(x) = f_A(x) \oplus f_B(x)$, *where* $\oplus$ *denotes addition mod 2.*]

Paper 3, Section I
10D Quantum Information and Computation

Let $|\psi\rangle_{AB}$ be the joint state of a bipartite system AB with subsystems A and B separated in space. Suppose that Alice and Bob have access only to subsystems A and B respectively, on which they can perform local quantum operations.

Alice performs a unitary operation U on A and then a (generally incomplete) measurement on A, with projectors $\{\Pi_a\}$ labelled by her possible measurement outcomes a. Then Bob performs a complete measurement on B relative to the orthonormal basis $\{|b\rangle\}$ labelled by his possible outcomes b.

Show that the probability distribution of Bob's measurement outcomes is unaffected by whether or not Alice actually performs the local operations on A described above.

Paper 4, Section I
10D Quantum Information and Computation

Let $\mathcal{H}$ be a state space of dimension N with standard orthonormal basis $\{|k\rangle\}$ labelled by $k \in \mathbb{Z}_N$. Let QFT denote the quantum Fourier transform mod N and let S denote the operation defined by $S|k\rangle = |k+1 \mod N\rangle$.

(a) Introduce the basis $\{|\chi_k\rangle\}$ defined by $|\chi_k\rangle = \mathrm{QFT}^{-1}|k\rangle$. Show that each $|\chi_k\rangle$ is an eigenstate of S and determine the corresponding eigenvalue.

(b) By expressing a generic state $|v\rangle \in \mathcal{H}$ in the $\{|\chi_k\rangle\}$ basis, show that $\mathrm{QFT}\,|v\rangle$ and $\mathrm{QFT}(S|v\rangle)$ have the same output distribution if measured in the standard basis.

(c) Let A, r be positive integers with $Ar = N$, and let x_0 be an integer with $0 \leqslant x_0 < r$. Suppose that we are given the state

$$|\xi\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr \mod N\rangle \ ,$$

where x_0 and r are unknown to us. Using part (b) or otherwise, show that a standard basis measurement on $\mathrm{QFT}\,|\xi\rangle$ has an output distribution that is independent of x_0.

Paper 2, Section II

15D Quantum Information and Computation

Alice and Bob are separated in space and can communicate only over a noiseless public classical channel, i.e. they can exchange bit string messages perfectly, but the messages can be read by anyone. An eavesdropper Eve constantly monitors the channel, but cannot alter any passing messages. Alice wishes to communicate an m-bit string message to Bob whilst keeping it secret from Eve.

(a) Explain how Alice can do this by the one-time pad method, specifying clearly any additional resource that Alice and Bob need. Explain why in this method, Alice's message does, in fact, remain secure against eavesdropping.

(b) Suppose now that Alice and Bob do not possess the additional resource needed in part (a) for the one-time pad, but that they instead possess n pairs of qubits, where $n \gg 1$, with each pair being in the state

$$|\psi\rangle_{AB} = t\,|00\rangle_{AB} + s\,|11\rangle_{AB}\,,$$

where the real parameters (t, s) are known to Alice and Bob and obey $t > s > 0$ and $t^2 + s^2 = 1$. For each qubit pair in state $|\psi\rangle_{AB}$, Alice possesses qubit A and Bob possesses qubit B. They each also have available a supply of ancilla qubits, each in state $|0\rangle$, and they can each perform local quantum operations on qubits in their possession.

Show how Alice, using only local quantum operations, can convert each $|\psi\rangle_{AB}$ state into $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$ by a process that succeeds with non-zero probability. [*Hint: It may be useful for Alice to start by adjoining an ancilla qubit* $|0\rangle_{A'}$ *and work locally on her two qubits in* $|0\rangle_{A'}\,|\psi\rangle_{AB}$.]

Hence, or otherwise, show how Alice can communicate a bit string of expected length $(2s^2)n$ to Bob in a way that keeps it secure against eavesdropping by Eve.

Paper 3, Section II

15D Quantum Information and Computation

Let $\mathcal{B}_n$ denote the set of all n-bit strings and let $\mathcal{H}_n$ denote the space of n qubits.

(a) Suppose $f : \mathcal{B}_2 \to \mathcal{B}_1$ has the property that $f(x_0) = 1$ for a unique $x_0 \in \mathcal{B}_2$ and suppose we have a quantum oracle U_f.

(i) Let $|\psi_0\rangle = \frac{1}{2}\sum_{x\in\mathcal{B}_2} |x\rangle$ and introduce the operators

$$I_{x_0} = I_2 - 2\,|x_0\rangle\langle x_0| \qquad \text{and} \qquad J = I_2 - 2\,|\psi_0\rangle\langle\psi_0|$$

on $\mathcal{H}_2$, where I_2 is the identity operator. Give a geometrical description of the actions of $-J$, I_{x_0} and $Q = -JI_{x_0}$ on the 2-dimensional subspace of $\mathcal{H}_2$ given by the real span of $|x_0\rangle$ and $|\psi_0\rangle$. [You may assume without proof that the product of two reflections in $\mathbb{R}^2$ is a rotation through twice the angle between the mirror lines.]

(ii) Using the results of part (i), or otherwise, show how we may determine x_0 with certainty, starting with a supply of qubits each in state $|0\rangle$ and using U_f only once, together with other quantum operations that are independent of f.

(b) Suppose $\mathcal{H}_n = A \oplus A^\perp$, where A is a fixed linear subspace with orthogonal complement $A^\perp$. Let Π_A denote the projection operator onto A and let $I_A = I - 2\,\Pi_A$, where I is the identity operator on $\mathcal{H}_n$.

(i) Show that any $|\xi\rangle \in \mathcal{H}_n$ can be written as $|\xi\rangle = \sin\theta\,|\alpha\rangle + \cos\theta\,|\beta\rangle$, where $\theta \in [0, \pi/2]$, and $|\alpha\rangle \in A$ and $|\beta\rangle \in A^\perp$ are normalised.

(ii) Let $I_\xi = I - 2\,|\xi\rangle\langle\xi|$ and $Q = -I_\xi I_A$. Show that $Q|\alpha\rangle = -\sin 2\theta\,|\beta\rangle + \cos 2\theta\,|\alpha\rangle$.

(iii) Now assume, in addition, that $Q|\beta\rangle = \cos 2\theta\,|\beta\rangle + \sin 2\theta\,|\alpha\rangle$ and that $|\xi\rangle = U\,|0\ldots0\rangle$ for some unitary operation U. Suppose we can implement the operators U, $U^\dagger$, I_A as well as the operation $I - 2|0\ldots0\rangle\langle 0\ldots0|$. In the case $\theta = \pi/10$, show how the n-qubit state $|\alpha\rangle$ may be made exactly from $|0\ldots0\rangle$ by a process that succeeds with certainty.

Paper 1, Section I

10C Quantum Information and Computation

Suppose we measure an observable $A = \hat{n} \cdot \vec{\sigma}$ on a qubit, where $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli operators.

(i) Express A as a 2×2 matrix in terms of the components of $\hat{n}$.

(ii) Representing $\hat{n}$ in terms of spherical polar coordinates as $\hat{n} = (1, \theta, \phi)$, rewrite the above matrix in terms of the angles θ and ϕ.

(iii) What are the possible outcomes of the above measurement?

(iv) Suppose the qubit is initially in a state $|1\rangle$. What is the probability of getting an outcome 1?

(v) Consider the three-qubit state

$$|\psi\rangle = a\,|000\rangle + b\,|010\rangle + c\,|110\rangle + d\,|111\rangle + e\,|100\rangle\,.$$

Suppose the second qubit is measured relative to the computational basis. What is the probability of getting an outcome 1? State the rule that you are using.

Paper 2, Section I

10C Quantum Information and Computation

Consider the set of states

$$|\beta_{zx}\rangle := \frac{1}{\sqrt{2}}[|0x\rangle + (-1)^z\,|1\overline{x}\rangle],$$

where $x, z \in \{0, 1\}$ and $\overline{x} = x \oplus 1$ (addition modulo 2).

(i) Show that

$$(H \otimes \mathbb{I}) \circ \mathrm{CX}\,|\beta_{zx}\rangle = |zx\rangle \quad \forall\, z, x \in \{0, 1\},$$

where H denotes the Hadamard gate and CX denotes the controlled-X gate.

(ii) Show that for any $z, x \in \{0, 1\}$,

$$(Z^z X^x \otimes \mathbb{I})\,|\beta_{00}\rangle = |\beta_{zx}\rangle\,. \qquad (*)$$

[*Hint: For any unitary operator U, we have* $(U \otimes \mathbb{I})\,|\beta_{00}\rangle = (\mathbb{I} \otimes U^T)\,|\beta_{00}\rangle$, *where U^T denotes the transpose of U with respect to the computational basis.*]

(iii) Suppose Alice and Bob initially share the state $|\beta_{00}\rangle$. Show using $(*)$ how Alice can communicate two classical bits to Bob by sending him only a single qubit.

Paper 3, Section I

10C Quantum Information and Computation

For $\phi \in [0, 2\pi)$ and $|\psi\rangle \in \mathbb{C}^4$ consider the operator

$$R_\psi^\phi = \mathbb{I} - \left(1 - e^{i\phi}\right) |\psi\rangle \langle\psi| \,.$$

Let U be a unitary operator on $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ with action on $|00\rangle$ given as follows

$$U|00\rangle = \sqrt{p}\,|g\rangle + \sqrt{1-p}\,|b\rangle =: |\psi_{\text{in}}\rangle \,, \qquad (\dagger)$$

where p is a constant in $[0, 1]$ and $|g\rangle, |b\rangle \in \mathbb{C}^4$ are orthonormal states.

(i) Give an explicit expression of the state $R_g^\phi U|00\rangle$.

(ii) Find a $|\psi\rangle \in \mathbb{C}^4$ for which $R_\psi^\pi = U R_{00}^\pi U^\dagger$.

(iii) Choosing $p = 1/4$ in equation $(\dagger)$, calculate the state $U R_{00}^\pi U^\dagger R_g^\phi U|00\rangle$. For what choice of $\phi \in [0, 2\pi)$ is this state proportional to $|g\rangle$?

(iv) Describe how the above considerations can be used to find a marked element g in a list of four items $\{g, b_1, b_2, b_3\}$. Assume that you have the state $|00\rangle$ and can act on it with a unitary operator that prepares the uniform superposition of four orthonormal basis states $|g\rangle, |b_1\rangle, |b_2\rangle, |b_3\rangle$ of $\mathbb{C}^4$. [You may use the operators U (defined in $(\dagger)$), $U^\dagger$ and R_ψ^ϕ for any choice of $\phi \in [0, 2\pi)$ and any $|\psi\rangle \in \mathbb{C}^4$.]

Paper 4, Section I

10C Quantum Information and Computation

(i) What is the action of QFT_N on a state $|x\rangle$, where $x \in \{0, 1, 2, \ldots, N-1\}$ and QFT_N denotes the Quantum Fourier Transform modulo N?

(ii) For the case $N = 4$ write $0, 1, 2, 3$ respectively in binary as $00, 01, 10, 11$ thereby identifying the four-dimensional space as that of two qubits. Show that $\mathrm{QFT}_N|10\rangle$ is an unentangled state of the two qubits.

(iii) Prove that $(\mathrm{QFT}_N)^2|x\rangle = |N - x\rangle$, where $(\mathrm{QFT}_N)^2 \equiv \mathrm{QFT}_N \circ \mathrm{QFT}_N$.
[*Hint: For* $\omega = e^{2\pi i/N}$, $\sum_{m=0}^{N-1} \omega^{mK} = 0$ *if* K *is not a multiple of* N.]

(iv) What is the action of $(\mathrm{QFT}_N)^4$ on a state $|x\rangle$, for any $x \in \{0, 1, 2, \ldots, N-1\}$? Use the above to determine what the eigenvalues of QFT_N are.

Paper 2, Section II

15C Quantum Information and Computation

(a) Show how the n-qubit state

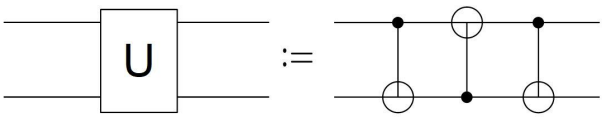
$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle$$

can be generated from a computational basis state of $\mathbb{C}^n$ by the action of Hadamard gates.

(b) Prove that $CZ = (I \otimes H) CNOT_{12} (I \otimes H)$, where CZ denotes the controlled-Z gate. Justify (without any explicit calculations) the following identity:

$$CNOT_{12} = (I \otimes H) CZ (I \otimes H).$$

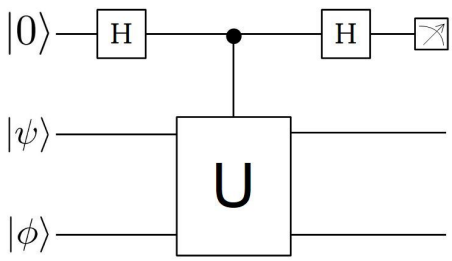
(c) Consider the following two-qubit circuit:



What is its action on an arbitrary 2-qubit state $|\psi\rangle \otimes |\phi\rangle$? In particular, for two given states $|\psi\rangle$ and $|\phi\rangle$, find the states $|\alpha\rangle$ and $|\beta\rangle$ such that

$$U(|\psi\rangle \otimes |\phi\rangle) = |\alpha\rangle \otimes |\beta\rangle \,.$$

(d) Consider the following quantum circuit diagram



where the measurement is relative to the computational basis and U is the quantum gate from part (c). Note that the second gate in the circuit performs the following controlled operation:

$$|0\rangle\,|\psi\rangle\,|\phi\rangle \mapsto |0\rangle\,|\psi\rangle\,|\phi\rangle \;\;;\;\; |1\rangle\,|\psi\rangle\,|\phi\rangle \mapsto |1\rangle\, U\left(|\psi\rangle\,|\phi\rangle\right).$$

(i) Give expressions for the joint state of the three qubits after the action of the first Hadamard gate; after the action of the quantum gate U; and after the action of the second Hadamard gate.

(ii) Compute the probabilities p_0 and p_1 of getting outcome 0 and 1, respectively, in the measurement.

(iii) How can the above circuit be used to determine (with high probability) whether the two states $|\psi\rangle$ and $|\phi\rangle$ are identical or not? [Assume that you are given arbitrarily many copies of the three input states and that the quantum circuit can be used arbitrarily many times.]

Paper 3, Section II

15C Quantum Information and Computation

Consider the quantum oracle U_f for a function $f : B_n \to B_n$ which acts on the state $|x\rangle\,|y\rangle$ of $2n$ qubits as follows:

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle\,. \tag{1}$$

The function f is promised to have the following property: there exists a $z \in B_n$ such that for any $x, y \in B_n$,

$$[f(x) = f(y)] \quad \text{if and only if} \quad x \oplus y \in \{0^n, z\}, \tag{2}$$

where $0^n \equiv (0, 0, \ldots, 0) \in B_n$.

(a) What is the nature of the function f for the case in which $z = 0^n$, and for the case in which $z \neq 0^n$?

(b) Suppose initially each of the $2n$ qubits are in the state $|0\rangle$. They are then subject to the following operations:

1. Each of the first n qubits forming an input register are acted on by Hadamard gates;
2. The $2n$ qubits are then acted on by the quantum oracle U_f;
3. Next, the qubits in the input register are individually acted on by Hadamard gates.

(i) List the states of the $2n$ qubits after each of the above operations; the expression for the final state should involve the n-bit "dot product" which is defined as follows:

$$a \cdot b = (a_1 b_1 + a_2 b_2 + \ldots + a_n b_n) \bmod 2,$$

where $a, b \in B_n$ with $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$.

(ii) Justify that if $z = 0^n$ then for any $y \in B_n$ and any $\varphi(x, y) \in \{-1, +1\}$, the following identity holds:

$$\left\| \sum_{x \in B_n} \varphi(x, y)\,|f(x)\rangle \right\|^2 = \left\| \sum_{x \in B_n} \varphi(x, y)\,|x\rangle \right\|^2. \tag{3}$$

(iii) For the case $z = 0^n$, what is the probability that a measurement of the input register, relative to the computational basis of $\mathbb{C}^n$ results in a string $y \in B_n$?

(iv) For the case $z \neq 0^n$, show that the probability that the above-mentioned measurement of the input register results in a string $y \in B_n$, is equal to the following:

zero for all strings $y \in B_n$ satisfying $y \cdot z = 1$, and

$2^{-(n-1)}$ for any fixed string $y \in B_n$ satisfying $y \cdot z = 0$.

[State any identity you may employ. You may use $(x \oplus z) \cdot y = (x \cdot y) \oplus (z \cdot y)$, $\forall\, x, y, z \in B_n$.]

Paper 4, Section I

10D Quantum Information and Computation

(a) Define the *order* of α mod N for coprime integers α and N with $\alpha < N$. Explain briefly how knowledge of this order can be used to provide a factor of N, stating conditions on α and its order that must be satisfied.

(b) Shor's algorithm for factoring N starts by choosing $\alpha < N$ coprime. Describe the subsequent steps of a single run of Shor's algorithm that computes the order of α mod N with probability $O(1/\log\log N)$.

[*Any significant theorems that you invoke to justify the algorithm should be clearly stated (but proofs are not required). In addition you may use without proof the following two technical results.*

Theorem FT: For positive integers t and M with $M \geqslant t^2$, and any $0 \leqslant x_0 < t$, let K be the largest integer such that $x_0 + (K-1)t < M$. Let QFT denote the quantum Fourier transform mod M. Suppose we measure $QFT\left(\frac{1}{\sqrt{K}}\sum_{k=0}^{K-1}|x_0+kt\rangle\right)$ to obtain an integer c with $0 \leqslant c < M$. Then with probability $O(1/\log\log t)$, c will be an integer closest to a multiple $j(M/t)$ of M/t for which the value of j (between 0 and t) is coprime to t.

Theorem CF: For any rational number a/b with $0 < a/b < 1$ and with integers a and b having at most n digits each, let p/q with p and q coprime, be any rational number satisfying

$$\left|\frac{a}{b} - \frac{p}{q}\right| \leqslant \frac{1}{2q^2}.$$

Then p/q is one of the $O(n)$ convergents of the continued fraction of a/b and all the convergents can be classically computed from a/b in time $O(n^3)$.]

Paper 3, Section I

10D Quantum Information and Computation

Let B_n denote the set of all n-bit strings and write $N = 2^n$. Let I denote the identity operator on n qubits and for $G = \{x_1, x_2, \ldots, x_k\} \subset B_n$ introduce the n-qubit operator

$$Q = -H_n I_0 H_n I_G$$

where $H_n = H \otimes \ldots \otimes H$ is the Hadamard operation on each of the n qubits, and I_0 and I_G are given by

$$I_0 = I - 2\left|00\ldots0\right\rangle\left\langle 00\ldots0\right| \qquad I_G = I - 2\sum_{x\in G}\left|x\right\rangle\left\langle x\right|.$$

Also introduce the states

$$\left|\psi_0\right\rangle = \frac{1}{\sqrt{N}}\sum_{x\in B_n}\left|x\right\rangle \qquad \left|\psi_G\right\rangle = \frac{1}{\sqrt{k}}\sum_{x\in G}\left|x\right\rangle \qquad \left|\psi_B\right\rangle = \frac{1}{\sqrt{N-k}}\sum_{x\notin G}\left|x\right\rangle.$$

Let $\mathcal{P}$ denote the real span of $\left|\psi_0\right\rangle$ and $\left|\psi_G\right\rangle$.

(a) Show that Q maps $\mathcal{P}$ to itself, and derive a geometrical interpretation of the action of Q on $\mathcal{P}$, stating clearly any results from Euclidean geometry that you use.

(b) Let $f : B_n \to B_1$ be the Boolean function such that $f(x) = 1$ iff $x \in G$. Suppose that $k = N/4$. Show that we can obtain an $x \in G$ with certainty by using just one application of the standard quantum oracle U_f for f (together with other operations that are independent of f).

Paper 2, Section I

10D Quantum Information and Computation

The BB84 quantum key distribution protocol begins with Alice choosing two uniformly random bit strings $X = x_1 x_2 \ldots x_m$ and $Y = y_1 y_2 \ldots y_m$.

(a) In terms of these strings, describe Alice's process of conjugate coding for the BB84 protocol.

(b) Suppose Alice and Bob are distantly separated in space and have available a noiseless quantum channel on which there is no eavesdropping. They can also communicate classically publicly. For this idealised situation, describe the steps of the BB84 protocol that results in Alice and Bob sharing a secret key of expected length $m/2$.

(c) Suppose now that an eavesdropper Eve taps into the channel and carries out the following action on each passing qubit. With probability $1-p$, Eve lets it pass undisturbed, and with probability p she chooses a bit $w \in \{0,1\}$ uniformly at random and measures the qubit in basis B_w where $B_0 = \{|0\rangle, |1\rangle\}$ and $B_1 = \{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$. After measurement Eve sends the post-measurement state on to Bob. Calculate the bit error rate for Alice and Bob's final key in part (b) that results from Eve's action.

Paper 1, Section I

10D Quantum Information and Computation

Introduce the 2-qubit states

$$|\beta_{xz}\rangle = (Z^z X^x) \otimes I \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) ,$$

where X and Z are the standard qubit Pauli operations and $x, z \in \{0, 1\}$.

(a) For any 1-qubit state $|\alpha\rangle$ show that the 3-qubit state $|\alpha\rangle_C |\beta_{00}\rangle_{AB}$ of system CAB can be expressed as

$$|\alpha\rangle_C |\beta_{00}\rangle_{AB} = \frac{1}{2} \sum_{x,z=0}^{1} |\beta_{xz}\rangle_{CA} |\mu_{xz}\rangle_B ,$$

where the 1-qubit states $|\mu_{xz}\rangle$ are uniquely determined. Show that $|\mu_{10}\rangle = X |\alpha\rangle$.

(b) In addition to $|\mu_{10}\rangle = X |\alpha\rangle$ you may now assume that $|\mu_{xz}\rangle = X^x Z^z |\alpha\rangle$. Alice and Bob are separated distantly in space and share a $|\beta_{00}\rangle_{AB}$ state with A and B labelling qubits held by Alice and Bob respectively. Alice also has a qubit C in state $|\alpha\rangle$ whose identity is unknown to her. Using the results of part (a) show how she can transfer the state of C to Bob using only local operations and classical communication, i.e. the sending of quantum states across space is not allowed.

(c) Suppose that in part (b), while sharing the $|\beta_{00}\rangle_{AB}$ state, Alice and Bob are also unable to engage in any classical communication, i.e. they are able only to perform local operations. Can Alice now, perhaps by a modified process, transfer the state of C to Bob? Give a reason for your answer.

Paper 3, Section II

15D Quantum Information and Computation

Let $\mathcal{H}_d$ denote a d-dimensional state space with orthonormal basis $\{|y\rangle : y \in \mathbb{Z}_d\}$. For any $f : \mathbb{Z}_m \to \mathbb{Z}_n$ let U_f be the operator on $\mathcal{H}_m \otimes \mathcal{H}_n$ defined by

$$U_f |x\rangle |y\rangle = |x\rangle |y + f(x) \bmod n\rangle$$

for all $x \in \mathbb{Z}_m$ and $y \in \mathbb{Z}_n$.

(a) Define QFT, the quantum Fourier transform mod d (for any chosen d).

(b) Let S on $\mathcal{H}_d$ (for any chosen d) denote the operator defined by

$$S |y\rangle = |y + 1 \bmod d\rangle$$

for $y \in \mathbb{Z}_d$. Show that the Fourier basis states $|\xi_x\rangle = QFT |x\rangle$ for $x \in \mathbb{Z}_d$ are eigenstates of S. By expressing U_f in terms of S find a basis of eigenstates of U_f and determine the corresponding eigenvalues.

(c) Consider the following oracle promise problem:
Input: an oracle for a function $f : \mathbb{Z}_3 \to \mathbb{Z}_3$.
Promise: f has the form $f(x) = sx + t$ where s and t are unknown coefficients (and with all arithmetic being mod 3).
Problem: Determine s with certainty.

Can this problem be solved by a single query to a classical oracle for f (and possible further processing independent of f)? Give a reason for your answer.

Using the results of part (b) or otherwise, give a quantum algorithm for this problem that makes just one query to the quantum oracle U_f for f.

(d) For any $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, let $f_1(x) = f(x + 1)$ and $f_2(x) = -f(x)$ (all arithmetic being mod 3). Show how U_{f_1} and U_{f_2} can each be implemented with one use of U_f together with other unitary gates that are independent of f.

(e) Consider now the oracle problem of the form in part (c) except that now f is a quadratic function $f(x) = ax^2 + bx + c$ with unknown coefficients a, b, c (and all arithmetic being mod 3), and the problem is to determine the coefficient a with certainty. Using the results of part (d) or otherwise, give a quantum algorithm for this problem that makes just two queries to the quantum oracle for f.

Paper 2, Section II

15D Quantum Information and Computation

Let $|\alpha_0\rangle \neq |\alpha_1\rangle$ be two quantum states and let p_0 and p_1 be associated probabilities with $p_0 + p_1 = 1$, $p_0 \neq 0$, $p_1 \neq 0$ and $p_0 \geqslant p_1$. Alice chooses state $|\alpha_i\rangle$ with probability p_i and sends it to Bob. Upon receiving it, Bob performs a 2-outcome measurement $\mathcal{M}$ with outcomes labelled 0 and 1, in an attempt to identify which state Alice sent.

(a) By using the extremal property of eigenvalues, or otherwise, show that the operator $D = p_0 |\alpha_0\rangle \langle\alpha_0| - p_1 |\alpha_1\rangle \langle\alpha_1|$ has exactly two nonzero eigenvalues, one of which is positive and the other negative.

(b) Let P_S denote the probability that Bob correctly identifies Alice's sent state. If the measurement $\mathcal{M}$ comprises orthogonal projectors $\{\Pi_0, \Pi_1\}$ (corresponding to outcomes 0 and 1 respectively) give an expression for P_S in terms of p_1, Π_0 and D.

(c) Show that the optimal success probability P_S^{opt}, i.e. the maximum attainable value of P_S, is

$$P_S^{\text{opt}} = \frac{1 + \sqrt{1 - 4p_0 p_1 \cos^2\theta}}{2},$$

where $\cos\theta = |\langle\alpha_0|\alpha_1\rangle|$.

(d) Suppose we now place the following extra requirement on Bob's discrimination process: whenever Bob obtains output 0 then the state sent by Alice was definitely $|\alpha_0\rangle$. Show that Bob's P_S^{opt} now satisfies $P_S^{\text{opt}} \geqslant 1 - p_0 \cos^2\theta$.

Paper 4, Section I

10D Quantum Information and Computation

Let B_n denote the set of all n-bit strings. Suppose we are given a 2-qubit quantum gate I_{x_0} which is promised to be of the form

$$I_{x_0}\,|\,x\rangle = \begin{cases} \;\;|\,x\rangle & x \neq x_0 \\ -\,|\,x\rangle & x = x_0 \end{cases}$$

but the 2-bit string x_0 is unknown to us. We wish to determine x_0 with the least number of queries to I_{x_0}. Define $A = I - 2\,|\,\psi\rangle\langle\psi|$, where I is the identity operator and $|\,\psi\rangle = \frac{1}{2}\sum_{x\in B_2}|\,x\rangle$.

(a) Is A unitary? Justify your answer.

(b) Compute the action of I_{x_0} on $|\,\psi\rangle$, and the action of $|\,\psi\rangle\langle\psi|$ on $|\,x_0\rangle$, in each case expressing your answer in terms of $|\,\psi\rangle$ and $|\,x_0\rangle$. Hence or otherwise show that x_0 may be determined with certainty using only one application of the gate I_{x_0}, together with any other gates that are independent of x_0.

(c) Let $f_{x_0} : B_2 \to B_1$ be the function having value 0 for all $x \neq x_0$ and having value 1 for $x = x_0$. It is known that a single use of I_{x_0} can be implemented with a single query to a quantum oracle for the function f_{x_0}. But suppose instead that we have a classical oracle for f_{x_0}, *i.e.* a black box which, on input x, outputs the value of $f_{x_0}(x)$. Can we determine x_0 with certainty using a single query to the classical oracle? Justify your answer.

Paper 3, Section I

10D Quantum Information and Computation

Let B_n denote the set of all n-bit strings. For any Boolean function on 2 bits $f : B_2 \to B_1$ consider the linear operation on 3 qubits defined by

$$U_f \,|\, x\rangle \,|\, y\rangle = |\, x\rangle \,|\, y \oplus f(x)\rangle$$

for all $x \in B_2$, $y \in B_1$ and $\oplus$ denoting addition of bits modulo 2. Here the first register is a 2-qubit register and the second is a 1-qubit register. We are able to apply only the 1-qubit Pauli X and Hadamard H gates to any desired qubits, as well as the 3-qubit gate U_f to any three qubits. We can also perform measurements in the computational basis.

(a) Describe how we can construct the state

$$|\, f\rangle = \frac{1}{2} \sum_{x \in B_2} (-1)^{f(x)} \,|\, x\rangle$$

starting from the standard 3-qubit state $|\, 0\rangle \,|\, 0\rangle \,|\, 0\rangle$.

(b) Suppose now that the gate U_f is given to us but f is not specified. However f is promised to be one of two following cases:

(i) f is a constant function (i.e. $f(x) = 0$ for all x, or $f(x) = 1$ for all x),

(ii) for any 2-bit string $x = b_1 b_2$ we have $f(b_1 b_2) = b_1 \oplus b_2$ (with $\oplus$ as above).

Show how we may determine with certainty which of the two cases (i) or (ii) applies, using only a *single* application of U_f.

Paper 2, Section I

10D Quantum Information and Computation

(a) The classical controlled-NOT operation applied to the 2-bit string $b0$ (for $b = 0$ or 1) achieves the cloning of b, i.e. the result is bb. Let CX denote the quantum controlled-X (or controlled-NOT) operation on two qubits. For which qubit states $|\, \psi\rangle = a\,|\, 0\rangle + b\,|\, 1\rangle$ will the application of CX to $|\, \psi\rangle \,|\, 0\rangle$ (with the first qubit being the control qubit) achieve the cloning of $|\, \psi\rangle$? Justify your answer.

(b) Let $|\, \alpha_0\rangle$ and $|\, \alpha_1\rangle$ be two distinct non-orthogonal quantum states. State and prove the quantum no-cloning theorem for unitary processes.

Paper 1, Section I

10D Quantum Information and Computation

(a) Define what it means for a 2-qubit state $|\psi\rangle_{AB}$ of a composite quantum system AB to be *entangled*.

Consider the 2-qubit state

$$|\alpha\rangle = \frac{1}{\sqrt{3}}\Big(2\,|00\rangle - H \otimes H\,|11\rangle\Big)$$

where H is the Hadamard gate. From the definition of entanglement, show that $|\alpha\rangle$ is an entangled state.

(b) Alice and Bob are distantly separated in space. Initially they each hold one qubit of the 2-qubit entangled state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\Big(\,|00\rangle + |11\rangle\Big).$$

They are able to perform local quantum operations (unitary gates and measurements) on quantum systems they hold. Alice wants to communicate two classical bits of information to Bob. Explain how she can achieve this (within their restricted operational resources) by sending him a single qubit.

Paper 2, Section II

15D Quantum Information and Computation

(a) Suppose that Alice and Bob are distantly separated in space and each has one qubit of the 2-qubit state $|\,\phi^+\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle)$. They also have the ability to perform local unitary quantum operations and local computational basis measurements, and to communicate only classically. Alice has a 1-qubit state $|\,\alpha\rangle$ (whose identity is unknown to her) which she wants to communicate to Bob. Show how this can be achieved using only the operational resources, listed above, that they have available.

Suppose now that a third party, called Charlie, joins Alice and Bob. They are all mutually distantly separated in space and each holds one qubit of the 3-qubit state

$$|\,\gamma\rangle = \frac{1}{\sqrt{2}}\big(\,|\,000\rangle + |\,111\rangle\,\big).$$

As previously with Alice and Bob, they are able to communicate with each other only classically, e.g. by telephone, and they can each also perform only local unitary operations and local computational basis measurements. Alice and Bob phone Charlie to say that they want to do some quantum teleportation and they need a shared $|\,\phi^+\rangle$ state (as defined above). Show how Charlie can grant them their wish (with certainty), given their joint possession of $|\,\gamma\rangle$ and using only their allowed operational resources. [*Hint: It may be useful to consider application of an appropriate Hadamard gate action.*]

(b) State the quantum no-signalling principle for a bipartite state $|\,\psi\rangle_{AB}$ of the composite system AB.

Suppose we are given an unknown one of the two states

$$|\,\phi^+\rangle_{AB} = \tfrac{1}{\sqrt{2}}\big(\,|\,00\rangle_{AB} + |\,11\rangle_{AB}\,\big),$$
$$|\,\phi^-\rangle_{AB} = \tfrac{1}{\sqrt{2}}\big(\,|\,00\rangle_{AB} - |\,11\rangle_{AB}\,\big),$$

and we wish to identify which state we have. Show that the minimum error probability for this state discrimination task is zero.

Suppose now that we have access only to qubit B of the received state. Show that we can now do no better in the state discrimination task than just making a random guess as to which state we have.

Paper 3, Section II

15D Quantum Information and Computation

In this question you may assume the following fact about the quantum Fourier transform QFT mod N: if $N = Ar$ and $0 \leqslant x_0 < r$, where $A, r, x_0 \in \mathbb{Z}$, then

$$QFT \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |\, x_0 + kr \rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \omega^{x_0 l A} \,|\, lA \rangle$$

where $\omega = e^{2\pi i/N}$.

(a) Let $\mathbb{Z}_N$ denote the integers modulo N. Let $f : \mathbb{Z}_N \to \mathbb{Z}$ be a periodic function with period r and with the property that f is one-to-one within each period. We have one instance of the quantum state

$$|\, f \rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |\, x \rangle \,|\, f(x) \rangle$$

and the ability to calculate the function f on at most two x values of our choice.

Describe a procedure that may be used to determine the period r with success probability $O(1/\log\log N)$. As a further requirement, at the end of the procedure we should know if it has been successful, or not, in outputting the correct period value. [You may assume that the number of integers less than N that are coprime to N is $O(N/\log\log N)$].

(b) Consider the function $f : \mathbb{Z}_{12} \to \mathbb{Z}_{10}$ defined by $f(x) = 3^x \mod 10$.

(i) Show that f is periodic and find the period.

(ii) Suppose we are given the state $|\, f \rangle = \frac{1}{\sqrt{12}} \sum_{x=0}^{11} |\, x \rangle \,|\, f(x) \rangle$ and we measure the second register. What are the possible resulting measurement values y and their probabilities?

(iii) Suppose the measurement result was $y = 3$. Find the resulting state $|\, \alpha \rangle$ of the first register after the measurement.

(iv) Suppose we measure the state $QFT \,|\, \alpha \rangle$ (with $|\, \alpha \rangle$ from part (iii)). What is the probability of each outcome $0 \leqslant c \leqslant 11$?