UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday 27 May, 2004 1.30 to 3.30

PAPER 53

INTRODUCTION TO QUANTUM COMPUTATION

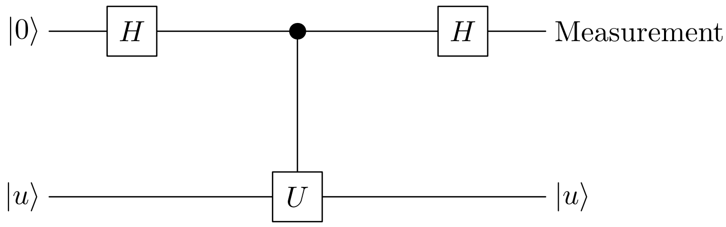
Attempt **THREE** *questions.*

There are **four** *questions in total.*

The questions carry equal weight.

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 Consider a quantum network represented by the following diagram:



Here the top horizontal line represents a qubit and the bottom one an auxiliary physical system, U is a unitary operation $U \in SU(N)$, and $|\,u\,\rangle$ is an eigenvector of U, such that $U|\,u\,\rangle = e^{i\phi}|\,u\,\rangle$. The measurement on the qubit can be performed either in the $\{|\,0\,\rangle, |\,1\,\rangle\}$ basis or in the conjugate basis $\{|+\rangle, |-\rangle\}$, $|\pm\rangle = (|\,0\,\rangle \pm i|\,1\,\rangle)/\sqrt{2}$.

1. What are the probabilities $P_0(\phi)$ and $P_1(\phi)$ that the qubit initially in state $|\,0\,\rangle$ will be found respectively in states $|\,0\,\rangle$ and $|\,1\,\rangle$ at the output if it is measured in the $\{|\,0\,\rangle, |\,1\,\rangle\}$ basis? What are the corresponding probabilities $P_+(\phi)$ and $P_-(\phi)$ if the qubit is measured in the $\{|+\rangle, |-\rangle\}$ basis? Suppose you do not know the eigenvalue of $|\,u\,\rangle$ but can run the above network many times and perform measurements in the $\{|\,0\,\rangle, |\,1\,\rangle\}$ and the $\{|+\rangle, |-\rangle\}$ bases. How would you estimate $\langle\, u\,|U|\,u\,\rangle$?

2 Instead of a pure state, $|\,u\,\rangle$, the auxiliary system is prepared in a more general state described by the density operator

$$\rho = p_1|u_1\rangle\langle u_1| + p_2|u_2\rangle\langle u_n| + \ldots + p_N|u_N\rangle\langle u_N|, \tag{1}$$

where $\{|\,u_k\,\rangle\}$ is an orthonormal set of eigenvectors of U with eigenvalues $e^{i\phi_k}$ and with probabilities $p_k \geqslant 0$ such that $\sum_k p_k = 1$. How would you estimate $\sum_{k=1}^{N} p_k e^{i\phi_k}$?

3. Explain how the network above can be used to estimate $\mathrm{Tr}U$.

2 The Fourier transform over the Abelian group $(\mathbb{Z}_2)^n$, also known as the Hadamard transform, is defined as

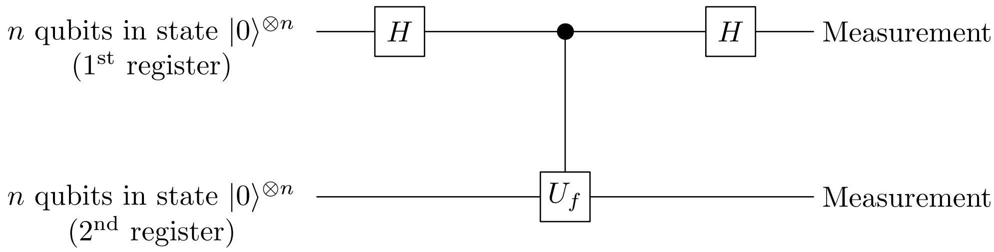
$$|\, x\,\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |\, y\,\rangle, \tag{2}$$

where $x, y \in \{0,1\}^n$ and the operation $x \cdot y$ is defined as

$$x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \pmod 2 \tag{3}$$

1. Sketch the quantum network which effects the Hadamard transform and explain why it is often useful as the first operation in quantum algorithms.

Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a 2-to-1 function such that $f(x+s) = f(x)$ for some $s \in \{0,1\}^n$. In the network below the H operations denote the Hadamard transform on n qubits and the U_f operation represents a quantum evaluation of f; $|\, x\,\rangle |\, y\,\rangle \mapsto |\, x\,\rangle |\, y + f(x)\,\rangle$.



2. What is the state of the two registers right after the quantum function evaluation?
3. The second register is measured bit by bit in the computational basis and a binary string $k \in \{0,1\}^n$ is registered. What is the state of the first register after the measurement?
4. Subsequently the Hadamard transform is performed on the first register, followed by a measurement in the computational basis. The result is a binary string, z. Show that $z \cdot s = 0$.

5. Suppose the function f is presented as an oracle. How many calls to the oracle are required in order to find s? How does it compare with a classical algorithm for the same problem?

3 A qubit in a pure state $|\,\Psi\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle$ is exposed to decoherence which can be described as

$$|\,0\rangle\,|\,R\rangle \longrightarrow |\,0\rangle\,|\,R_0\rangle\,, \tag{4}$$
$$|\,1\rangle\,|\,R\rangle \longrightarrow |\,1\rangle\,|\,R_1\rangle\,, \tag{5}$$

where $|\,R\,\rangle$, $|\,R_0\,\rangle$ and $|\,R_1\,\rangle$ are three normalized states of an environment.

1. Show that the density operator of the qubit evolves as,

$$|\Psi\rangle\langle\Psi| \mapsto (1-p)|\Psi\rangle\langle\Psi| + p\;\sigma_z|\Psi\rangle\langle\Psi|\sigma_z \tag{6}$$

and express p in terms of $\langle R_0|R_1\rangle$. This means that with the probability $1-p$ the qubit is not affected by environment and with the probability p the qubit undergoes the phase-flip error.

The trace norm of an operator X is defined as

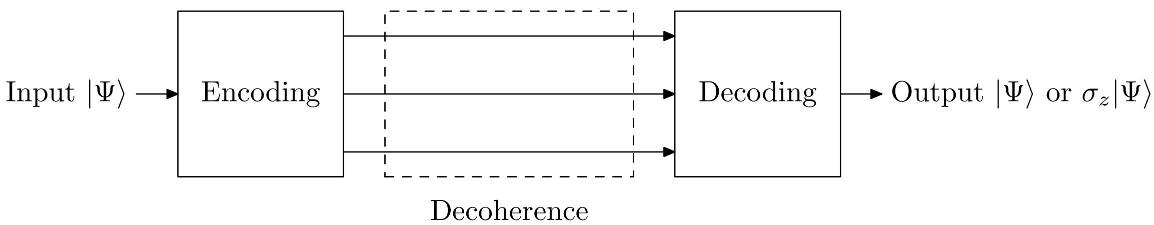
$$||X|| = \mathrm{Tr}\left(\sqrt{X^\dagger X}\right) \tag{7}$$

and the trace distance between two operators X and Y as

$$d(X,Y) = \frac{1}{2}||X-Y||\,. \tag{8}$$

2. What is the trace distance between the original state $|\Psi\rangle\langle\Psi|$ and this state after the decoherence?

Consider a quantum error correcting code which encodes a single qubit into three qubits and corrects for up to one phase-flip error. A qubit in state $|\,\Psi\,\rangle$ is encoded into a three qubit state which is then exposed to decoherence. Subsequently a decoding operation is performed which returns one qubit either in the original state $|\,\Psi\,\rangle$ or in $|\,\Psi\,\rangle$ modified by the phase-flip error.



The decoding operation can correct for up to one phase-flip error on any of the three qubits of the code.

3. What is the probability of successful recovery of the input state $|\,\psi\,\rangle$ and what is the density operator of the decoded qubit? How far, in terms of the trace distance, is the decoded qubit from the original state?

4 A quantum algorithm $\mathcal{A}$, which solves a certain problem in the complexity class NP, can be viewed as a unitary operation A on n qubits. The operator A acts in the 2^n dimensional Hilbert space spanned by the computational basis $|\, x \,\rangle$, such that x represents a binary string of length n, $x \in \{0,1\}^n$. Let $x = 0$ denote a string x of n zeros. The action $A|\, 0 \,\rangle$ prepares the state $|\, \Psi \,\rangle$ which is a superposition of binary strings representing possible, not necessarily correct, outputs. It is known that a subsequent measurement in the computational basis provides a correct answer to the problem with the probability $p \ll 1$ and that $|\, \Psi \,\rangle$ can be written as

$$|\, \Psi \,\rangle = \sqrt{p}\, |\, \Psi_g \,\rangle + \sqrt{1-p}\, |\, \Psi_b \,\rangle, \tag{9}$$

where $|\, \Psi_g \,\rangle$ is a projection of $|\, \Psi \,\rangle$ on the subspace spanned by the binary strings corresponding to good answers and $|\, \Psi_b \,\rangle$ is a projection of $|\, \Psi \,\rangle$ on the subspace spanned by the binary strings corresponding to bad answers. Both $|\, \Psi_g \,\rangle$ and $|\, \Psi_b \,\rangle$ are normalized.

1. How many applications of $\mathcal{A}$ followed by the measurement are required on average to obtain a correct answer.

Suppose you can construct V_0, such that $V_0|\, x \,\rangle = -|\, x \,\rangle$ if $x = 0$ and $V_0|\, x \,\rangle = |\, x \,\rangle$ otherwise, and another quantum operation V which verifies the output of $\mathcal{A}$, as follows

$$V|\, x \,\rangle = \begin{cases} -|\, x \,\rangle, & \text{when } x \in \{0,1\}^n \text{ is correct} \\ |\, x \,\rangle, & \text{when } x \in \{0,1\}^n \text{ is not correct} \end{cases} \tag{10}$$

Furthermore you can run $\mathcal{A}$ backwards, i.e. you can implement $A^\dagger$. Consider the operation

$$Q = -AV_0A^\dagger V \tag{11}$$

2. Show that the subspace spanned by $|\, \Psi_g \,\rangle$ and $|\, \Psi_b \,\rangle$ is invariant under the action of Q and express $Q|\, \Psi_g \,\rangle$ and $Q|\, \Psi_b \,\rangle$ as linear superpositions of $|\, \Psi_g \,\rangle$ and $|\, \Psi_b \,\rangle$.

3. Show that after r applications of operator Q to the state $|\, \Psi \,\rangle$ we obtain

$$Q^r|\, \Psi \,\rangle = \cos((2r+1)\theta)|\, \Psi_b \,\rangle + \sin((2r+1)\theta)|\, \Psi_g \,\rangle, \tag{12}$$

where $\sin^2\theta = p$.

4. How many times do you have to apply A or $A^\dagger$ before you can perform a measurement and obtain a correct answer with probability at least $1-p$?