UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 3 June 2003 9 to 11

PAPER 47

INTRODUCTION TO QUANTUM COMPUTATION

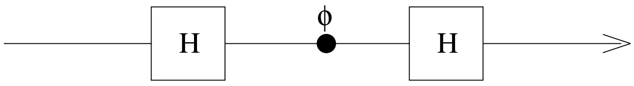
Attempt **THREE** *questions.*

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

The questions are of equal weight.

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

1 A quantum network which describes single qubit interference can be represented as follows:



(1) What is the probability $P_0(\phi)$ that a qubit initially in state $|\,0\,\rangle$ will be found in state $|\,0\,\rangle$ at the output if it is measured in the $\{|\,0\,\rangle, |\,1\,\rangle\}$ basis?

(2) Now suppose, that after the phase gate and before the second Hadamard gate, the qubit undergoes decoherence by interacting with an environment in state $|\,e\,\rangle$ so that:

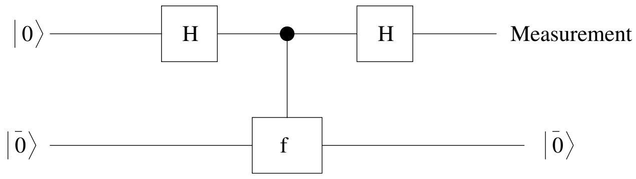
$$|\,0\,\rangle|\,e\,\rangle \mapsto |\,0\,\rangle|\,e_0\,\rangle, \tag{1}$$

$$|\,1\,\rangle|\,e\,\rangle \mapsto |\,1\,\rangle|\,e_1\,\rangle, \tag{2}$$

where $|\,e_0\,\rangle$ and $|\,e_1\,\rangle$ are the new states of the environment which are normalized but not necessarily orthogonal. The decoherence modifies $P_0(\phi)$ which becomes a function of ϕ and of the scalar product $\langle\,e_0\,|\,e_1\,\rangle$. Writing $\langle\,e_0\,|\,e_1\,\rangle = ve^{i\alpha}$ express P_0 as a function of ϕ, v, and α.

(3) Suppose the decoherence takes place between the first Hadamard gate and the phase gate, how different is the expression for $P_0(\phi, v, \alpha)$?

(4) Deutsch's algorithm with an oracle $f : \{0,1\} \mapsto \{0,1\}$, is implemented by the following network, where the central two-qubit gate is the oracle implementing the operation, $|\,x\,\rangle|\,y\,\rangle \mapsto |\,x\,\rangle|\,x \oplus f(y)\,\rangle$ and $|\,\bar{0}\,\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle - |\,1\,\rangle)$:



Assume that only the first (top) qubit is affected by decoherence as described by Eqs.(1) and (2). How reliably can you tell whether f is constant or balanced?

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

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

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

$$x \cdot y = x_1y_1 + x_2y_2 + \ldots + x_ny_n \,(\text{mod } 2)$$

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

(2) Suppose the Hadamard transform acts on n qubits in state

$$|\, \Psi_{IN}\,\rangle = \tfrac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x} |\, x\,\rangle,$$

where $a \in \{0,1\}^n$. What is the output state?

(3) Suppose you are given an oracle $f : \{0,1\}^n \mapsto \{0,1\}$ such that $f(x) = a \cdot x$ and the parameter $a \in \{0,1\}^n$ is unknown. Your task is to find a.

- How many calls to the oracle are needed in the classical case?
- Sketch a quantum network which outputs a and which calls the oracle only once.

3 Let A and B be two 2×2 matrices. The inner product of A and B is defined as $\frac{1}{2}\mathrm{Tr}\left(A^\dagger B\right)$. Show that the identity $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the bit flip $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, the phase flip $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and the bit and phase flip $\sigma_2 = i\sigma_1\sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ form an orthonormal basis in a space of 2×2 matrices, i.e. any 2×2 matrix E can be written as

$$E = \frac{1}{2}\sum_{k=0}^{3} \mathrm{Tr}\left(\sigma_k E\right)\ \sigma_k\,. \qquad (3)$$

Suppose error $\mathcal{E}$ entangles a qubit with its environment according to the rules

$$\begin{aligned} |\,0\,\rangle|\,e\,\rangle &\mapsto |\,0\,\rangle|\,e_{00}\,\rangle + |\,1\,\rangle|\,e_{01}\,\rangle \\ |\,1\,\rangle|\,e\,\rangle &\mapsto |\,0\,\rangle|\,e_{10}\,\rangle + |\,1\,\rangle|\,e_{11}\,\rangle, \end{aligned}$$

where $|\,e\,\rangle, |\,e_{nm}\,\rangle,\ n, m = 0, 1$ are the states of the environment which are not necessarily orthogonal or normalized. The r.h.s. of the two equations above can be conveniently written in the matrix form as

$$\begin{pmatrix} |\,e_{00}\,\rangle & |\,e_{01}\,\rangle \\ |\,e_{10}\,\rangle & |\,e_{11}\,\rangle \end{pmatrix} \begin{pmatrix} |\,0\,\rangle \\ |\,1\,\rangle \end{pmatrix}. \qquad (4)$$

Using Eq.(4) together with Eq.(3), or otherwise, show that for any pure state of the qubit $|\,\Psi\,\rangle$, the action of the error $\mathcal{E}$ can be represented as

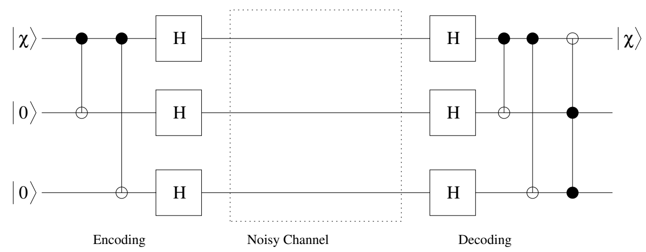
$$|\,\Psi\,\rangle|\,e\,\rangle \mapsto \sum_{k=0}^{3} \left(\sigma_k|\,\Psi\,\rangle\right)|\,e_k\,\rangle,$$

for some states of the environment $|\,e_k\,\rangle$ which are not necessarily orthonormal. Express $|\,e_k\,\rangle$ in terms of $|\,e_{mn}\,\rangle$.

Suppose we are given a noisy single qubit channel in which the probability of a phase flip error is q and no other errors occur. Consider an arrangement, shown in the diagram below, in which the qubit in some unknown state of the form $|\,\chi\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle$ is encoded into a three qubit state

$$\alpha|\,\bar{0}\,\rangle|\,\bar{0}\,\rangle|\,\bar{0}\,\rangle + \beta|\,\bar{1}\,\rangle|\,\bar{1}\,\rangle|\,\bar{1}\,\rangle,$$

where $|\,\bar{0}\,\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle)$ and $|\,\bar{1}\,\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle - |\,1\,\rangle)$. The three qubits are transmitted through the channel and subsequently decoded.



What is the probability of successful recovery of the input state $\alpha|\,0\,\rangle + \beta|\,1\,\rangle$?

4 The quantum Fourier transform on the group $\mathbb{Z}_N$ acts on a Hilbert space of dimension $N = 2^n$. It is defined by linearity and its action on an orthonormal basis, $\{|\,0\,\rangle, |\,1\,\rangle, |\,2\,\rangle, \ldots, |\,N-1\,\rangle\}$:

$$QF_n : \quad |\,x\,\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |\,y\,\rangle.$$

The single qubit unitary transformation R_k is defined as

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}.$$

(1) Show that QF_n can be implemented by a quantum network of size $O(n^2)$ built from Hadamard gates and controlled R_k gates for $k = 1, 2, \ldots, n$.

(2) If $U_1, U_2, ...U_m$ and $V_1, V_2, ...V_m$ are unitary operators with $||U_k - V_k|| < \epsilon$ for $k = 1, 2, \ldots, m$, show that

$$||U_1 U_2 ... U_m - V_1 V_2 ... V_m|| < m\epsilon,$$

where the operator norm is defined as, $||A||^2 = \sup_{||\psi||=1} \langle\,\psi\,|A^+ A|\,\psi\,\rangle$.

Suppose that an approximate QF_n network is built with approximate Hadamard and approximate controlled R_k gates which implement unitary operations G' that approximate the specified gate operators G in the sense that

$$||G' - G|| \leq \frac{1}{n^4}.$$

Show that the resulting network operation U_n satisfies

$$||U_n - QF_n|| = 0\left(\frac{1}{n^2}\right).$$

Comment briefly on the practical implications.