UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 5 June, 2009 9:00 am to 11:00 am

PAPER 51

QUANTUM COMPUTATION

*Attempt no more than **THREE** questions.*

*There are **FOUR** questions in total.*

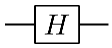
The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

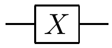
SPECIAL REQUIREMENTS
None

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

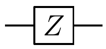
The following standard gate notation is used in this paper



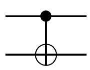
$$H = \frac{1}{\sqrt{2}}\big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \big)$$



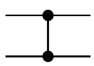
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$



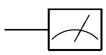
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$



$$C_X = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

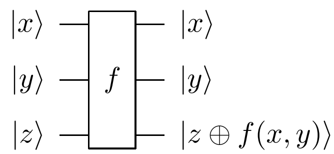


$$C_Z = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$



Computational basis measurement

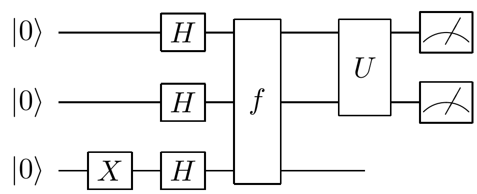
1 You are given a unitary oracle implementing an unknown function $f : \{0,1\}^2 \to \{0,1\}$, such that the computational basis states transform as



where $\oplus$ denotes addition modulo 2. We parameterize the possible functions by $a, b, c, d \in \{0,1\}$, writing

$$f_{abcd}(x, y) = axy \oplus bx \oplus cy \oplus d.$$

Consider inserting the oracle in the quantum circuit below, where U is a two-qubit unitary operation, and measurements are in the computational basis.



(**a**) Find the quantum state $|\psi_{abcd}\rangle$ of the three qubits just after the oracle, given that the oracle implements f_{abcd}.

(**b**) Consider the case in which $U = H \otimes H$. Show that this circuit can distinguish with certainty the oracles corresponding to the four functions f_{0001}, f_{0010}, f_{0100}, f_{0110}.

(**c**) Give a U such that the circuit can distinguish the oracles corresponding to f_{1000}, f_{1011}, f_{1101}, f_{1111} with certainty.

(**d**) Calculate $\langle\psi_{0000}|\psi_{1111}\rangle$. Hence, prove that there does not exist a U such that the circuit can distinguish the oracles corresponding to f_{0000} and f_{1111} with certainty.

(**e**) Suppose that instead of a quantum oracle, you are given a classical oracle (that acts on classical bits in the same way as the quantum oracle acts on computational basis states). Show that 3 oracle queries are required to distinguish the functions f_{0001}, f_{0010}, f_{0100}, f_{0110}.

2 Consider an oracle encoding a function $f : \{0,1\}^n \to \{0,1\}$, that gives a non-zero output only for a particular input a:

$$f(x) = \begin{cases} 1 & \text{if} \quad x = a \\ 0 & \text{if} \quad x \neq a \end{cases} .$$

We want to find a using Grover's search algorithm. However, we are also given the promise that a lies in a small subset A of all possible bit strings, $a \in A \subseteq \{0,1\}^n$, where A contains $|A|$ elements. Define the state $|\psi_A\rangle$ as the uniform superposition of all states in A:

$$|\psi_A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle .$$

(**a**) Consider the 2-dimensional subspace $\mathcal{V}$ spanned by $|a\rangle$ and $|\psi_A\rangle$. Find a vector $|\omega\rangle \in \mathcal{V}$ such that $|a\rangle$ and $|\omega\rangle$ form an orthonormal basis, and

$$|\psi_A\rangle = \sin(\theta) |a\rangle + \cos(\theta) |\omega\rangle$$

for $0 \leqslant \theta \leqslant \frac{\pi}{2}$. Find θ as a function of $|A|$.

(**b**) The Grover operation is $G = -V_{|\psi_A\rangle} V_{|a\rangle}$, where

$$V_{|\psi_A\rangle} = I - 2 |\psi_A\rangle \langle\psi_A| , \qquad V_{|a\rangle} = I - 2 |a\rangle \langle a| .$$

Show that when applied to states in $\mathcal{V}$, G acts as

$$G = \cos(2\theta) (|a\rangle \langle a| + |\omega\rangle \langle\omega|) + \sin(2\theta) (|a\rangle \langle\omega| - |\omega\rangle \langle a|) .$$

(**c**) It follows that $G^k |\psi_A\rangle = \sin((2k+1)\theta) |a\rangle + \cos((2k+1)\theta) |\omega\rangle$. Show that the minimal integer k such that a computational basis measurement on $G^k |\psi_A\rangle$ yields a with probability $\geqslant \cos^2(\theta)$ satisfies

$$k < \frac{\pi\sqrt{|A|}}{4}.$$

(**d**) Consider the case in which $|A| = 2^m$ for an integer $m = O(\log_2 n)$. Given that we can efficiently (i.e. with a circuit of size poly(n)) implement the unitary operation

$$U_{x,y} = I - |x\rangle \langle x| - |y\rangle \langle y| + |x\rangle \langle y| + |y\rangle \langle x| ,$$

where $|x\rangle$ and $|y\rangle$ are computational basis states of $n + m$ qubits, show that we can efficiently prepare $|\psi_A\rangle$.

3 Consider a family of single qubit phase measurements, parameterised by θ, that are characterised by the measurement operators

$$M_0(\theta) = |v_0(\theta)\rangle \langle v_0(\theta)|\,, \quad M_1(\theta) = |v_1(\theta)\rangle \langle v_1(\theta)|\,,$$

where

$$|v_0(\theta)\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right), \quad |v_1(\theta)\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i\theta}|1\rangle\right).$$

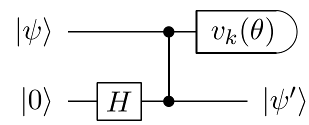
A phase measurement with angle θ that gives result k is denoted $v_k(\theta)$.

(**a**) Consider the single qubit unitary

$$U(\theta) = |0\rangle \langle v_0(\theta)| + |1\rangle \langle v_1(\theta)|\,.$$

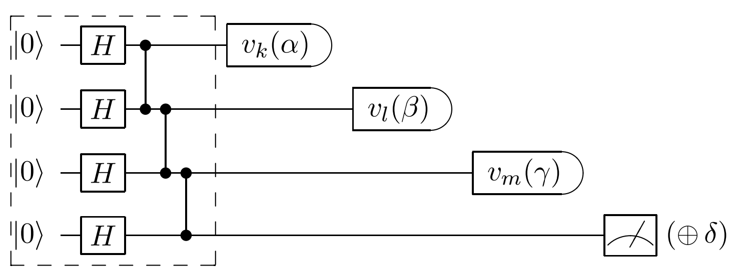
Prove the relations $U(\theta)Z = XU(\theta)$, and $U(\theta)X = e^{-i\theta}ZU(-\theta)$.

(**b**) Consider the following circuit, incorporating a C_Z gate:

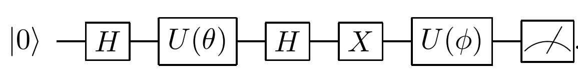


Show that $|\psi'\rangle = X^k U(\theta)|\psi\rangle$ and that the results $k = 0$ and $k = 1$ are equiprobable.

Consider the procedure below, which consists of preparing a four qubit graph state (the dashed section) then performing a sequence of measurements on it. The lowest qubit is measured in the computational basis, then $\delta \in \{0, 1\}$ is added to the outcome (modulo 2) to give the result r.



(**c**) Show that for an appropriate (adaptive) choice of α, β, γ and δ, the result r will perfectly simulate the measurement result in the circuit



(**d**) Show that when ϕ is an integer multiple of $\frac{\pi}{2}$, it is possible to simulate the circuit above by making all measurements on the graph state simultaneously (i.e. non-adaptively).

4 A qubit stored inside a quantum computer experiences decoherence. When it is stored for a time τ, its density operator ρ evolves according to the completely positive map $D_\epsilon(\rho)$ below, where $0 < \epsilon < \frac{1}{2}$.

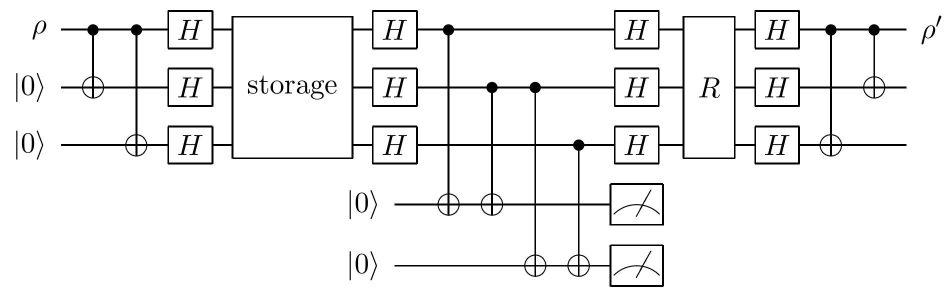
$$D_\epsilon(\rho) = (1 - \epsilon)\rho + \epsilon Z \rho Z.$$

(**a**) Show that when the qubit is stored for a time $n\tau$, where n is an integer, its evolution is described by $D_{\epsilon_n}(\rho)$, where

$$\epsilon_n = \frac{1}{2}\left(1 - (1 - 2\epsilon)^n\right).$$

(**b**) Find $\lim_{n\to\infty} D_{\epsilon_n}(\rho)$, and show that it corresponds to making a computational basis measurement on the qubit and ignoring the result.

To protect against decoherence, we can use an error-correction scheme such as the one pictured below.



(**c**) Suppose that during storage a Z gate is applied to k of the 3 qubits. Give recovery operations R dependent on the measurement results, such that $\rho' = \rho$ when k=0 or 1. What is ρ' when k=2 or 3?

(**d**) Suppose that each qubit experiences independent decoherence D_ϵ during storage. Given that R is as specified in the previous part, find ρ' in this case.

(**e**) The evolution $D_\epsilon(\rho)$ can be explained by the qubit inside the quantum computer interacting with a qubit in the environment via a controlled-Z gate. Show this by finding a state $|\psi_E\rangle$ such that

$$\mathrm{tr}_E\left(C_Z\left(\rho \otimes |\psi_E\rangle\langle\psi_E|\right) C_Z\right) = D_\epsilon(\rho),$$

where tr_E denotes the partial trace over the environment.

END OF PAPER