UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 3 June 2008 1.30 to 3.30

PAPER 57

INTRODUCTION TO QUANTUM COMPUTATION

Attempt no more than ***THREE*** *questions.*
There are ***FOUR*** *questions in total.*
The questions carry equal weight.

The following standard definitions hold throughout the paper

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} / \sqrt{2}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$cNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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.

1 In this question, we define the state $|\,\Psi_M^N\,\rangle$ to be a (normalized) state of N qubits which is the uniform superposition of all computational basis states containing M $|\,1\,\rangle$s and $(N-M)$ $|\,0\,\rangle$s. For example,

$$|\,\Psi_2^3\,\rangle \;=\; \frac{1}{\sqrt{3}}(|\,110\,\rangle + |\,101\,\rangle + |\,011\,\rangle).$$

It obeys the recursion relation

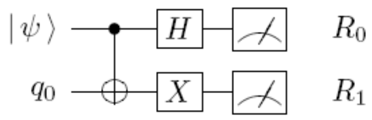
$$|\,\Psi_M^N\,\rangle \;=\; \sqrt{\frac{N-M}{N}}|\,0\,\rangle|\,\Psi_M^{N-1}\,\rangle \;+\; \sqrt{\frac{M}{N}}|\,1\,\rangle|\,\Psi_{M-1}^{N-1}\,\rangle,$$

where the qubit which has been singled out is an arbitrary choice.

Consider $N+1$ parties, labelled 0 to N, where N is odd. Each holds a single qubit from the state $|\,\Psi_{(N+1)/2}^{N+1}\,\rangle$. Party 0, Alice, also holds a single copy of an unknown pure 1-qubit state $|\,\psi\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle$ $(|\alpha|^2 + |\beta|^2 = 1)$, and wishes to transmit a copy of this state to all the other parties, without retaining a copy herself.

(a) Prove that Alice cannot achieve this perfectly if $N > 1$.

Alice performs the following teleportation-like protocol, replacing the Bell pair with the state $|\,\Psi_{(N+1)/2}^{N+1}\,\rangle$ in an effort to transmit $|\,\psi\,\rangle$ to Bob (party 1), and the others.



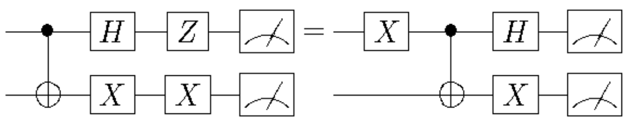
q_0 is the qubit in $|\,\Psi_{(N+1)/2}^{N+1}\,\rangle$ that Alice holds and measurement is in the computational $(|\,0\,\rangle/|\,1\,\rangle)$ basis. Assuming that both of Alice's measurement results are $|\,0\,\rangle$.

(b) What is the final state shared between all the parties $1 \ldots N$?

(c) What is the state ρ that Bob receives? Prove that it satisfies

$$\langle\,\psi\,|\rho|\,\psi\,\rangle \;=\; \frac{N+1+2|\alpha|^2|\beta|^2(N-1)}{2N}\,.$$

(d) In a teleportation protocol, the output state should be the same for all measurement outcomes following some corrective operations. Using the following circuit identity, or otherwise, what is the effective state that Alice teleported, and what correction should Bob and the other parties apply if Alice gets the measurement result $R_0 = 0$, $R_1 = 1$?



2 In Grover's Search Algorithm, the target is to find one of the $M \ll 2^N$ solutions $f(x) = 1$, where $f : \{0,1\}^N \mapsto \{0,1\}$. This is typically achieved by defining two unitary operators, each acting on N qubits,

$$U_f |\, x \,\rangle = \begin{cases} \ \ |\, x \,\rangle & f(x) = 0 \\ -|\, x \,\rangle & f(x) = 1 \end{cases}$$

$$V_y |\, x \,\rangle = \begin{cases} \ \ |\, x \,\rangle & x \neq y \\ -|\, x \,\rangle & x = y \end{cases},$$

and the algorithm proceeds to calculate

$$G^n |\, \phi \,\rangle$$

where $G = -H^{\otimes N} V_0 H^{\otimes N} U_f$ acts on the initial state $|\, \phi \,\rangle = H^{\otimes N} |\, 0 \,\rangle$.

(a) Express $|\, \phi \,\rangle$ in terms of the two states

$$|\, \Psi_g \,\rangle \ = \ \frac{1}{\sqrt{M}} \sum_{f(x)=1} |\, x \,\rangle$$

$$|\, \Psi_b \,\rangle \ = \ \frac{1}{\sqrt{2^N - M}} \sum_{f(x)=0} |\, x \,\rangle$$

and prove that G acts as a rotation on these states.

(b) Hence give the smallest number of repetitions, n, which guarantees that we have a probability of at least 50% of finding an x for which $f(x) = 1$.

(c) If, instead, we are provided with a V_y where $y \neq 0$ is known, what two states $|\, \tilde{\Psi}_g \,\rangle$ and $|\, \tilde{\Psi}_b \,\rangle$ are acted on in the same way by $-H^{\otimes N} V_y H^{\otimes N} U_f$ as $|\, \Psi_g \,\rangle$ and $|\, \Psi_b \,\rangle$ were by G?

(d) Hence, how should you change the input state such that the algorithm still functions?

3 In the following, you may assume that, for some set of real numbers J_n, the Hamiltonian

$$H_T = \sum_{n=0}^{N-1} J_n(|\, n\,\rangle\langle\, n+1\,| + |\, n+1\,\rangle\langle\, n\,|)$$

satisfies $e^{-iH_T\pi/2}|\, n\,\rangle = |\, N-n\,\rangle$ where $\langle\, n\,|\, m\,\rangle = \delta_{nm}$ (we take $\hbar = 1$).

Consider the Hamiltonian of $2N+1$ qubits (labelled 0 to $2N$)

$$H_e = \sum_{n=0}^{2N-1} \frac{K_n}{2}(X_n X_{n+1} + Y_n Y_{n+1}),$$

where $K_{2N-n-1} = K_n = J_{N-1-n}$ for $n = 0 \ldots N-2$, and $K_{N-1} = K_N = J_0/\sqrt{2}$. Define the notation $|\, \tilde{n}\,\rangle = X_{N+n}|\, 0\,\rangle^{\otimes 2N+1}$ to mean the state of $2N+1$ qubits where all are in the $|\, 0\,\rangle$ state except for the qubit $N+n$, which is in state $|\, 1\,\rangle$.

(a) Calculate the action of $\frac{1}{2}(X \otimes X + Y \otimes Y)$ on the four basis states $|\, 00\,\rangle$, $|\, 01\,\rangle$, $|\, 10\,\rangle$ and $|\, 11\,\rangle$.

(b) Calculate $H_e|\, \tilde{0}\,\rangle$ and $H_e^2|\, \tilde{0}\,\rangle$ and compare to $H_T|\, 0\,\rangle$ and $H_T^2|\, 0\,\rangle$.

(c) Hence, demonstrate a mapping from H_e, restricted to the subspace that governs the evolution of $|\, \tilde{0}\,\rangle$, into H_T. What is the output of $e^{-iH_e\pi/2}|\, \tilde{0}\,\rangle$, and what is the state when you trace out all qubits except for qubits 0 and $2N$?

(d) How might you modify the setup to produce an output state between 3 of the qubits of $(|\, 001\,\rangle + |\, 010\,\rangle + |\, 100\,\rangle)/\sqrt{3}$, starting from an initial product state? A suitable diagrammatic representation of your solution is acceptable.

4

(a) There is a one-qubit unitary gate V for which we wish to determine the eigenvalues. Assuming we are provided with gates controlled-V^{2^n} for $n = 0 \ldots N-1$, an eigenstate $|\, v_j\,\rangle$ of V which satisfies $V|\, v_j\,\rangle = e^{i\phi_j}|\, v_j\,\rangle$, and a supply of qubits in the state $(|\,0\,\rangle + |\,1\,\rangle)/\sqrt{2}$, show how to create the state

$$\frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} e^{i\phi_j x}|\, x\,\rangle,$$

justifying your answer.

(b) Using the inverse Quantum Fourier Transform,

$$U_{QFT}^{\dagger} = \frac{1}{\sqrt{2^N}} \sum_{x,y=0}^{2^N-1} e^{-i\frac{2\pi xy}{2^N}}|\, x\,\rangle\langle\, y\,|\,,$$

on the generated state, prove that the minimum probability with which we obtain the best N-bit approximation to $2^{N-1}\phi_j/\pi$ is lower bounded by

$$\frac{4}{\pi^2}.$$

(c) Instead of using $|\, v_j\,\rangle$, assume we use the maximally mixed state $\rho = (|\,0\,\rangle\langle\,0\,| + |\,1\,\rangle\langle\,1\,|)/2$. What are the possible outputs and their corresponding probabilities in this case?

(d) If, instead, you were just given the unitary V, and a supply of ancillas on which you can enact arbitrary single-qubit unitary rotations and measurements, how might you determine the eigenvalues of V? What are the advantages and disadvantages of this method in contrast to the previous one?

END OF PAPER