UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 6 June, 2006 1.30 to 3.30

PAPER 58

INTRODUCTION TO QUANTUM COMPUTATION

*Attempt **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.

1 A quantum register of n qubits is prepared in a state

$$|\psi_m\rangle = \tfrac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{i\phi_m l} |l\rangle,$$

where $N = 2^n$, l and $m = 0, 1, \ldots N-1$, and the phase $\phi_m = \left(\frac{2\pi}{N}\right) m$.

(a) Suppose the phase ϕ_m is unknown. Show that it can be revealed by applying the Quantum Fourier Transform

$$U = \tfrac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} e^{-2\pi i jk/N} |k\rangle\langle j|$$

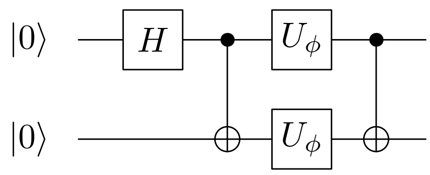
to the state $|\psi_m\rangle$ and measuring in the computational basis.

(b) For any m the state $|\psi_m\rangle$ is separable. Express it as a tensor product of quantum states of individual qubits. (You may wish to use the symbol $\bigotimes_{j=1}^{n}$ to denote the tensor product of n separate systems indexed by j.)

(c) Assume that you have a one-qubit phase gate U_ϕ that acts as follows,

$$U_\phi|0\rangle = |0\rangle,$$
$$U_\phi|1\rangle = e^{i\phi}|1\rangle.$$

Consider the circuit below. It is composed of one Hadamard gate followed by two U_ϕ gates sandwiched between the two control-NOT operations.



What is the quantum state of the two qubits at the output?

(d) Suppose you are given many identical copies of a U_ϕ gate and are promised that the phase ϕ takes one of the following values: 0, $\pi/4$, $\pi/2$, $3\pi/4$, π, $5\pi/4$, $3\pi/2$, $7\pi/4$. Assume that application of U_ϕ requires one time step and that the operations of all other quantum gates, including the Quantum Fourier Transform, take negligible time. Show how to obtain the value of ϕ in a single time step but with as many parallel applications of U_ϕ as needed.

2 Consider an ion trap quantum computer, or any other quantum computer, where $|0\rangle$ and $|1\rangle$ have different energies E_0 and E_1, and one-qubit gates are effected using light fields containing photons with energy (roughly) equal to $E_1 - E_0$. If the light field interacting with the qubit consists of exactly n photons, then a transition from $|1\rangle$ to $|0\rangle$ (photon emission) leaves $n+1$ photons in the light field and a transition from $|0\rangle$ to $|1\rangle$ (photon absorbtion) leaves $n-1$ photons in the light field; otherwise the number of photons is not affected. In general such interactions entangle the light field with the qubit, which may prevent any subsequent quantum interference in the qubit. However, for some states of the light field the effect of this entanglement is negligible.

Quantum states of laser light are well described by "coherent states", which are special superpositions of different numbers of photons. Here, for simplicity, we assume that the light field before the interaction with the qubit is in the state

$$|\Psi_k\rangle = \tfrac{1}{\sqrt{k}} \sum_{n=2}^{k+1} |n\rangle,$$

where $|n\rangle$ denotes the state with n identical photons.

Let H be the interaction between a pulse of the light field and the qubit that maps

$$|0\rangle|n\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle|n\rangle + |1\rangle|n-1\rangle),$$
$$|1\rangle|n\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle|n+1\rangle - |1\rangle|n\rangle).$$

(a) Suppose the qubit and light field start in the state $(\alpha|0\rangle + \beta|1\rangle)|\Psi_k\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$ and $\alpha, \beta \in \mathbb{C}$, and then they interact according to H. Compute the density matrix ρ which describes the final state of the qubit.

(b) The gate we would like to have implemented is the Hadamard gate, which converts

$$|0\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|1\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

and changes $\alpha|0\rangle + \beta|1\rangle$ into $|\psi_d\rangle$. We can evaluate the overlap with the desired state, $\langle\psi_d|\rho|\psi_d\rangle$, and find it to be

$$1 - \tfrac{1+(|\alpha|^2-|\beta|^2)(\alpha\beta^* + \alpha^*\beta)}{2k}.$$

When is the effect of the entanglement between the qubit and the light field negligible?

(c) Calculate the average overlap over all possible initial states of the qubit.

3 The Bloch Sphere is a convenient way of representing quantum states of a qubit and provides many insights into operations and measurements which can be performed on the qubit.

(a) Sketch the Bloch vectors corresponding to the states

$$|z(\theta,\varphi)\rangle = \cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle$$

and

$$|\bar{z}(\theta,\varphi)\rangle = \sin\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\cos\tfrac{\theta}{2}|1\rangle$$

for some values θ and φ of your choice ($0 < \theta < \pi/2$ and $0 \leqslant \varphi \leqslant 2\pi$).

(b) Show that for any two states $|u\rangle$ and $|v\rangle$ of a qubit,

$$|\langle u|v\rangle|^2 = \tfrac{1}{2}\left(1 + u\cdot v\right),$$

where $u\cdot v$ is the scalar product of the two Bloch vectors representing states $|u\rangle$ and $|v\rangle$.

(c) You are given a qubit which is prepared, with equal likelihood, either in the state $|z(\theta,\varphi)\rangle$ or $|\bar{z}(\theta,\varphi)\rangle$. In this particular case, the optimal identification method, which minimizes the probability of error, requires you to measure the qubit in the $|0\rangle/|1\rangle$ basis and to declare the state to be $|z\rangle$ if the result is 0, and $|\bar{z}\rangle$ if the result is 1. What is the probability of correctly identifying the state?

(d) What is the best way to distinguish between the states $|x(\theta,\varphi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ and $|\bar{x}(\theta,\varphi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i(\pi-\varphi)}\sin\frac{\theta}{2}|1\rangle$ and what is the probability of a correct identification?

(e) Alice has 3 classical bits of information, and Bob wants one of these, but Alice does not know which one. Having previously agreed on a protocol and a coordinate system with Bob, Alice is only allowed to send a single qubit to Bob. No additional communication (classical or quantum) is allowed between the parties, and they do not share any entanglement. How should Alice encode the information, and how should Bob extract the bit that he wants with maximum probability?

4 Imagine that we have a black box that accepts inputs $i \in \{0, 1, \ldots, N-1\}$ and outputs $f(i) \in \{0, 1\}$. Our aim is to find a value of i for which $f(i) = 1$. Let us assume there are m such values.

(a) The best classical strategy is to pick a random value of i and evaluate $f(i)$. If $f(i) = 1$, the sequence terminates. Otherwise, we pick another value of i and keep going. What is the probability that this algorithm terminates after exactly k steps, $1 \leqslant k \leqslant N - m$?

(b) If $m = 1$, by how much is the probability of success boosted after each guess?

We now define a quantum state

$$\begin{aligned}|\psi\rangle &= \tfrac{1}{\sqrt{N}} \left(\sum_{f(i)=0} |i\rangle + \sum_{f(i)=1} |i\rangle \right) \\ &\equiv |\psi_0\rangle + |\psi_1\rangle\end{aligned}$$

where the two terms $|\psi_1\rangle$ and $|\psi_0\rangle$ are not normalised.

(c) Let $\mathcal{A}$ be a reversible quantum algorithm that can be applied to $|\psi\rangle$. We introduce two operators, S_0^ϕ and S_f^θ which are defined as follows,

$$\begin{aligned} S_0^\phi |j\rangle &= \left\{ \begin{array}{c} e^{i\phi}|j\rangle, j = 0 \\ |j\rangle, j \neq 0 \end{array} \right) \\ S_f^\theta |j\rangle &= e^{if(j)\theta}|j\rangle. \end{aligned}$$

Calculate the action of $Q = -\mathcal{A} S_0^\phi \mathcal{A}^{-1} S_f^\theta$ on $|\psi_1\rangle$ and $|\psi_0\rangle$.

(d) Simplify this in the case that $\mathcal{A}|0\rangle = |\psi\rangle$ and $\langle\psi_1|\psi_1\rangle = \sin^2\chi$, expressing Q as a 2×2 unitary matrix.

(e) Given that $\sin^2\chi \ll 1$, how many applications of Q are required to find one of the good solutions ($f(i) = 1$) with probability $\geqslant \frac{1}{2}$? Take $e^{i\phi} = e^{i\theta} = -1$.

END OF PAPER