UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 3 June, 2011 1:30 pm to 3:30 pm

PAPER 49

QUANTUM COMPUTATION

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

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

The questions carry equal weight.

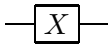
STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

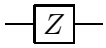
You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

The following standard gate notation is used in this paper. Note that I denotes the identity transformation throughout.

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



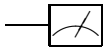
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$



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

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

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



Computational basis measurement

1

This question is about a quantum oracle problem and its query complexity.

If $\mathbf{a} = a_1 \ldots a_n$ and $\mathbf{x} = x_1 \ldots x_n$ are n-bit strings, the Hamming distance $h(\mathbf{a}, \mathbf{x})$ is defined to be the number of positions at which the bit strings $\mathbf{a}$ and $\mathbf{x}$ differ (so $0 \leqslant h(\mathbf{a}, \mathbf{x}) \leqslant n$).

Let $\mathbf{B}_n$ denote the set of all n-bit strings, and let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ denote the set of integers mod 4. For each $\mathbf{a} \in \mathbf{B}_n$ introduce the function $H_\mathbf{a} : \mathbf{B}_n \to \mathbb{Z}_4$ defined by

$$H_\mathbf{a}(\mathbf{x}) = h(\mathbf{a}, \mathbf{x}) \mod 4.$$

Also let M denote the 1-qubit gate defined in the computational basis by

$$M|a\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \mathbf{B}_1} i^{h(a,x)} |x\rangle \qquad \text{for } a \in \mathbf{B}_1 \quad (\text{where } i = \sqrt{-1}).$$

(**a**) Calculate $M|0\rangle$ and $M|1\rangle$. Hence (or otherwise) show that M is unitary.

(**b**) Show that for each $\mathbf{a} \in \mathbf{B}_n$

$$M \otimes \ldots \otimes M |\mathbf{a}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathbf{B}_n} i^{H_\mathbf{a}(\mathbf{x})} |\mathbf{x}\rangle .$$

Next, introduce the shift operation S defined by $S|y\rangle = |y + 1 \mod 4\rangle$ for $y \in \mathbb{Z}_4$, and introduce the state $|\alpha\rangle = \frac{1}{2}(|0\rangle - i|1\rangle - |2\rangle + i|3\rangle)$.

(**c**) Show that $|\alpha\rangle$ is an eigenstate of S and determine its eigenvalue.

Now consider the following oracle promise problem **HAM**:
Input: an oracle for a function $f : \mathbf{B}_n \to \mathbb{Z}_4$;
Promise: f is $H_\mathbf{a}$ for some n-bit string $\mathbf{a}$;
Problem: determine the n-bit string $\mathbf{a}$ with certainty.

For quantum computing, the oracle is given as the unitary operation U_f defined by

$$U_f |\mathbf{x}\rangle |y\rangle = |\mathbf{x}\rangle |y + f(\mathbf{x}) \mod 4\rangle \qquad \text{for } \mathbf{x} \in \mathbf{B}_n \text{ and } y \in \mathbb{Z}_4.$$

(**d**) Using the results of (b) and (c) above (or otherwise) show how **HAM** may be solved with only a single query to the oracle (together with further operations that do not depend on the oracle).
Draw a circuit diagram for your quantum algorithm.
(Hint: note that $U_f |\mathbf{x}\rangle |y\rangle = |\mathbf{x}\rangle S^{f(\mathbf{x})} |y\rangle$).

2

This question is about the quantum Fourier transform and periodicity determination.

In this question you may assume the following statements (S1) and (S2) about QFT, the quantum Fourier transform mod N:
(S1): if $N = Ar$ where A and r are integers and $0 \leqslant x_0 < r$ then

$$QFT \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + kr\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \omega^{x_0 l A} |lA\rangle \qquad \text{where } \omega = e^{2\pi i/N}.$$

(S2): QFT may be implemented in $\text{poly}(\log N)$ time.

(**a**) Let $\mathbb{Z}_N$ denote the integers mod N. Let $f : \mathbb{Z}_N \to \mathbb{Z}_N$ be a periodic function with period r and with the property that f is one-to-one within each period. Suppose we are given one instance of the quantum state

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle .$$

Using (S1) and (S2), describe an efficient procedure that may be used to determine the period r with probability $O(1/\log\log N)$. (You may also assume that the number of integers less than K that are coprime to K is $O(K/\log\log K)$).

(**b**) Consider the function $f : \mathbb{Z}_{12} \to \mathbb{Z}_{10}$ defined by $f(x) = 3^x \mod 10$.

(**i**) Suppose we are given the state $|f\rangle = \frac{1}{\sqrt{12}} \sum_{x=0}^{11} |x\rangle |f(x)\rangle$ and we measure the second register. What are the possible measurement values y and their probabilities?

(**ii**) Suppose the measurement result was $y = 3$. Find the resulting state $|\phi\rangle$ of the first register after the measurement.

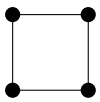
(**iii**) Suppose we measure the state $QFT |\phi\rangle$ (with $|\phi\rangle$ from (ii)). What is the probability of each outcome $0 \leqslant c \leqslant 11$?

3

This question is about measurement-based quantum computation.

Given a graph, the corresponding graph state is obtained by preparing a qubit in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ for every node in the graph, then applying a C_Z gate between every pair of qubits linked by an edge.

Consider the graph state $|\psi_{2\times 2}\rangle$ corresponding to the graph



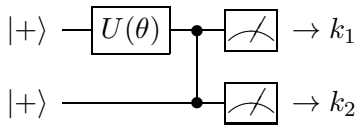
(**a**) Show that if one of the qubits is measured in the computational basis with result r, the remaining qubits will be left in the state $(Z^r \otimes I \otimes Z^r)|\psi_3\rangle$, where $|\psi_3\rangle$ is the graph state corresponding to the graph

(**b**) Next, the first qubit of the state $(Z^r \otimes I \otimes Z^r)|\psi_3\rangle$ is measured in the basis $\{|v_0(\theta)\rangle, |v_1(\theta)\rangle\}$, where $|v_s(\theta)\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^s e^{i\theta}|1\rangle\right)$, and result s is obtained. Show that the remaining qubits are left in the state

$$C_Z\left(X^{(r+s)}U(\theta) \otimes Z^r\right)|+\rangle|+\rangle,$$

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

(**c**) Using your previous answers, explain how you could simulate the results of the circuit



using single-qubit measurements on $|\psi_{2\times 2}\rangle$ and classical processing of the results.

(**d**) Suppose that you prepare a qubit in the state $|0\rangle$ for every node in a graph, and apply the same two-qubit gate V along every edge.

Find a V, and appropriate single-qubit measurements, which would allow you to perform universal quantum computation using such states.

4

This question is about error correction and fault-tolerance.

Suppose you are trying to build a quantum circuit, but the components you are using are prone to errors. Specifically, you know that in the circuit:

- Every single qubit gate or preparation of a qubit in the $|0\rangle$ state has probability ϵ of being followed by an X-error.
- Every C_X gate has probability ϵ of being followed by an X-error on the target qubit only. The control qubit is unaffected by errors.
- Every measurement of a qubit in the computational basis has probability ϵ of having its outcome bit flipped.

To protect against these errors you encode the logical state of a qubit using the bit-flip code $|0\rangle \to |0\rangle|0\rangle|0\rangle, |1\rangle \to |1\rangle|1\rangle|1\rangle$. In particular, to generate the encoded version of a $|0\rangle$ state, you prepare three qubits in the state $|0\rangle$.

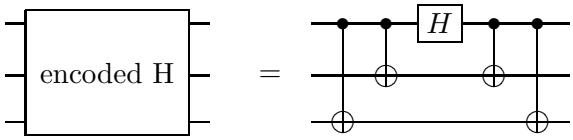
(**a**) Given the error model above, describe a fault-tolerant procedure for each of the following tasks:

(**i**) Performing an X gate on an encoded qubit.

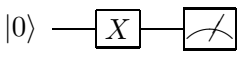
(**ii**) Performing a computational basis measurement on an encoded qubit.

(**iii**) Performing error-correction on an encoded qubit, which will recover the original state if it has suffered at most one X error.

(**b**) The circuit below will perform a Hadamard gate on an encoded qubit. Explain why it is not fault-tolerant.



(**c**) In order to simulate the simple circuit



using the procedures defined above, we replace each component by its encoded version followed by error correction (except that we do not perform error correction after the final measurement).

Show that the error probability for this encoded circuit will be less than that for the original circuit if ϵ is below some threshold.

END OF PAPER