Introduction to Molecular and Quantum Computation: Exercise Sheet 4

Dr Iain Styles

5 February 2008

1. Shor's Algorithm

For the following combinations of a, N, apply Shor's algorithm to find the factors of N. If the algorithm fails, clearly identify at which stage the failure occurs. Assume that each register has 15 qubits.

a) $N = 15$, $a = 7$
b) $N = 91$, $a = 4$
c) $N = 21$, $a = 5$

You should show **all** your working, including the states of the two registers after each calculation.

You may find the following information useful:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$7^x \mod 15$	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4	13	1
$4^x \mod 91$	1	4	16	64	74	23	1	4	16	64	74	23	1	4	16	64	74
$5^x \mod 21$	1	5	4	20	16	17	1	5	4	20	16	17	1	5	4	20	16

2. The Quantum Move Operation

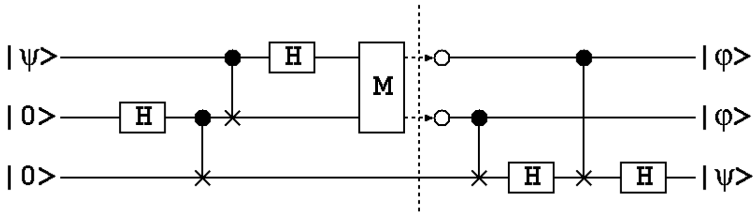
In lecture 5, we proved an important result: the no-cloning theorem which states that we cannot copy a general quantum state: we must know what the state is. Quantum teleportation relies on us being able to perform a general "quantum move" operation, which we write as $U|\psi\rangle|0\rangle = |0\rangle|\psi\rangle$: the operator U moves the state in the first regsiter into the second.

Show that if we can define U such that $U|\phi_1\rangle|0\rangle = |0\rangle|\phi_1\rangle$ and $U|\phi_2\rangle|0\rangle = |0\rangle|\phi_2\rangle$, then U will move a general state $|\alpha\rangle = a_1|\phi_1\rangle + a_2|\phi_2\rangle$.

Can you write down a matrix which does the quantum move operation on a two-qubit system?

3. A Teleportation Circuit

Consider the following quantum circuit:



In the lectures, we showed how the circuit to the left of the dotted line could be used by Alice to teleport a quantum state $|\psi\rangle$ to Bob. Show that the circuit to the right of the dotted line will convert the state Bob receives to the state Alice wanted to teleport, with the resulting state on the lowest qubit. You should assume that the box M simply measures the top two qubits, leaving them in the states corresponding to the measurements.

4. Grover's Algorithm

Perform two iterations of Grover's algorithm on a system with $N = 4$ and solution indexed by $x = 0$. The state you will need to start with is $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$. Comment on the result.

5. Some Experiments with Grover's Algorithm

Using the code provided, investigate the following:

1. The claim that the optimum number of iterations is $\frac{\pi}{4}\sqrt{N/M}$
2. What happens when there are multiple solutions? On measurement, are both solutions equally likely? Do all solutions emerge at the same rate?