Solutions to 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

Solutions:

Each of these questions starts in essentially the same way.

First of all, we start with the combined state $|0\rangle\,|0\rangle$. Fourier Transforming the first register gives us

$$\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle\,|0\rangle\,,$$

where $\omega = 2^{15}$. We now apply some transformation which calculate $f(x) = a^x \mod N$ and puts the result in the second register. For each of the three problems, the states are now:

a) $\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle\,|f(x)\rangle = \frac{1}{\sqrt{\omega}}\left[|0\rangle\,|1\rangle + |1\rangle\,|7\rangle + |2\rangle\,|4\rangle + |3\rangle\,|13\rangle + |4\rangle\,|1\rangle + \ldots\right]$

b) $\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle\,|f(x)\rangle = \frac{1}{\sqrt{\omega}}\left[|0\rangle\,|1\rangle + |1\rangle\,|4\rangle + |2\rangle\,|16\rangle + |3\rangle\,|64\rangle + |4\rangle\,|74\rangle + \ldots\right]$

c) $\frac{1}{\sqrt{\omega}}\sum_{x=0}^{\omega-1}|x\rangle\,|f(x)\rangle = \frac{1}{\sqrt{\omega}}\left[|0\rangle\,|1\rangle + |1\rangle\,|5\rangle + |2\rangle\,|4\rangle + |3\rangle\,|20\rangle + |4\rangle\,|16\rangle + \ldots\right]$

We now measure the second register. Let's say we measure

a) $f(x) = 4$
b) $f(x) = 16$

c) $f(x) = 5$

Then the state of the system collapses down into

a) $\frac{1}{\sqrt{v}} [|2\rangle + |6\rangle + |10\rangle + |14\rangle + \dots] |4\rangle$

b) $\frac{1}{\sqrt{v}} [|2\rangle + |8\rangle + |14\rangle + |20\rangle + \dots] |16\rangle$

c) $\frac{1}{\sqrt{v}} [|1\rangle + |7\rangle + |13\rangle + |19\rangle + \dots] |5\rangle$

It is then easy to deduce that the period of $f(x) = a^x \mod N$ in each of these cases is

a) $r = 4$
b) $r = 6$
c) $r = 6$

Note that this would be done in practice using a measurement of the first register, followed by an application of the continued fractions expansion. We do not cover this in detail in this course.

We now use this to deduce the factors of N in each case. First we note that r is even in every case, so we can continue. Then we must check that $a^{r/2} \mod N \neq -1 \mod N$:

a) $a^{r/2} \mod N = 7^2 \mod 15 = 4$; and $-1 \mod N = 14$
b) $a^{r/2} \mod N = 4^3 \mod 91 = 64$; and $-1 \mod N = 90$
c) $a^{r/2} \mod N = 5^3 \mod 21 = 20$; and $-1 \mod N = 20$

Shor's algorithm fails at this step for part (c). This can be resolved using slightly more complex computations which are beyond the scope of this course. For parts (a) and (b), we can continue. The next step is to compute the factors using $\gcd(a^{r/2} \pm 1, N)$. We find

a) $\gcd(a^{r/2} \pm 1, N) = \gcd(7^2 \pm 1, 15)$. For $+$, we have $\gcd(50, 15) = 5$, and for $-$, we have $\gcd(48, 15) = 3$. So $\boxed{15 = 3 \times 5}$.

b) $\gcd(a^{r/2} \pm 1, N) = \gcd(4^3 \pm 1, 91)$. For $+$, we have $\gcd(65, 91) = 13$, and for $-$, we have $\gcd(63, 91) = 7$. So $\boxed{91 = 13 \times 7}$.

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?

Solution:

We begin with $U |\phi_1\rangle |0\rangle = |0\rangle |\phi_1\rangle$ and $U |\phi_2\rangle |0\rangle = |0\rangle |\phi_2\rangle$. Then we apply U to the

general state $|\alpha\rangle = a_1 |\phi_1\rangle + a_2 |\phi_2\rangle$:

$$\begin{aligned} U|\alpha\rangle|0\rangle &= U(a_1|\phi_1\rangle + a_2|\phi_2\rangle)|0\rangle \\ &= a_1 U|\phi_1\rangle|0\rangle + a_2 U|\phi_2\rangle|0\rangle \\ &= a_1|0\rangle|\phi_1\rangle + a_2|0\rangle|\phi_2\rangle \\ &= |0\rangle(a_1|\phi_1\rangle + a_2|\phi_2\rangle) \\ &= |0\rangle|\alpha\rangle \end{aligned}$$

So the "quantum move" operator is quite general.

It turns out that we have already seen the operator for quantum move on two-qubit systems: in this special case it is the same as the two-qubit swap gate:

$$U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

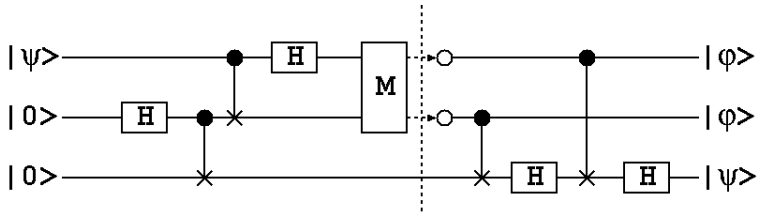
Then the composite state $(a_0|0\rangle + a_1|1\rangle)|0\rangle = a_0|00\rangle + a_1|10\rangle$ transforms under U_2 into

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ 0 \\ a_1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} = a_0|00\rangle + a_1|01\rangle = |0\rangle(a_0|0\rangle + a_1|1\rangle).$$

So U_2 moves a general quantum state from one qubit to another.

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. You should assume that the box M simply measures top two qubits, leaving them in the states corresponding to the measurements.

Solution

You should have had enough practice by now with quantum circuits to be able to find the matrix representing this circuit. It is quite straightforward to show that the transfor-

mation implemented by the circuit is

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

Now recall from the lecture how Bob must tranform the state of the third qubit depending on the state of the first two:

$$\begin{aligned} 00 &\mapsto I \\ 01 &\mapsto X \\ 10 &\mapsto Z \\ 11 &\mapsto ZX \end{aligned}$$

So if, for example, the measurement is 11, and Bob receives a qubit in state $-b\,|0\rangle + a\,|1\rangle$, then the state vector of the three qubits is $-b\,|110\rangle + a\,|111\rangle$. Applying the transformation matrix U to this gives

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -b \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ a \\ b \end{pmatrix} = a\,|110\rangle + b\,|111\rangle = |11\rangle \otimes (a\,|0\rangle + b\,|1\rangle)$$

So this does indeed implement the desired transformations. It is similarly easy to check the other case.

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.

Solution

1. Begin with the state $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$.
2. Apply the Oracle to the state, which flips the sign of $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}(-|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

3. Apply the QFT to this state. I think it's easiest to do this in matrix form, where we have

$$|\psi\rangle \mapsto F_2 |\psi\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \end{pmatrix}\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \equiv \frac{1}{2}\left(|0\rangle - |1\rangle - |2\rangle - |3\rangle\right)$$

4. Flip the signs of all terms except $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$
5. Apply the inverse QFT:

$$|\psi\rangle \mapsto F_2 |\psi\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv |0\rangle$$

So after one iteration, the state of the system is $|\psi\rangle = |0\rangle$, and so a measurement guarantees us the correct answer. What happens if we apply the second iteration?

1. Apply the Oracle: $|\psi\rangle \mapsto -|0\rangle$
2. Apply the QFT: $|\psi\rangle \mapsto \frac{1}{2}\left(-|0\rangle - |1\rangle - |2\rangle - |3\rangle\right)$
3. Flip the signs of all terms except $|0\rangle$: $|\psi\rangle \mapsto \frac{1}{2}\left(-|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$
4. Inverse QFT: $|\psi\rangle \mapsto \frac{1}{2}\left(|0\rangle - |1\rangle - |2\rangle - |3\rangle\right)$

So a measurement of the state no longer guarantees the correct result. This illustrates the importance of measuring the result of Grover's algorithm after the correct number of iterations.

5. Some Experiments

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?

Solution There are no hard and fast rules to observe here, but some observations that you should have made include:

- With a bit of error in each direction, the optimum number of iterations is indeed very close to $\frac{\pi}{4}\sqrt{N/M}$. You should be able to produce a graph which shows that this is true.

- When there are multiple solutions possible, both emerge at the same rate: the probability of each solution on measurement is the same for any number of iterations. So all solutions are equally likely. For example, if there are two solutions and we measure after the optimal number of iterations, the probability of measuring each of them is one half. This means that we can't get all the solutions to the problem in one go; we must run Grover's algorithm multiple times. If this system is big enough, this is still likely to be quicker than a classical algorithm, unless the number of repeats required is $O(\sqrt{N})$. This might occur if there are a large number of solutions.