School of Mathematics **Spring 2018**

QUANTUM COMPUTATION

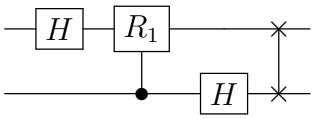
Exercise sheet 3

Ashley Montanaro, University of Bristol
ashley.montanaro@bristol.ac.uk

1. **The QFT and periodicity.**

   (a) Write down the circuit for the quantum Fourier transform Q_4 on 2 qubits. Multiply out the matrices corresponding to the circuit in the computational basis and check that the result is what you expect.

   Answer: The circuit, including the final SWAP gate, is



   and the corresponding matrix is

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

   as claimed in the lecture notes. Note that it would also be reasonable to omit the final SWAP gate and label the output qubits in the reverse order to the input qubits. In that case, two of the rows / columns of the matrix would need to be swapped.

   (b) Write the state $Q_4|3\rangle$ as a tensor product of two single-qubit states, each of the form $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i z}|1\rangle\right)$ for some binary fraction z (i.e. something of the form $(.x_{j-1}\ldots x_0)$). Expand out the resulting state and check that the answer is what you expect.

   Answer: For any $x \in \mathbb{Z}_4$, we can write

$$Q_N|x\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(.x_0)}|1\rangle\right)\right)\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(.x_1x_0)}|1\rangle\right)\right).$$

   The binary digits of 3 are $(1,1)$. So

$$\begin{aligned} Q_N|3\rangle &= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(.1)}|1\rangle\right)\right)\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(.11)}|1\rangle\right)\right) \\ &= \left(\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right)\left(\frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)\right) \\ &= \frac{1}{2}\left(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle\right) \end{aligned}$$

which is as expected.

(c) Let $f : \mathbb{Z}_{16} \to \mathbb{Z}_4$ be the periodic function such that $f(0) = 2$, $f(1) = 1$, $f(2) = 3$, $f(3) = 0$, and $f(x) = f(x-4)$ for all x (so $f(4) = 2$, etc.).

i. Work through all the steps of the periodicity determination algorithm, writing down the state at each stage, and assuming that the measurement outcome in step 3 is 1, and the measurement outcome in step 5 is 12. Does the algorithm succeed?

Answer: Initially, we have

$$|0\rangle|0\rangle \mapsto \frac{1}{4}\sum_{x=0}^{15}|x\rangle|0\rangle \mapsto \frac{1}{4}\sum_{x=0}^{15}|x\rangle|f(x)\rangle.$$

When we see outcome 1 in step 3, the state of the first register collapses to

$$\frac{1}{2}(|1\rangle + |5\rangle + |9\rangle + |13\rangle) = \frac{1}{2}\sum_{j=0}^{3}|1+4j\rangle.$$

Using the general expression given in the lecture notes (p19) for the result of applying the QFT to a state of this form, after step 4 we have a state

$$\begin{aligned}\frac{1}{8}\sum_{j=0}^{3}\left(\sum_{y=0}^{15}\omega_{16}^{y(1+4j)}|y\rangle\right) &= \frac{1}{8}\sum_{y=0}^{15}\omega_{16}^{y}\left(\sum_{j=0}^{3}\omega_{16}^{4jy}\right)|y\rangle \\ &= \frac{1}{2}\sum_{\ell=0}^{3}\omega_{16}^{4\ell}|4\ell\rangle \\ &= \frac{1}{2}(|0\rangle + i|4\rangle - |8\rangle + i|12\rangle).\end{aligned}$$

This could also be shown by direct calculation. If we receive measurement outcome 12 in step 5, we simplify the fraction 12/16 to 3/4 and return 4. This is correct, so the algorithm succeeds.

ii. Now assume that the measurement outcome in step 5 is 8. Does the algorithm succeed?

Answer: Now we simplify the fraction 8/16 to 1/2 and return 2. This is incorrect, so the algorithm fails.

2. **Shor's algorithm.**

(a) Suppose we would like to factorise $N = 85$ and we choose $a = 3$, which is coprime to N. Follow steps 3-5 of the integer factorisation algorithm to factorise 85 using

this value of a (calculating the order of a classically!). You might like to use a computer.

Answer: The order of a is 16, which is even, so the check in step 3 succeeds. $3^{16/2} - 1 = 6560$, and the greatest common divisor of 6560 and 85 is 5. So the algorithm outputs 5, which is indeed a factor of 85.

(b) Imagine we want to factorise $N = 21$ and we choose $a = 4$. Does the integer factorisation algorithm work or not?

Answer: 4 and 21 are coprime, so the check in step 2 of the algorithm succeeds. The order of a is 3, as demonstrated by $4^3 = 64 \equiv 1 \bmod 21$. So it might seem that the algorithm has failed. However, because 4 is even, we can still write

$$4^3 - 1 = (4^{3/2} + 1)(4^{3/2} - 1) \equiv 0 \bmod 21.$$

The greatest common divisor of $4^{3/2} - 1 = 7$ and 21 is 7, which is indeed a factor of 21.

3. **Approximate implementation of the QFT (optional).** This part proves a claim made at the end of Section 4 of the lecture notes. Define the distance $D(U, V)$ between unitary operators U and V as the maximum over all states $|\psi\rangle$ of $\|U|\psi\rangle - V|\psi\rangle\|$.

(a) Show that $D(\cdot, \cdot)$ is subadditive: $D(U_1U_2, V_1V_2) \leq D(U_1, V_1) + D(U_2, V_2)$.

Answer: For any $|\psi\rangle$,

$$\begin{aligned} \|U_1U_2|\psi\rangle - V_1V_2|\psi\rangle\| &= \|(U_1U_2 - V_1V_2)|\psi\rangle\| \\ &= \|(U_1U_2 - V_1U_2 + V_1U_2 - V_1V_2)|\psi\rangle\| \\ &\leq \|(U_1U_2 - V_1U_2)|\psi\rangle\| + \|(V_1U_2 - V_1V_2)|\psi\rangle\| \\ &= \|(U_1 - V_1)U_2|\psi\rangle\| + \|V_1(U_2 - V_2)|\psi\rangle\| \\ &\leq D(U_1, V_1) + D(U_2, V_2), \end{aligned}$$

where the first inequality is the triangle inequality and the second uses that V_1 is unitary, and hence does not change the ℓ_2 norm.

(b) Show that $D(R_d, I) = O(2^{-d})$ and argue that the same holds for controlled-R_d.

Answer: We have

$$D(R_d, I) = \max_{|\psi\rangle} \|(R_d - I)|\psi\rangle\| = |e^{\pi i/2^d} - 1|$$

by the definition of $D(\cdot, \cdot)$ and R_d. Using the Taylor series for e^x or that $|e^{i\theta} - 1| = |e^{i\theta/2} - e^{-i\theta/2}| = 2|\sin(\theta/2)|$, it follows that this expression is upper-bounded by $O(2^{-d})$. The same argument holds for controlled-R_d, as this acts in the same way as R_d on a subspace of $\mathbb{C}^{2^n}$, and as the identity elsewhere.

(c) Describe how to produce a quantum circuit for an operator $\widetilde{Q}_{2^n}$ on n qubits such that $\widetilde{Q}_{2^n}$ uses $O(n \log n)$ gates and $D(\widetilde{Q}_{2^n}, Q_{2^n}) = O(1/n)$.

Answer: We start with the standard circuit for Q_{2^n}, and remove all controlled-R_d gates such that $d \geq \ell$, for some ℓ to be determined. By the previous two parts, removing a controlled-R_d gate from Q_{2^n} gives a circuit Q'_{2^n} such that $D(Q'_{2^n}, Q_{2^n}) = O(2^{-d})$, and this procedure can be repeated. Each controlled-R_d gate appears at most n times in the circuit, so removing all controlled-R_d gates for $d \geq \ell$ gives a new circuit $\widetilde{Q}_{2^n}$ such that

$$D(\widetilde{Q}_{2^n}, Q_{2^n}) \leq n \sum_{d=\ell}^{n-1} O(2^{-d}) = O(n2^{-\ell}).$$

So taking $\ell = O(\log n)$ is sufficient to achieve $D(\widetilde{Q}_{2^n}, Q_{2^n}) = O(1/n)$. The resulting circuit has $O(n \log n)$ gates.