Quantum Computing: Exercise Sheet 3

Steven Herbert and Anuj Dawar

1. Express controlled-R_n and controlled-$R_n^\dagger$, as defined in lecture 9, in matrix form – and show that the latter is indeed the inverse of the former.

2. (a) What is the state after the controlled-unitary stage of the QPE algorithm estimating the phase of unitary $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$, with three qubits in the first register, and the second register initialised in the state $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$?
   (b) What will the measurement outcomes be after the inverse QFT stage of the QPE algorithm?

3. Show that permutation matrices are unitary.

4. This question concerns using Shor's algorithm to factor the number 21.
   (a) Step through Shor's algorithm on Slide 8 of lecture 10 with $N = 21$. Verify that 21 is neither even nor a prime power, and then use $x = 10$ for step 3 – find the order of $10 \mod 21$ and use this to factor 21.
   (b) Say we were to run Shor's algorithm in full with $x = 10$, and were to measure the phase corresponding to the eigenvector u_1 (as defined on Slide 14), express this eigenvector (in full, not as abbreviated by a sum) and its eigenvalue.

5. What would happen if we could only approximately prepare the state $|1\rangle$ as the input to the second register in Shor's algorithm?

6. (a) Show that, as claimed in lecture 11:
$$e^{-i(\mathrm{H}_1+\mathrm{H}_2)\Delta t} = e^{-i\mathrm{H}_1\Delta t}e^{-i\mathrm{H}_2\Delta t} + \mathcal{O}(\Delta t^2)$$
   (b) Show that we can obtain a more accurate simulation if, to estimate $e^{-i(\mathrm{H}_1+\mathrm{H}_2)\Delta t}$, we instead use:
$$e^{-i\mathrm{H}_1\Delta t/2}e^{-i\mathrm{H}_2\Delta t}e^{-i\mathrm{H}_1\Delta t/2}$$

7. If we are performing quantum chemistry on a n-qubit Hamiltonian, and we prepare the input to the second register as a uniform superposition of all eigenvectors, what is the probability that QPE gives us the ground-state phase?

8. The matrices defining probabilistic automata, as defined on Slide 7 of lecture 12, have the property that the entries in each column add up to 1. Prove that this property is preserved under matrix multiplication.

9. (a) What is the language accepted by the quantum automaton described on Slide 8 of lecture 12?

(b) Prove that there is no two-state probabilistic automaton with this behaviour.

(c) Describe a probabilistic automaton (with more than two states) that exhibits this behaviour.

10. Consider a quantum finite automaton with two basis states, $|0\rangle$ being the start state and $|1\rangle$ the only accepting state. The automaton operates on a two letter alphabet, with matrices:

$$M_a = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad ; \quad M_b = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Give a complete description of the probabilities of acceptance associated with various possible input strings.

11. Suppose M is a quantum Turing machine that accepts a language L in the bounded probability sense: for each string $w \in L$, there is a probability $> \frac{2}{3}$ that M is observed in an accepting state after reading w and for each string $w \notin L$, there is a probability $< \frac{1}{3}$ that M is observed in an accepting state after reading w. We define a new machine M_0 that, on input w makes three independent runs of M on input w and decides acceptance by majority. What is the probability that M_0 accepts $w \in L$? What about $w \notin L$?

12. (**Optional**) It can be proven that entanglement is necessary for exponential speed-ups. Give a sketch of a proof of this, by showing that an initial product state, which undergoes a circuit consisting of gates which always output a product state when a product state is input, can be simulated on a classical computer with only a polynomial overhead in the number of computations.