Quantum Computing: Exercise Sheet 2

Anuj Dawar

February 22, 2007

Quantum Information Applications

1. Verify that the four states on slide 11 form an orthonormal basis for $\mathbb{C}^4$. Let $|h_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|h_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Write the four Bell states in the basis $|h_0h_0\rangle, |h_0h_1\rangle, |h_1h_0\rangle, |h_1h_1\rangle$.

2. Write the unitary operator depicted in the circuit on slide 12 in matrix form. Do the same for the circuit on slide 15. Verify that the two matrices are inverses of each other.

3. Suppose that Eve intercepts the qubit transmitted by Alice in the superdense coding protocol. Can she infer which of the four pairs of bits $00, 01, 10$, or 11 Alice was trying to transmit? If so, how? If not, why not?

4. Verify the four identities on slide 18 for an arbitrary $|\theta\rangle = \alpha|0\rangle + \beta|1\rangle$.

Quantum Searching

5. The purpose of this exercise is to verify the claim on slide 9, that the $cZ^{\otimes n}$ operator can be implemented using the cZ gate and Toffoli gates. Show that you can implement such a circuit which takes n input bits, along with $n-2$ work bits, which may be assumed to be all in the state $|0\rangle$ and the result of which is to apply $cZ^{\otimes n}$ to the n input bits and restore the work bits to the state $|0\rangle$. (Hint: Use Toffoli gates to form the *And* of $n-1$ of the bits on the workbits and use this as a control for a cZ gate.)

6. Suppose a search problem has M solutions out of N possibilities. We refer to the solutions as "marked states". Let $|\alpha\rangle$ be an equal superposition of all unmarked states, and let $|\beta\rangle$ be an equal superposition of all marked states. Let $\sin\theta = \sqrt{M/N}$.

   (a) Show that the superposition of all computational basis states, $|\Psi\rangle$ can be written as

   $$|\Psi\rangle = \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle.$$

   (b) Show that in the $|\alpha\rangle, |\beta\rangle$ basis, we can write the Grover iterate as

   $$G = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}.$$

(c) Hence, determine the eigenvalues of G in terms of θ.

7. Suppose we apply Grover's algorithm to a 4 qubit register, assuming exactly one of the states is marked. What is the probability of measuring the marked state after applying the Grover iterate 0,1,2,3 times? Note, 4 is too small a value for the approximation $\theta \sim \sin\theta$ to work.

Quantum Factoring

8. Find the period of the function $f(x) = 10^x \pmod{21}$. Use this to factor 21.

9. **Discrete Fourier Transform**

   (a) Verify that the matrix on slide 9 correctly implements the discrete Fourier transform as described on slide 8.

   (b) (The exercise on slide 10). Verify that the D as given on slide 9 is unitary, and the matrix on slide 10 is the inverse of D.

   (c) What is the matrix representation of the quantum Fourier transform acting on one qubit?

10. (The exercise on slide 12). Verify the formula given on slide 12 for the quantum Fourier transform of a basis state described by a binary string $x_1 \cdots x_n$.

11. Verify that the circuit described on slide 13 implements the transform as described on slide 12.

12. Consider the probability of measuring a state $|y\rangle$ calculated on slide 18.

    - Taking $n = 5$ and $r = 6$, calculate the probability of measuring the states $y = 1$ and $y = 5$.
    - Show that if $2^n/r$ is an integer, there are r distinct states $|y\rangle$ for which $yr/2^n$ is an integer. Show that the probability that a measurement will yield one of these states is 1.

Automata and Complexity

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

14. Prove that there is no *two-state* probabilistic automaton with the behaviour described at the bottom of slide 12: i.e. it accepts odd length strings with probability 0.5, strings of length $2 \pmod 4$ with probability 1 and strings of length $0 \pmod 4$ with probability 0. Describe a probabilistic automaton that exhibits this behaviour.

15. 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 $M_a = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$ and $M_b = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Give a complete description of the probabilities of acceptance associated with various possible input strings.

16. **Probability amplification** 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' that, on input w makes three independent runs of M on input w and decides acceptance by majority. What is the probability that M' accepts $w \in L$? What about $w \notin L$?