Quantum Computing: Exercise Sheet 2

Anuj Dawar and Ben Travaglione

February 2, 2004

Grover's Algorithm

1. Suppose a search problem has M solutions out of N possibilities. Let $|\alpha\rangle$ be an equal superposition of all unmarked states, and let $|\beta\rangle$ be an equal superposition of all marked states. Let $\sin\theta/2 = \sqrt{M/N}$.

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

   $$|\psi\rangle = \cos\theta/2|\alpha\rangle + \sin\theta/2|\beta\rangle.$$

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

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

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

2. (The exercise on slide 25). 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?

Shor's Algorithm

3. **Discrete Fourier Transform**

   (a) Verify the formula for x_j on slide 8.

   (b) Verify the formula for y_j on slide 10.

4. What is the matrix representation of the QFT acting on one qubit?

5. Determine the eigenvalues and eigenvectors of the NOT gate.

6. Verify that the phase-estimation algorithm, with one index qubit will return the eigenvalue of the NOT gate if it takes as input either eigenvector.

7. (The exercise on slide 35). Using the reduction of factoring to order-finding, and the fact that 10 is co-prime to 21, factor 21.

8. (The exercise on slide 39). Show $|1\rangle = \sum_{k=1}^{r} |\psi_k\rangle$ where

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{\frac{-2\pi ikj}{r}} |a^j \mathrm{mod} N\rangle.$$

Implementations

9. Write down the density matrix for an arbitrary single qubit state.

10. Any arbitrary density matrix can always be written as a convex combination of normalized pure states. What is the trace of an arbitrary density matrix?

11. Briefly describe one of the possible schemes for implementing a quantum computer.

12. What are some of the problems associated with the scheme you described in the previous question?

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 rejects odd length strings with probability 0.5, accepts strings of length 2(mod 4) with probability 1 and strings of length 0(mod4) with probability 0. What is the smallest 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 $w \notin L$?