Quantum Computing: An Applied Approach

Chapter 9 Problems: Quantum Computing Methods

1. This problem guides you through how expectation values of single qubit operators can be computed on a quantum computer.

   (a) Let $|\psi\rangle$ be the state of a qubit. From Born's rule, show that the probability of measuring the zero state is $p(0) = |\langle 0|\psi\rangle|^2$.

   (b) Similar to above, what is the probability of measuring the one state, $p(1)$?

   (c) Define the projectors $\Pi_0 = |0\rangle\langle 0|$ and $\Pi_1 = |1\rangle\langle 1|$. Show that $p(0) = \langle\psi|\Pi_0|\psi\rangle$ and $p(1) = \langle\psi|\Pi_1|\psi\rangle$.

   (d) Prove that $Z = \Pi_0 - \Pi_1$.

   (e) Prove that $\langle\psi|Z|\psi\rangle = p(0) - p(1)$. Thus, by measuring in the Z-basis (many times), we can estimate the expectation of Pauli Z by subtracting the frequency of the outcomes.

   (f) Suppose now we wanted to measure $\langle\psi|X|\psi\rangle$. Show that this can be done with the above steps by adding a Hadamard gate before measuring in the computational basis. *Hint*: $HZH = X$.

   (g) The same idea above can be applied to measuring $\langle\psi|Y|\psi\rangle$. What gate(s) should be added before measuring in the computational basis to achieve this?

2. Problem 1 demonstrates how we can measure single qubit expectation values. Consider the qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha = 3/5$ and $\beta = 4/5$.

(a) Compute analytically $\langle X \rangle$, $\langle Y \rangle$, and $\langle Z \rangle$ where angled brackets denote expectation value in ψ.

(b) Design a quantum circuit to prepare the state $|\psi\rangle$.

(c) Design a quantum circuit to estimate $\langle X \rangle$. How does the accuracy improve as you increase the number of repetitions of the circuit?

(d) Do the above for Y and Z.

3. For Hamiltonians on multiple qubits, we will have to measure expectation values of operators such as $X \otimes Z$ or $Y \otimes Y \otimes Z$. These are known as *generalized Pauli operators*.

   (a) Consider for simplicity the generalized Pauli operator $X \otimes Z$. We know how to compute the expectation value of each term via the technique in Problem 1. Show that we can compute $\langle X \otimes Z \rangle$ by implementing $H \otimes I$ then measuring in the Z basis, and computing

$$p(00) - p(01) - p(10) + p(11) \tag{1}$$

   where $p(00)$ is the probability of measuring bitstring 00, etc.

   (b) Prove that generalized Pauli operators form a basis for all unitaries. Combined with problems 1-3, this shows that we can estimate expectation values of any unitary matrix (although we may not be able to do so efficiently).

   (c) Express the following single-qubit unitaries as a sum of Pauli operators.

      i. H.

      ii. S.

      iii. T.

      iv. $R_Y(\theta)$ for $\theta = \pi/4$.

4. Suppose we wish to use quantum phase estimation (QPE) to estimate an eigenvalue of a unitary U, and that controlled-U can be implemented in a circuit with u gates. If we use n qubits of precision, how many total gates are required in the circuit? Make a plot of the number of gates for, say, $1 \leq n \leq 10$.

5. *Iterative quantum phase estimation* (IQPE) is a modification of the phase estimation algorithm to use fewer resources. In phase estimation, we use a *single* circuit with n qubits of precision to estimate an eigenvalue using n bits. In *iterative* quantum phase estimation, we use n circuits with *one* qubit of precision to estimate an eigenvalue using n bits.

For the following three parts, let U be a unitary on m qubits, and let

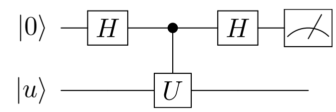
$$U|u\rangle = e^{2\pi i\phi}|u\rangle. \tag{2}$$

Further, suppose that ϕ has the binary decimal expansion

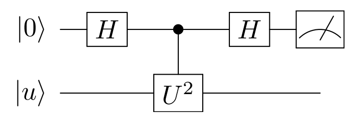
$$\phi = 0.\phi_1\phi_2\cdots\phi_n, \tag{3}$$

i.e. $\phi = \sum_{j=1}^{n}\phi_j 2^{-j}$

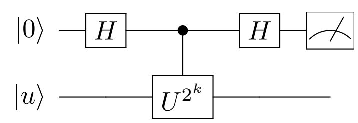
(a) Show that the following circuit estimates ϕ_1.



(b) Show that the following circuit estimates ϕ_2.



(c) Show that the following circuit estimates ϕ_k.



(d) Argue that n circuits with the above structure are sufficient to estimate $\phi = \phi_1\phi_2\cdots\phi_n$.

(e) What is the largest number of gates required in a single circuit? Assume that controlled-U can be implemented in a circuit with u gates. How does this answer compare with Question 7? Explain.

(f) What is the total number of gates required across *all* n circuits? How does this answer compare with Question 7? Explain.

6. Design a *biased* quantum random bit generator algorithm which produces $|0\rangle$ with probability 25 percent and $|1\rangle$ with probability 75 percent.

7. Describe how a classical computer generates “random” numbers. How can we test for the randomness of a bitstring created in this manner?

8. Suggest at least two more methods of generating a random number if you did not have access to a quantum computer

Literature questions

1. The authors of *Variational quantum factoring* (https://arxiv.org/abs/1808.08927) present an near-term quantum algorithm for prime factorization. This algorithm can be understood as an implementation of QAOA—which we discussed in this chapter—for a specific *factoring Hamiltonian* H_f. How is this Hamiltonian constructed from a given integer to be factored?

2. In *Low-depth gradient measurements can improve convergence in variational hybrid quantum-classical algorithms* (https://arxiv.org/abs/1901.05374), the authors advocate the following finite-difference approximation for the gradient of a function:
$$\frac{\partial f}{\partial \theta_i}(\theta) \approx \frac{1}{2\epsilon}(f(\theta + \epsilon\hat{e}_i) - f(\theta - \epsilon\hat{e}_i))$$
Why is this formula preferred over the alternative formula $\frac{\partial f}{\partial \theta_i}(\theta) \approx (f(\theta+\epsilon\hat{e}_i) - f(\theta))/\epsilon$?

3. Harrow and Napp define particular black-box models of gradient and non-gradient oracles. How are these black-box models the same or different from a real quantum computer?

4. Do the theorems in this paper settle the case of gradient vs non-gradient optimization? How might you get around the assumptions?

5. One of the main results of *For Fixed Control Parameters the Quantum Approximate Optimization Algorithm's Objective Function Value Concentrates for Typical Instances* (https://arxiv.org/abs/1812.04170 is that the expectation value of the cost function for MaxCut on 3-regular graphs in the QAOA algorithm at fixed p is independent of the graph, as long as the graph size is large. Explain why this is the case. How would the result change if we looked at 4-regular graphs?