CS-151 Quantum Computer Science: Problem Set 8

Professor: Saeed Mehraban
TA: Dale Jacobs

Spring, 2024

Guidelines: ***The deadline to return this problem set is 11.59pm on Wednesday, April 17***. *You are responsible for solving 3 out of 4 questions (the last question would be extra credit). But all questions will be considered as material for the final exam. Remember that you can collaborate with each other in the preliminary stages of your progress, but each of you must write their solutions independently. Submission of the problem set should be via Gradescope only.*

Problem 1 (25 points). *In this question, we'll illustrate some aspects of Grover's algorithm by contrasting it with a problem known as 'Vaidman's bomb'. At the beginning, we are handed a package that may or may not contain a bomb. Unfortunately, this bomb is so sensitive that even just looking to see whether it exists can result in an explosion. We will see that quantum mechanics allows us to devise a procedure to check whether there is a bomb, without setting it off.*

a) *Consider a single-qubit quantum state which is initialized to the $|0\rangle$ state. This state is rotated towards $|1\rangle$ by an angle $\theta = \frac{\pi}{2N}$ where $N \in \mathbb{N}$. i.e., the rotation is given by,*

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

Let's analyze this process.

(i) *What is the probability of obtaining $|1\rangle$ if we measure the state after N such rotations? (Hint: Show that $R^N_{\theta=\pi/2N} = R_{\pi/2}$)*

(ii) *Now, let's imagine that we were to measure the state after each application of the R_θ-rotation. What's the probability of obtaining $|0\rangle$ after a single rotation?*

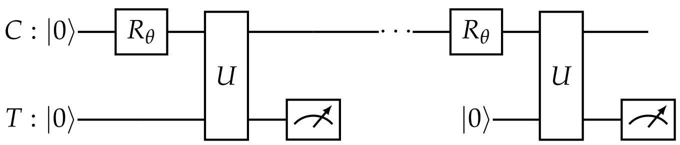
(iii) *Suppose we repeated the step in part (ii) for T rounds. What is the probability of obtaining a 1 during the steps $1, \ldots, N$? How large should we choose T in order to obtain a 1 with a large probability? What is this probability for $T = N$? Is it slower than the process in part (i) or faster? (Hint: for small $\theta \ll 1$ use the approximation $\sin\theta \approx \theta$ and $\cos\theta \approx \sqrt{1-\theta^2}$).*

b) *We will now use the above observations to design an algorithm to detect a bomb without opening the package! Let C be a control register initially set to $|0\rangle$. Let T be another register initially set to $|0\rangle$. If T ever gets set to $|1\rangle$ the bomb gets triggered and there will be an explosion.*

We define a unitary operation U as follows: if there is not a bomb, then it acts as the identity $U = I$, and if there is a bomb, $U = CNOT_{C,T}$ (i.e. applies a NOT gate to T if C is set to $|1\rangle$).

Consider the following quantum circuit, where R_θ is defined in part (a) and U is described above.

There are N occurrences of the 'rotation-measurement' block in the above circuit.



(i) Analyze the case where there is no bomb. What is the final state of the control (first) qubit? How do the measurements of the second qubit affect the algorithm?

(ii) Now, assume there's a bomb present. After the first rotation-measurement 'block' of the circuit, what is the state over the two qubits? When measuring the second qubit, what's the probability of triggering the bomb (i.e., setting T to $|1\rangle$)?

(iii) If the measurement in the last step did not trigger the bomb, what happens to the overall state? What is the overall probability of detecting the bomb after N steps of this algorithm?

(iv) Describe how we can use the above procedure to detect a bomb without triggering it.

(v) (Extra credit) Now, we want to generalize this problem to the case where we have M packages, such that $M-1$ of them contain a bomb and one doesn't. During this procedure, we might set off some of the bombs. Our goal is to find the one clear package and do it with the least explosions possible. Classically we will have to make $M-1$ explosions in the worst case. Show that quantumly, you can do this by setting off at most $O(\sqrt{M})$ of the bombs. (Hint: You may wish to read this paper.)

Problem 2. *Let $f : \{0,1\}^2 \to \{0,1\}$ be a function of 2 bits. Suppose we have a phase oracle for f, P_f.*

a) Suppose we know that f outputs 1 on exactly one input, but we do not know which input. How many classical queries must we make to determine which input? Now suppose the hidden input is 01 and analyze Grover's search to show that we can find the hidden input using fewer than 3 queries.

b) What happens if we keep running the algorithm instead of measuring? Write the state after 4 rounds of the algorithm. Give a brief explanation for what is happening.

c) Now suppose that f outputs 1 on exactly two inputs. Repeat the analysis from part (a) for this case. How many quantum queries are needed to find x such that $f(x) = 1$?

d) Extra credit: Analyze k items among N. Show that the runtime is $O(\sqrt{N/k})$.

Problem 3. *Let N be divisible by 2 and let*

$$f : \{1,2,\ldots,N\} \to \{1,2,\ldots,N/2\}.$$

where for each $x \in \{1,2,\ldots,N\}$ there is exactly one $y \in \{1,2,\ldots,N\}$, $y \neq x$, such that $f(x) = f(y)$.

a) How many classical queries are necessary to find a collision, that is, how many classical queries to find x and $y \neq x$ with $f(x) = f(y)$?

b) Give an $O(\sqrt{N})$ quantum algorithm based on Grover's search to find a collision. (hint: first make a deterministic query, then use Grover's search on the remaining inputs)

c) Show that there is an $O(N^{1/3})$ quantum algorithm based on Grover's search to find a collision. (hint: first make k deterministic queries, then use Grover's search on the remaining inputs)

Problem 4 (Hamiltonian simulation)**.** *Let $A = \sqrt{2}\pi X$ and $B = \sqrt{2}\pi Z$. Recall for an operator H, $e^{iH} = I + iH + \frac{(iH)^2}{2!} + \frac{(iH)^3}{3!} + \ldots$ is given by the Taylor expansion.*

a) Prove that compute an expression for $e^{i(A+B)}$ and $e^{iA}e^{iB}$ in terms of 2×2 matrices and prove $e^{i(A+B)} \neq e^{iA}e^{iB}$. Explain why we don't get equality. (Hint: If for a Hermitian matrix C we have $C^2 = I$, then $e^{i\theta C} = \cos(\theta)I + i\sin(\theta)C$).

Now, suppose we choose a large number N and define $U_{\frac{1}{N}} = e^{iA/N}e^{iB/N}$. $U_{1/N}$ can be interpreted as evolving B for a short time then A for a short time. We want to show that by repeating these two slow evolutions interchangeably, we will eventually create $e^{i(A+B)}$, in other words, $\lim_{N\to\infty} U_{1/N}^{N} = U$.

b) *Let $\hat{U}_{1/N}$ be the expansion of $U_{1/N}$ up to $O(1/N^2)$ terms (i.e. toss out terms with $1/N^k$ coefficients for $k \geq 3$). Let us write $\hat{U}_{1/N} = F + G/N + H/N^2$ (F, G, H do not depend on N). What is the expression for F, G, and H? Your answer should be in terms of* 2×2 *matrices.*

c) *Let $\hat{U} = \hat{U}_{1/N}^{N} = (F + G/N)^N + Q_2/N + Q_3/N^2 + \ldots$. Write an expression for Q_2 and Q_3. Your answer should be in terms of* 2×2 *matrices.*

d) *Prove that $\lim_{N\to\infty} \hat{U}_{1/N}^{N} = e^{i(A+B)}$. (Hint: For an operator C, $\lim_{N\to\infty}(1 + C/N)^N = e^C$.)*

e) *Give an interpretation for the procedure we completed in parts (a)-(d).*