Homework 5

Zheng Xiaoyang
SID: 3035204227

C191A: Introduction to Quantum Computing, Fall 2025
Due: Monday, Oct. 6 2025, 10:00 pm

1 Grover Search

In this question, we'll try to get a geometric understanding of Grover's algorithm. Note that this analysis is a recap of material from lecture.

Recall that in Grover's algorithm we have some distinguished, marked element $a \in \{1, \ldots, N\} = [N]$ and have access to some function $f : [N] \to \{0, 1\}$ that recognizes a, i.e., $f(a) = 1$ and $f(x) = 0$ if $x \neq a$. Our goal is to use f to find a.

Let $|a\rangle$ be the standard basis state labeled with a, and define the uniform superposition over unmarked elements:

$$|e\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \in [N] \text{ and } x \neq a} |x\rangle .$$

At all times, we will maintain a quantum state in the two-dimensional subspace spanned by $|a\rangle$ and $|e\rangle$. That is, our state can be written as $\alpha |a\rangle + \beta |e\rangle$ $(\alpha, \beta \in \mathbb{R})$ and therefore we can understand the algorithm in a two dimensional space.

1.1

We start with the state $|u\rangle = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |x\rangle$. Express $|u\rangle$ in terms of $|a\rangle$ and $|e\rangle$. What is the angle θ between $|u\rangle$ and $|e\rangle$ in the two dimensional space in Fig. 1?

Solution

$$|u\rangle = \frac{1}{\sqrt{N}} |a\rangle + \sqrt{\frac{N-1}{N}} |e\rangle$$

The angle θ between $|u\rangle$ and $|e\rangle$ is given by:

$$\cos(\theta) = \langle e|u\rangle = \sqrt{\frac{N-1}{N}}$$

Thus,

$$\theta = \cos^{-1}\left(\sqrt{\frac{N-1}{N}}\right)$$

1.2

Apply the oracle U_f (defined as $U_f |x\rangle = (-1)^{f(x)} |x\rangle$) to $|u\rangle$, obtaining the state $|\psi\rangle$. Draw $|\psi\rangle$ in the above two dimensional space.

Solution

$$|\psi\rangle = U_f |u\rangle = \frac{1}{\sqrt{N}} |a\rangle - \sqrt{\frac{N-1}{N}} |e\rangle$$

This operation reflects $|u\rangle$ about the axis orthogonal to $|a\rangle$, resulting in the state $|\psi\rangle$.

1.3

Consider the matrix $2 |u\rangle \langle u| - I$. Prove that it is unitary.

Solution

To prove that $2 |u\rangle \langle u| - I$ is unitary, we need to show that:

$$(2 |u\rangle \langle u| - I)(2 |u\rangle \langle u| - I)^\dagger = I$$

Calculating the left-hand side:

$$(2 |u\rangle \langle u| - I)(2 |u\rangle \langle u| - I) = 4 |u\rangle \langle u| |u\rangle \langle u| - 2 |u\rangle \langle u| - 2 |u\rangle \langle u| + I$$

Since $\langle u| |u\rangle = 1$, we have:

$$= 4 |u\rangle \langle u| - 4 |u\rangle \langle u| + I = I$$

Thus, $2 |u\rangle \langle u| - I$ is unitary.

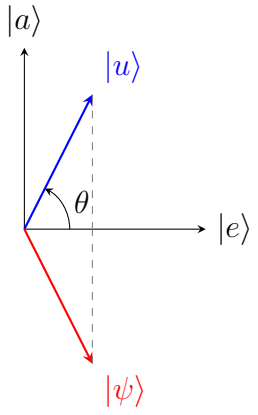

Figure 1: The two-dimensional subspace spanned by $|a\rangle$ and $|e\rangle$, showing $|u\rangle$ and $U_f |u\rangle = |\psi\rangle$.

1.4

Discuss how to implement the unitary operation $2\left|u\right\rangle\left\langle u\right| - I$ using 2-qubit gates.

Solution

To implement the unitary operation $2\left|u\right\rangle\left\langle u\right| - I$ using 2-qubit gates, we can follow these steps:

1. Prepare the state $|u\rangle$ using Hadamard gates on all qubits.
2. Use a series of controlled-NOT (CNOT) gates to create the reflection about $|u\rangle$. This involves creating an ancilla qubit that is flipped if the state is $|u\rangle$.
3. Apply a phase flip (Z gate) to the ancilla qubit.
4. Reverse the CNOT operations to disentangle the ancilla qubit.
5. Finally, apply Hadamard gates again to return to the original basis.

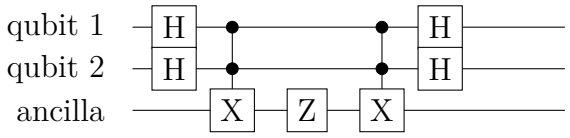

Figure 2: Diffusion operator circuit: implements the reflection $2\left|u\right\rangle\left\langle u\right| - I$ on two qubits using Hadamard, CNOT, ancilla, and phase flip.

1.5

Apply the unitary $2\left|u\right\rangle\left\langle u\right| - I$ to the state $|\psi\rangle$. Draw the resulting state in the above two dimensional space. What operation is it performing on this space?

Solution

Applying the unitary $2\left|u\right\rangle\left\langle u\right| - I$ to the state $|\psi\rangle$:

$$|\phi\rangle = (2\left|u\right\rangle\left\langle u\right| - I)\left|\psi\right\rangle$$

This operation reflects $|\psi\rangle$ about the axis defined by $|u\rangle$, resulting in the state $|\phi\rangle$. In the two-dimensional space, this operation effectively rotates the state closer to $|a\rangle$.

1.6

Apply the operation $(2\left|u\right\rangle\left\langle u\right| - I)U_f$ two more times on the resulting state from 1.5 and draw the two resulting states in the above two dimensional space. What angle of rotation does $(2\left|u\right\rangle\left\langle u\right| - I)U_f$ perform in the space?

Solution

Each application of $(2|u\rangle\langle u| - I)U_f$ rotates the state by an angle of 2θ towards $|a\rangle$. After two more applications, the total rotation from the initial state $|u\rangle$ is 5θ. The resulting states can be drawn in the two-dimensional space, showing the progressive rotation towards $|a\rangle$.

1.7

Grover's algorithm repeatedly applies $(2|u\rangle\langle u| - I)U_f$ to $|u\rangle$ to get close to $|a\rangle$. How many times should you apply this operation to get closest to the state $|a\rangle$? Hint: Use the small angle approximation $\sin(\theta) \approx \theta$.

Solution

To get closest to the state $|a\rangle$, we want to maximize the overlap with $|a\rangle$. The angle between $|u\rangle$ and $|a\rangle$ is $\frac{\pi}{2} - \theta$. Each application of $(2|u\rangle\langle u| - I)U_f$ rotates the state by 2θ. We want to find k such that:

$$(2k+1)\theta \approx \frac{\pi}{2}$$

Using the small angle approximation $\sin(\theta) \approx \theta$, we have:

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

Since $\theta \approx \frac{1}{\sqrt{N}}$ for large N, we get:

$$k \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$$

Thus, the number of applications needed is approximately $\frac{\pi}{4}\sqrt{N}$.

2 Shor's Factoring Algorithm

In this question, we will go through a small example of Shor's factoring algorithm. Recall the following facts about the quantum Fourier transform (QFT_M) applied to periodic and shifted states:

1. QFT on periodic states: Let $1 < r < M$ be an integer that divides M. Then,

$$\mathrm{QFT}_M\left(\frac{1}{\sqrt{r}}(|0\rangle + |r\rangle + |2r\rangle + \cdots + |M-r\rangle)\right) \tag{1}$$

$$= \frac{1}{\sqrt{r}}(|0\rangle + |M/r\rangle + |2M/r\rangle + \cdots + |(r-1)M/r\rangle) \tag{2}$$

2. QFT on shifted states: If $|\psi\rangle = \sum_{k=0}^{M-1} \alpha_k |k\rangle$ and $|\psi + t\rangle = \sum_{k=0}^{M-1} \alpha_k |k + t \bmod N\rangle)$, then QFT_M applied to the two states are related by: If

$$\mathrm{QFT}_M |\psi\rangle = \sum_{k=0}^{M-1} \beta_k |k\rangle\,, \tag{3}$$

then

$$\mathrm{QFT}_M |\psi + t\rangle = \sum_{k=0}^{M-1} \omega^{kt} \beta_k |k\rangle .$$

We will work through an example of factoring $N = 21$ using QFT_M with $M = 12$.

2.1

Let $a = 2$. Calculate the state $|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle |a^x \bmod N\rangle$.

Solution

Calculating $a^x \bmod N$ for $x = 0, 1, \ldots, 11$:

$$\begin{aligned}
2^0 \bmod 21 = 1; 2^1 \bmod 21 = 2; 2^2 \bmod 21 = 4 \\
2^3 \bmod 21 = 8; 2^4 \bmod 21 = 16; 2^5 \bmod 21 = 11 \\
2^6 \bmod 21 = 1; 2^7 \bmod 21 = 2; 2^8 \bmod 21 = 4 \\
2^8 \bmod 21 = 4; 2^9 \bmod 21 = 8; 2^{10} \bmod 21 = 16 \\
2^{11} \bmod 21 = 11
\end{aligned}$$

Thus, the state $|\psi\rangle$ is:

$$|\psi\rangle = \frac{1}{\sqrt{12}} \sum_{x=0}^{11} |x\rangle |a^x \bmod N\rangle$$

2.2

Suppose we measure the second register of $|\psi\rangle$ and obtain "1". What is the resulting state on the first register? Then perform QFT_M on the first register. What is the resulting state on the first register? Now measure this state in the standard basis. What are the possible measurement outcomes?

Solution

After measuring the second register and obtaining "1", the first register collapses to the superposition of states corresponding to x values where $a^x \bmod N = 1$. From the calculations above, this occurs at $x = 0, 6$. Thus, the resulting state on the first register is:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |6\rangle)$$

Now, applying QFT_M to $|\psi_1\rangle$:

$$\mathrm{QFT}_M |\psi_1\rangle = \frac{1}{\sqrt{2}} (\mathrm{QFT}_M |0\rangle + \mathrm{QFT}_M |6\rangle)$$

Using the QFT definition, we have:

$$\mathrm{QFT}_M |0\rangle = \frac{1}{\sqrt{12}} \sum_{k=0}^{11} |k\rangle$$

$$\mathrm{QFT}_M |6\rangle = \frac{1}{\sqrt{12}} \sum_{k=0}^{11} e^{2\pi i \cdot 6k/12} |k\rangle = \frac{1}{\sqrt{12}} \sum_{k=0}^{11} (-1)^k |k\rangle$$

Combining these, we get:

$$\mathrm{QFT}_M |\psi_1\rangle = \frac{1}{\sqrt{24}} \sum_{k=0}^{11} (1 + (-1)^k) |k\rangle = \frac{1}{\sqrt{6}} (|0\rangle + |2\rangle + |4\rangle + |6\rangle + |8\rangle + |10\rangle)$$

The possible measurement outcomes are $0, 2, 4, 6, 8, 10$.

2.3

Suppose we repeat the above experiment, now the first step (when measuring the second register) gives "4". Answer the same questions as above.

Solution

After measuring the second register and obtaining "4", the first register collapses to the superposition of states corresponding to x values where $a^x \bmod N = 4$. From the calculations above, this occurs at $x = 2, 8$. Thus, the resulting state on the first register is:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} (|2\rangle + |8\rangle)$$

Now, applying QFT_M to $|\psi_2\rangle$:

$$\mathrm{QFT}_M |\psi_2\rangle = \frac{1}{\sqrt{2}} (\mathrm{QFT}_M |2\rangle + \mathrm{QFT}_M |8\rangle)$$

Using the QFT definition, we have:

$$\mathrm{QFT}_M |2\rangle = \frac{1}{\sqrt{12}} \sum_{k=0}^{11} e^{2\pi i \cdot 2k/12} |k\rangle$$

$$\mathrm{QFT}_M |8\rangle = \frac{1}{\sqrt{12}} \sum_{k=0}^{11} e^{2\pi i \cdot 8k/12} |k\rangle$$

Combining these, we get:

$$\mathrm{QFT}_M |\psi_2\rangle = \frac{1}{\sqrt{24}} \sum_{k=0}^{11} (e^{2\pi i \cdot 2k/12} + e^{2\pi i \cdot 8k/12}) |k\rangle$$

The possible measurement outcomes can be calculated from the resulting state, which will yield a distribution over the basis states. The possible measurement outcomes are $0, 3, 6, 9$.

2.4

Suppose we repeat the above experiment 4 times in total. Each time we record a measurement outcome of the first register (after performing QFT_M). Suppose the recorded outcomes are all different. What is their greatest common divisor g?

Solution

Assuming the recorded outcomes from the four experiments are x_1, x_2, x_3, x_4, we can calculate their greatest common divisor g using the Euclidean algorithm. For example, if the outcomes are $0, 2, 4, 6$, then:

$$g = \gcd(0, 2, 4, 6) = 2$$

The actual value of g will depend on the specific outcomes obtained from the experiments.

2.5

Calculate $\gcd(N, a^{M/2g} - 1)$ and $\gcd(N, a^{M/2g} + 1)$. Are they prime factors of N?

Solution

Given $N = 21$, $a = 2$, $M = 12$, and $g = 2$ (from the previous example), we calculate:

$$a^{M/2g} = 2^{12/4} = 2^3 = 8$$

Now, we compute:

$$\gcd(21, 8 - 1) = \gcd(21, 7) = 7$$

$$\gcd(21, 8 + 1) = \gcd(21, 9) = 3$$

Both 7 and 3 are prime factors of $N = 21$.