GROVER'S SEARCH ALGORITHM

Notes for the Qiskit textbook section 3.

3.1. **More on Grover's search algorithm.** Suppose we have a function $f\colon \{0,1\}^n \to \{0,1\}$ that is defined by

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution,} \\ 0 & \text{if } x \text{ is not a solution} \end{cases}$$

Then the *search problem* is to find these solutions (i.e., to find each i such that $f(i) = 1$). Grover's search algorithm helps solve this more efficiently than its classical counterpart.

Definition.

- Let t be the number of solutions in x.
- We define the "good" state $|G\rangle$ as the superposition of the indexes of the states that are solutions (i.e., $f(i) = 1$). In other words,

$$|G\rangle = \frac{1}{\sqrt{t}} \sum_{i \in \{0,1\}^n; f(i)=1} |i\rangle$$

- And we define the "bad" state $|B\rangle$ as the superposition of the indexes of the states that are not solutions (i.e., $f(i) = 0$). In other words,

$$|B\rangle = \frac{1}{\sqrt{N-t}} \sum_{i \in \{0,1\}^n; f(i)=0} |i\rangle$$

Exercise 1. *Verify that we have $|G\rangle$ is orthogonal to $|B\rangle$.*

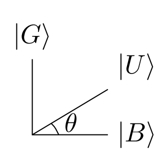
Algorithm. *Grover's search algorithm*:

Step 1: Start with $|0^n\rangle$.

Step 2: Apply Hadamard to get $|U\rangle = H^{\otimes n}|0^n\rangle$. So we have:

$$\begin{aligned} |U\rangle = H^{\otimes n}|0^n\rangle &= \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle \\ &= \sqrt{\frac{t}{N}}|G\rangle + \sqrt{\frac{N-t}{N}}|B\rangle \\ &= \sin\theta|G\rangle + \cos\theta|B\rangle \end{aligned}$$

where $\theta = \arcsin\sqrt{t/N}$. Geometrically, we have



Date: December 2022.

Step 3: Apply the *Grover diffusion* $\mathcal{G}$ to $|U\rangle$. If we know the number of solutions t, then we apply this $\lfloor k \rfloor$ times, where $k = \dfrac{\pi}{4\theta} - \dfrac{1}{2}$ and $\theta = \arcsin\sqrt{t/N}$.

We define the *Grover diffusion* as $\mathcal{G} = H^{\otimes n} R H^{\otimes n} \mathcal{O}_f$, where the oracle $\mathcal{O}_f$ is defined as $\mathcal{O}_f = (-1)^{f(i)}|i\rangle$, and R is the unitary transformation that applies a phase of -1 to all basis states $|i\rangle$ where $i \neq 0^n$, i.e.,

$$R = \begin{pmatrix} 1 & & & & 0 \\ & -1 & & & \\ & & -1 & & \\ & & & \ddots & \\ 0 & & & & -1 \end{pmatrix}$$

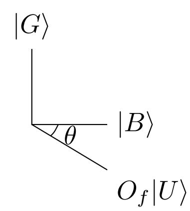
Exercise 2. *Verify that we can write $R = 2|0^n\rangle\langle 0^n| - 1$. Then deduce that we get $H^{\otimes n} R H^{\otimes n} = 2|U\rangle\langle U| - 1$, where $|U\rangle$ is our state from Step 2 (i.e., $|U\rangle = H^{\otimes n}|0^n\rangle$).*

Following the above exercise, we can then assume that the Grover diffusion is given by $\mathcal{G} = (2|U\rangle\langle U| - 1)\mathcal{O}_f$

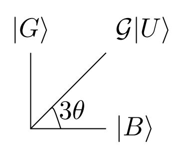
Applying the oracle to $|U\rangle$ gives us

$$\mathcal{O}_f|U\rangle = -\sin\theta|G\rangle + \cos\theta|B\rangle = \sin(-\theta)|G\rangle + \cos(-\theta)|B\rangle$$

This can be seen as



Applying $2|U\rangle\langle U| - I$ to the above state gives



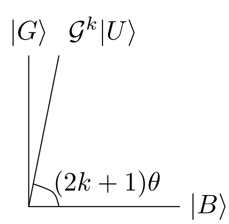
Step 4: Measure the first register.

Exercise 3. *Show that applying the Grover diffusion $k \in \mathbb{N}$ times to $|U\rangle = H^{\otimes n}|0^n\rangle$ gives*

$$\mathcal{G}^k|U\rangle = \sin((2k+1)\theta)|G\rangle + \cos((2k+1)\theta)|B\rangle$$

where $\theta = \arcsin\sqrt{t/N}$.

So if we apply $\mathcal{G}^k$ to our state $|U\rangle = H^{\otimes n}|0^n\rangle$, then, geometrically we get



So the closer the angle is to $\pi/2$, the higher the probability of the algorithm being successful.

Exercise 4. *Deduce that the number of iterations of the Grover diffusion in Grover's search algorithm we need in order to be successful is* $\lfloor k \rfloor$ *where* $k = \dfrac{\pi}{4\theta} - \dfrac{1}{2}$ *and* $\theta = \arcsin\sqrt{t/N}$.

3.2. **Example for two qubits.** Suppose we have our 2-qubit system with $|11\rangle$ being our marked state (i.e., the one we need to find). Exercise 4 tells us that to find this solution successfully, we need to apply the Grover diffusion $\dfrac{\pi}{4\arcsin(1/2)} - \dfrac{1}{2} = 1$ time.

We want our oracle $\mathcal{O}_f$ to apply a phase of -1 to our marked state $|11\rangle$ and to do nothing for the other states (so $f(11) = 1$). We can implement this with a controlled Z-gate.

So let our oracle $\mathcal{O}_f$ be the controlled Z-gate which we can write as $\mathcal{O}_f = 1 - 2|11\rangle\langle 11|$.

Exercise 5. *Verify that we can write the controlled Z-gate as* $1 - 2|11\rangle\langle 11|$.

Now we start with our search.

Step 1. Start with our initial state $|00\rangle$

Step 2. Apply $H^{\otimes 2}$ to our state:

$$|s\rangle = H^{\otimes 2}|00\rangle = |{+}{+}\rangle$$

Exercise 6. *Verify that we get* $\langle s|11\rangle = \frac{1}{2}$ *and* $\langle s|s\rangle = 1$.

Step 3. Apply the Grover diffusion operator $\mathcal{G}$ to our state $|s\rangle$:

$$\begin{aligned}
\mathcal{G}|s\rangle &= (2|s\rangle\langle s| - 1)\mathcal{O}_f|s\rangle \\
&= (2|s\rangle\langle s| - 1)(1 - 2|11\rangle\langle 11|)|s\rangle \\
&= (2|s\rangle\langle s| - 1)(|s\rangle - |11\rangle) \\
&= 2|s\rangle\langle s|s\rangle - 2|s\rangle\langle s|11\rangle - |s\rangle + |11\rangle \\
&= 2|s\rangle - |s\rangle - |s\rangle + |11\rangle \\
&= |11\rangle
\end{aligned}$$

Step 4. After measuring our register, we clearly get $|11\rangle$ with certainty.

Following the above example, we see that sometimes applying the Grover diffusion one time is sufficient to get the solution with certainty. This happens to be true for $N/4$ solutions.

Exercise 7. *If the number of markers equals $N/4$, then Grover's algorithm will always get the solution with certainty after one iteration. Here, $N = 2^n$ where n is the number of qubits.*

Exercise 8. *Repeat the above example, but this time apply the Grover diffusion twice. What do we get? Explain geometrically why and what happens if we keep applying Grover's diffusion more than* $\lfloor k \rfloor$ *times where* $k = \dfrac{\pi}{4\theta} - \dfrac{1}{2}$ *and* $\theta = \arcsin\sqrt{t/N}$.