Quantum Computing 2025 - Exercise Sheet 3

Grover's Algorithm

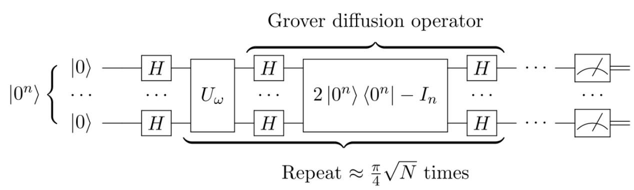
Grover's algorithm (developed by Lov Grover in 1996) provides a speedup over classical algorithms for unstructured search of a database. As we will see below, this algorithm employs a trick called "amplitude estimation" which can be used as subroutine in many other quantum algorithms.

Problem Statement

We are given some database with $N = 2^n$ elements. In this we are told to find the marked element w. This is an example of unstructured search since we are not given any information about how the elements are ordered. Here, each element will be labeled with a binary value e.g. for $n = 2$ bits ($N = 4$), The first item is $|00\rangle$, next item is $|01\rangle$, and then $|10\rangle$ and finally $|11\rangle$.

Classically, in the worst case you would have to check all N items, and on average $N/2$ items have to be checked. In other words it has complexity $O(N)$. We are going to show that Grover's algorithm has complexity $O(\sqrt{N})$, a quadratic speedup!

1. *(Algorithm Overview)*



Above, is the general circuit for Grover's algorithm.

(a) *As a reminder from the last exercise, write the state after applying the first set of Hadamard transforms. We will call this state $|s\rangle$.*

(b) *The next step is to apply the oracle U_w, which behaves similarly as the oracle in the DJ algorithm. This oracle maps the winning state $|w\rangle$ to $-|w\rangle$ and leaves all other states unaffected. What is U_w in Dirac notation?*

(c) *Write U_w as a matrix for $n = 3$ and $|101\rangle$ as the winning state?*

(d) *Next we apply the diffusion operator, we call this V, which is another oracle sandwiched between Hadamard transforms. Calculate V in Dirac notation.*

a) Recall that

$$H^{\otimes n} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

so when the initial state is $|0\rangle^{\otimes n}$ we get

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

.

b) We have that

$$U_w |w\rangle \to -|w\rangle \quad U_w |x\rangle \to |x\rangle, \forall x \neq w$$

So we could write

$$U_w = \sum_{x \neq w} |x\rangle\langle x| - |w\rangle\langle w|$$

Or in a more condense way, since $I = \sum_x |x\rangle\langle x|$, we can equivalently write

$$U_w = I_N - 2|w\rangle\langle w|$$

.

c) From the above, U_w will clearly only have diagonal elements with each value being a 1 and only the element which corresponds to the position of the marked state would have -1. So for $|w\rangle = |101\rangle$

$$|101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

In the above vector only the 6th element is nonzero, hence the $(U_w)_{66} = -1$. All other diagonal elements are 1 and the rest of the elements are 0.

$$U_w = \begin{bmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& -1 && \\ &&&&&& 1 & \\ &&&&&&& 1 \end{bmatrix}$$

d)

$$V = 2H^{\otimes n} |0\rangle^{\otimes n} \langle 0|^{\otimes n} H^{\otimes n} - H^{\otimes n} I_N H^{\otimes n}$$

For the first term just apply the operators to the *bra* and the *ket*.
If you remember from a previous exercise H is it's own unitary hence $H^{\otimes n} I_N H^{\otimes n} = H^{\otimes n} H^{\otimes n} = I_N$. Therefore,

$$V = 2|s\rangle\langle s| - I_N$$

.

2. *(Geometric View) Let's consider the initial state in terms of the winning state $|w\rangle$ and all other states $|w^{\perp}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$.*

(a) *What is $|s\rangle$, written in terms of these states?*

(b) *Equivalently we could write $|s\rangle = \sin\frac{\theta}{2}|w\rangle + \cos\frac{\theta}{2}|w^{\perp}\rangle$. What is the value of θ?*

(c) *Draw the state $|s\rangle$ on the $|w^{\perp}\rangle - |w\rangle$ plane (i.e. $|w\rangle$ on the y-axis).*

(d) *Draw the state after applying a single U_w and again after applying V*

(e) *What is the overall angle of rotation from $|s\rangle$ to $VU_w|s\rangle$. What is the angle after applying these gates r times?*

(f) *For what value of r should we use in order that we are in $|w\rangle$? What is it's relation to the number of elements N?*

(g) *Of course r can only be an integer though, so it's likely that we will not be in $|w\rangle$. What is the minimum bound on the probability $P(|w\rangle)$?*

(h) *For each step of Grover's algorithm, draw a bar chart of the probability amplitude for all the states.*

(i) *Consider what would happen if we had M winning elements to find. How many times would we need to apply r in this case?*

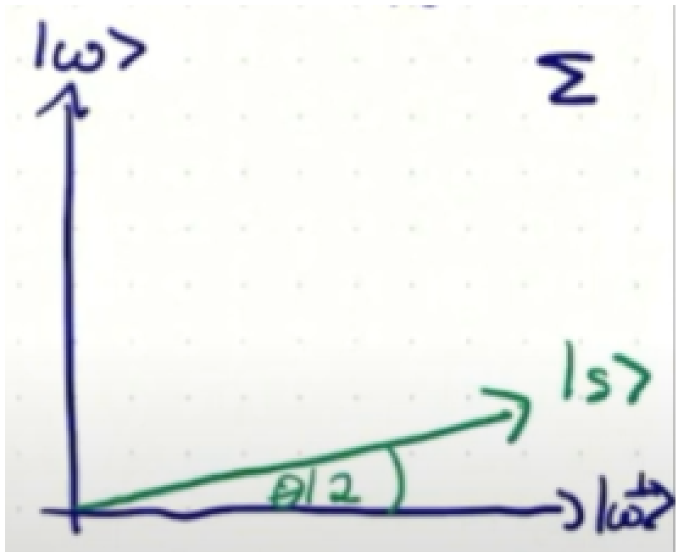
a)

$$|s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle = \frac{1}{\sqrt{N}} |w\rangle + \frac{1}{\sqrt{N}} \sum_{x \neq w} |x\rangle = \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |w^{\perp}\rangle$$

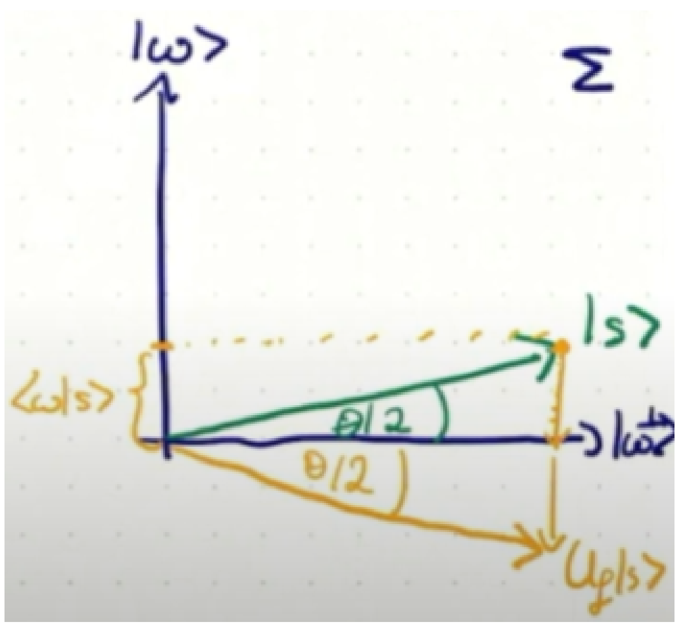
b)

$$\sin\theta/2 = \frac{1}{\sqrt{N}} \to \theta = 2\arcsin\frac{1}{\sqrt{N}}$$

c)



d) After U_w



After V

e) We have rotated by θ degrees. After r applications we rotate by $r\theta$

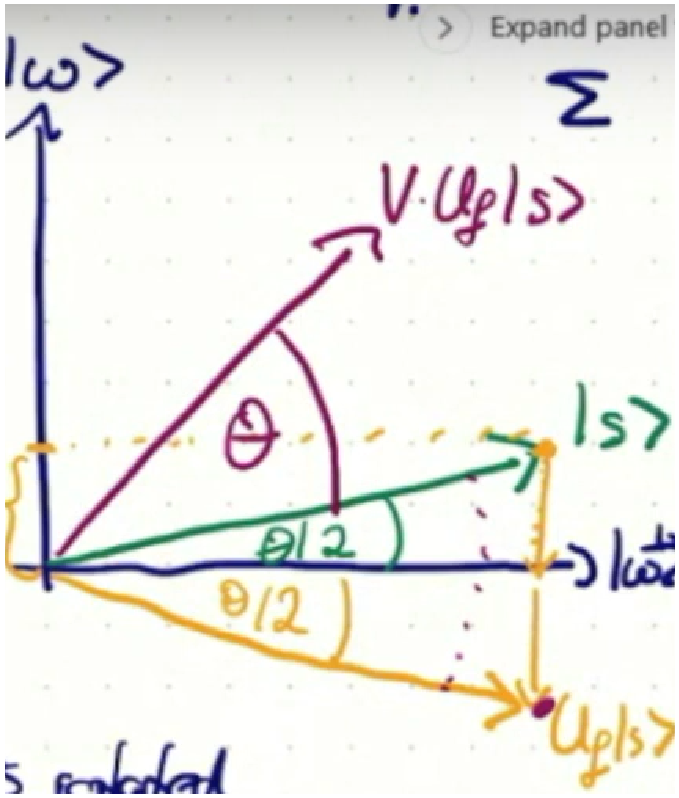
f) We want to project onto the state $|w\rangle$ which is at the angle $\frac{\pi}{2}$ from $|w^{\perp}\rangle$. Hence

$$r\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

Rearranging will give

$$r = \frac{\pi}{2\theta} - \frac{1}{2} = \frac{\pi}{4\arcsin\frac{1}{\sqrt{N}}} - \frac{1}{2}$$

For large N, $\arcsin N \approx N$ and we can discard the factor of $1/2$. Hence



$$r \approx \frac{\pi}{4}\sqrt{N}.$$

g) The farthest away we can be from the state $|w\rangle$ is $\frac{\pi}{2} - \frac{\theta}{2}$ (if we were closer then we stop applying the gates and if we were further we would apply them again). Hence

$$P(|w\rangle) \geq \sin^2(\frac{\pi}{2} - \frac{\theta}{2}) = 1 - \sin^2\frac{\theta}{2} = \cos^2\frac{\theta}{2}$$

h) See solution in class
i) The M marked elements would be represented by the state

$$|w\rangle = \frac{1}{\sqrt{M}}\sum_i |w_i\rangle$$

and the orthogonal state would be

$$|w^{\perp}\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\neq w} |x\rangle$$

so

$$|s\rangle = \sqrt{\frac{M}{N}}\,|w\rangle + \sqrt{\frac{N-M}{N}}\,|w^{\perp}\rangle$$

and $\theta = 2\arcsin\sqrt{M/N}$. Plugging this into r gives us

$$r \approx \frac{\pi}{4}\sqrt{\frac{M}{N}}$$

So having more elements to find reduces the complexity. This makes more sense when we look at what happens to the average amplitude.