Grover's Algorithm

It's a database-search algorithm, and its speedup is quadratic.

– When there is a large amount of unordered data

1. What is our problem?

Let $N=2^n$. Find x s.t. $f(x)=1$ after $O(\sqrt{N})$ evaluation

0	1	2		w-1	w	w+1		N-1
0	0	0	. . .	0	1	0	. . .	0

Classically, we can find this element after $O(N)$ evaluations.

Question: Can we find this element faster? Or in other words, can we find this element using fewer number of queries?

2. How to solve this problem?

(1) Consider an oracle: it is a block box that takes some inputs and produces some outputs. A query to an oracle produces answers.

At this stage, we don't care about the inner working of the oracle.

- $\boxed{U_w}$ $\qquad U_w|x\rangle = \begin{cases} -|x\rangle, & x=w \\ |x\rangle, & \text{otherwise} \end{cases}$

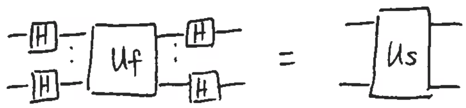
The Phase Inversion Operator

Alternatively, we can think of $U_w|x\rangle = (-1)^{f(x)}|x\rangle$, where $f: \{0,\dots,N-1\} \to \{0,1\}$

- When $x=w$, $f(x)=1$, w is identified, and we say "w satisfies f"
- When $x\neq w$, $f(x)=0$, and we say "x does not satisfy f".

Remark: Here we assume only one index out of $\{0,\dots,N-1\}$ satisfies f.

$$U_w = I - 2|w\rangle\langle w| \quad \begin{cases} U_w|w\rangle = (I-2|w\rangle\langle w|)|w\rangle = -|w\rangle \\ U_w|w^\perp\rangle = (I-2|w\rangle\langle w|)|w^\perp\rangle = |w^\perp\rangle \end{cases} \Rightarrow \text{Reflection about } |w^\perp\rangle$$

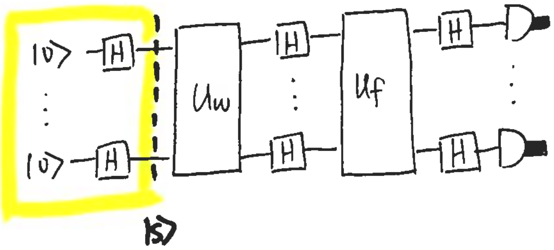
- 

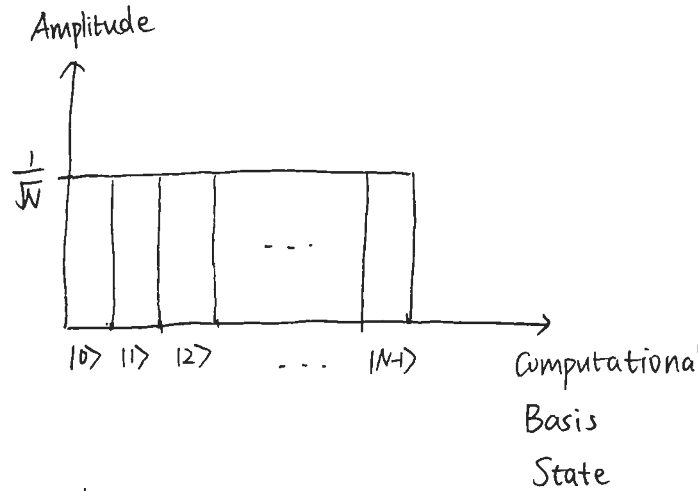
The Grover Diffusion Operator

$$U_s = 2|s\rangle\langle s| - I = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}$$

$$\begin{cases} U_s|s\rangle = (2|s\rangle\langle s| - I)|s\rangle = |s\rangle \\ U_s|s^\perp\rangle = (2|s\rangle\langle s| - I)|s^\perp\rangle = -|s^\perp\rangle \end{cases} \Rightarrow \text{Reflection about } |s\rangle$$

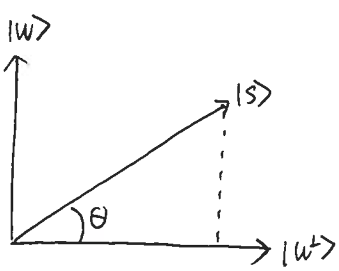
Step 1: Initialize the system to the uniform superposition over all states





$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

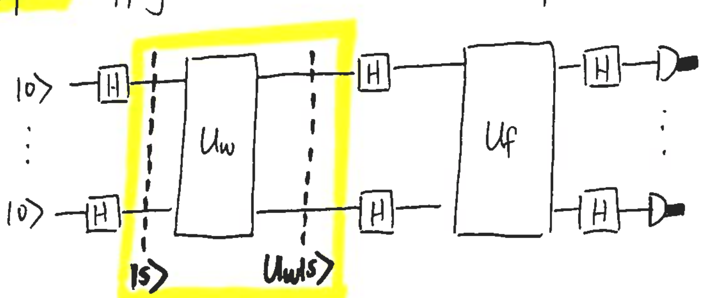
Then $|s\rangle = \sqrt{\frac{N-1}{N}}|w^\perp\rangle + \frac{1}{\sqrt{N}}|w\rangle$, where $\langle w^\perp|w\rangle = 0$.



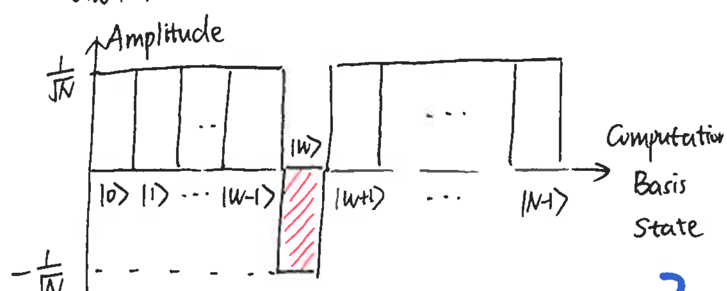
$\cos\theta = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \frac{1}{\sqrt{N}}$

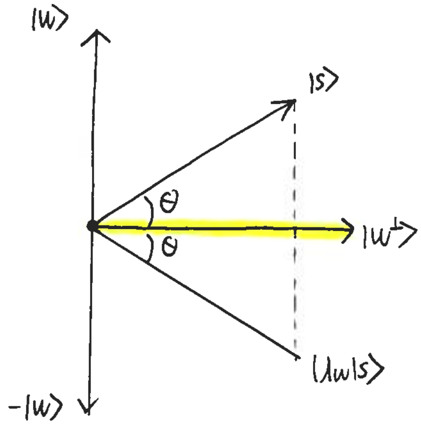
Hence $\theta = \arcsin\frac{1}{\sqrt{N}}$

Step 2: Apply the Phase Inversion Operator

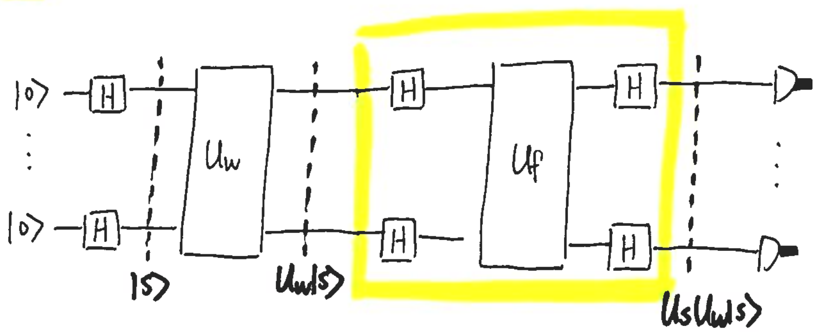


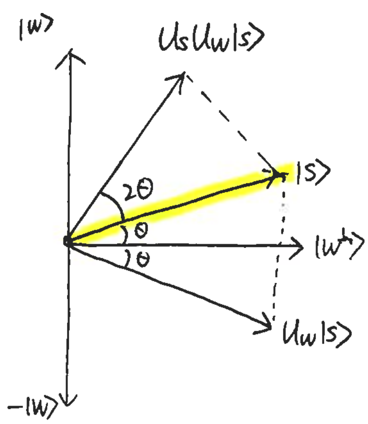
$U_w|w\rangle = -|w\rangle$ and $U_w|x\rangle = |x\rangle$ for $x \neq w$





Step 3: Apply the Grover Diffusion Operator

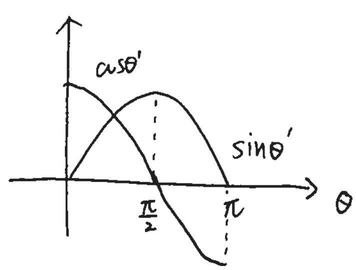


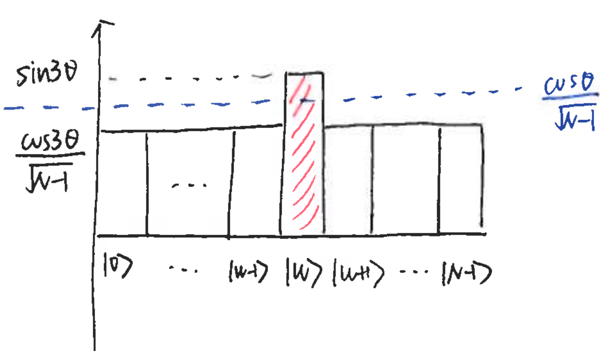


Angle between $|s\rangle$ and $|w^\perp\rangle$: θ

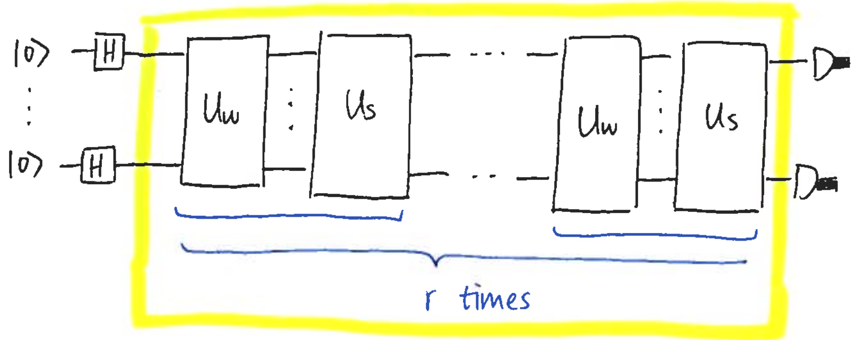
Angle between $U_sU_w|s\rangle$ and $|w^\perp\rangle$: $\theta' = 3\theta$

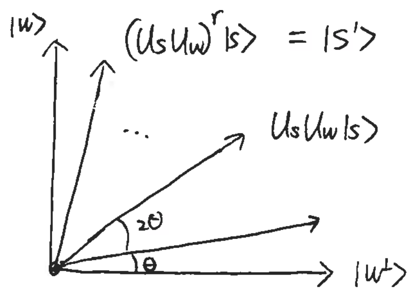
Since $|s\rangle = \cos\theta'|w^\perp\rangle + \sin\theta'|w\rangle$ with $\theta' \nearrow$ $\sin\theta' \nearrow$ and $\cos\theta' \downarrow$, the amplitude before $|w^\perp\rangle \downarrow$ and $|w\rangle \uparrow$.





Repeat steps 2 and 3 r times





$|s'\rangle = \cos\theta'|w^\perp\rangle + \sin\theta'|w\rangle$

Since $\theta' \to \frac{\pi}{2}$, $\cos\theta' \to 0$ and $\sin\theta' \to 1$

Moreover, $\theta' = 2r\theta + \theta = (2r+1)\theta \approx \frac{\pi}{2}$

Then $r = \left(\frac{\pi}{2\theta} - 1\right)\frac{1}{2} = \frac{\pi}{4\theta} - \frac{1}{2}$

Recall $\lim_{\theta \to 0} \frac{\sin\theta}{\theta} = 1$. That is $\sin\theta \approx \theta$, when θ is small.

Hence $\theta \approx \sin\theta = \sin \arcsin\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{N}}$

Ther $r \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2} = O(\sqrt{N})$

I. Unstructured Search

0	0	0	...	1	...	0
0	1	2	...	w	...	2^n-1

Let $N=2^n$.

we are looking for "w" in the list.

1. Using a classical computer, we can find such an element in $O(N)$ time. ($O(2^n) = O(N)$)
2. Using a quantum computer, the Grover's algorithm find such an element in $O(\sqrt{N})$ time.

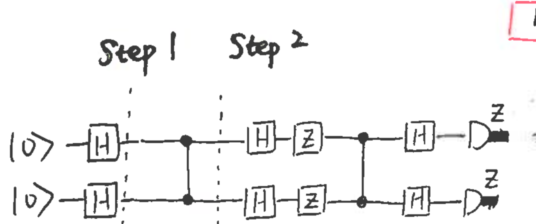
II Oracle Function

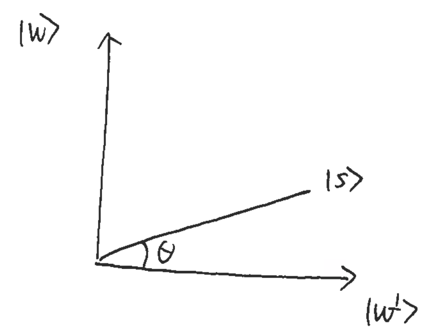
$$f(x) = \begin{cases} 0 & x = w \\ 1 & x \neq w \end{cases}$$

Oracle answers a question, but it's not necessarily clear how to implement it. You can think of it as a blackbox

Example $w = 11$

X	f(x)
00	0
01	0
10	0
11	1





Step 1: $H \otimes H |00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$= \frac{1}{2}|00\rangle + \frac{1}{2}(|01\rangle + |10\rangle + |11\rangle)$

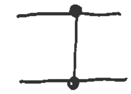
$\therefore\ |s\rangle = \frac{1}{2}|w\rangle + \frac{\sqrt{3}}{2}|w^{\perp}\rangle, \quad |w^{\perp}\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle)$

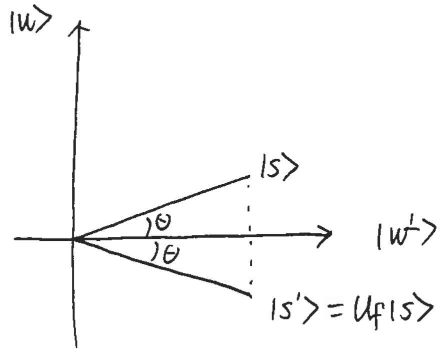
$\cos\theta = \frac{\sqrt{3}}{2}, \ \sin\theta = \frac{1}{2} \Rightarrow \theta = \frac{\pi}{6}$

Step 2: Oracle function $U_f|x\rangle = (-1)^{f(x)}|x\rangle$. Reflection about $|w^{\perp}\rangle$

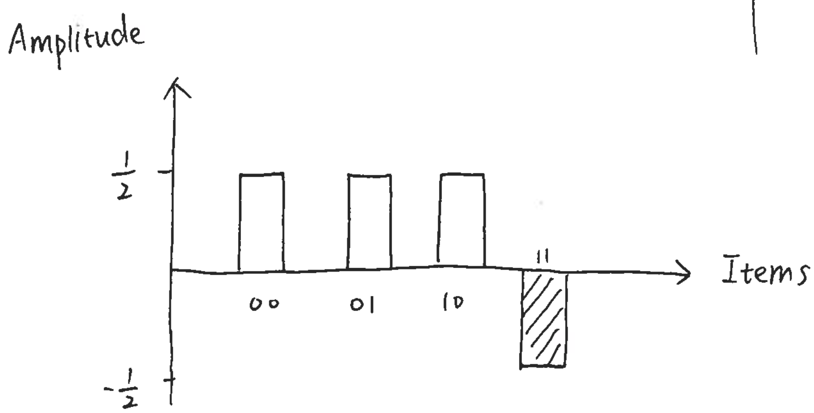
$U_f|00\rangle = |00\rangle$ $U_f|01\rangle = |01\rangle$ $U_f|10\rangle = |10\rangle$ $U_f|11\rangle = -|11\rangle$

$$U_f = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} =: CZ$$

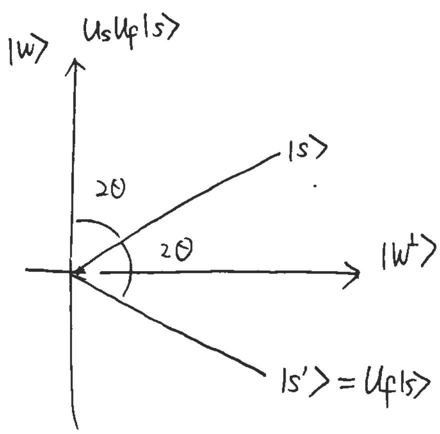




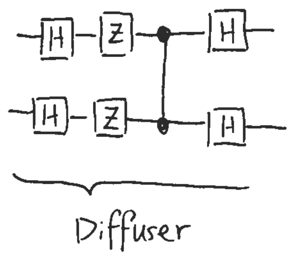
$\theta = \frac{\pi}{6}$

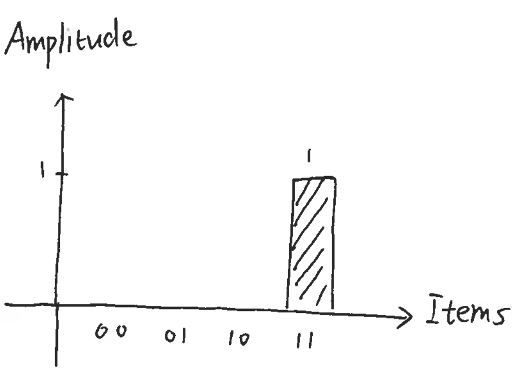


Step 3: $U_s = 2|s\rangle\langle s| - I$ Reflection about $|s\rangle$.

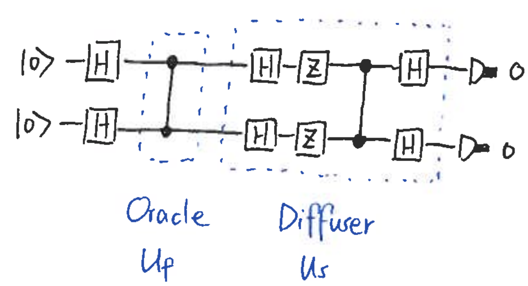


$3\theta = \frac{\pi}{2}$.





The Final Circuit for Solving the Two-Qubit Grover's Algorithm



Exercises :

1. What if $|w\rangle = |00\rangle$?

2. What if $|w\rangle = |01\rangle$?