$$|\psi\rangle = \sum_x a_x |x\rangle$$

$$|s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle \qquad N = 2^n$$

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x a_x$$

$$\bar{a} = \frac{1}{N} \sum_x a_x$$

$$\boxed{\langle s|\psi\rangle = \sqrt{N}\,\bar{a}}$$

$$U_s|\psi\rangle = \left(2|s\rangle\langle s| - I\right)|\psi\rangle$$

$$= \left(2|s\rangle\langle s| - I\right) \underbrace{\sum a_x |x\rangle}$$

$$= 2|s\rangle\langle s|\psi\rangle - |\psi\rangle$$

$$= 2|s\rangle \sqrt{N}\,\bar{a} - \sum a_x |x\rangle$$

$$= 2\sqrt{N}\,\bar{a}\, \frac{1}{\sqrt{N}} \sum |x\rangle - \sum a_x |x\rangle$$

$$\boxed{U_s|\psi\rangle = \sum \left(2\bar{a} - a_x\right)|x\rangle}$$

Before application of U_s, our amplitude of $|x\rangle$ in the state $|\psi\rangle$ was a_x

After application of U_s the amplitude is $(2\bar{a} - a_x)$

Initial amplitude w.r.t. the mean : $a_x - \bar{a}$

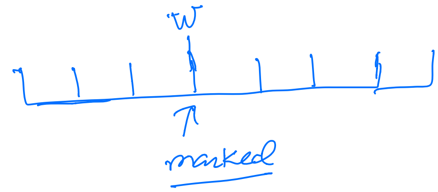
Final amplitude w.r.t. the mean : $(2\bar{a} - a_x) - \bar{a}$

$$= \bar{a} - a_x$$

Example

$N = 8$

$w = 4$



In $|s\rangle$ each basis state has strength $\frac{1}{\sqrt{8}}$

U_w inverts the amplitude of $|w\rangle$ state

After application of U_w, the amplitude of $|w\rangle$ becomes $-\frac{1}{\sqrt{8}}$, all others remain $\frac{1}{\sqrt{8}}$

Mean: $\frac{1}{8}\left[\frac{7}{\sqrt{8}} - \frac{1}{\sqrt{8}}\right] = \frac{3}{8\sqrt{2}}$

The amplitude of the unmarked state u is $\frac{1}{\sqrt{8}}$

Apply U_s:

New amplitude will be

$$2\bar{a} - a_x$$

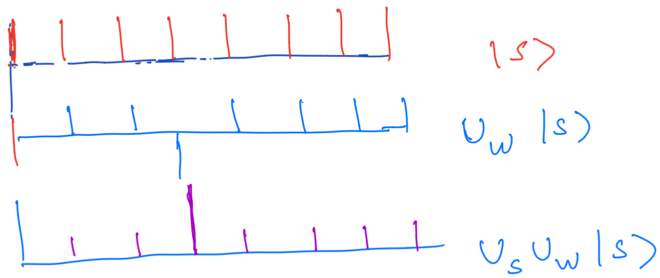
Every unmarked state will have an amplitude

$$2\,\frac{3}{8\sqrt{2}} - \frac{1}{\sqrt{8}} = \frac{1}{4\sqrt{2}}$$

The marked state will have the amplitude

$$\frac{3}{4\sqrt{2}} + \frac{1}{\sqrt{8}} = \frac{5}{4\sqrt{2}}$$

$\Rightarrow$ After application of U_s the marked state is amplified 5 times than that of unmarked state



The angle between $|s\rangle$ and $|w\rangle$ is $\frac{\pi}{2} - \theta$

Since each Grover rotation is by 2θ

we require after m iterations, we should have

$$m\, 2\theta \cong \frac{\pi}{2} - \theta$$

$$\Rightarrow \quad m \cong \frac{\pi}{4\theta} - \frac{1}{2}$$

$$\theta = \sin\theta = \frac{1}{\sqrt{N}}$$

$$\langle w|s\rangle = \frac{1}{\sqrt{N}}$$

For large N

$$\boxed{m = \frac{\pi\sqrt{N}}{4}}$$

$O(\sqrt{N})$ quantum

$O(N)$ classical

After m iterations the angle between $|s\rangle$ and $|w\rangle$ is

$$\frac{\pi}{2} - \theta - 2m\theta = \frac{\pi}{2} - \underline{(2m+1)\theta},$$

The amplitude of $|w\rangle$ in $|s\rangle$ is

$$\sin(2m+1)\theta$$

$$\approx \sin\left[\left(2\frac{\pi\sqrt{N}}{4} + 1\right)\frac{1}{\sqrt{N}}\right]$$

$$= \sin\left(\frac{\pi}{2} + \frac{1}{\sqrt{N}}\right)$$

$$= \cos\frac{1}{\sqrt{N}}$$

$$= 1 - \frac{1}{2N} \qquad (\text{for large } N)$$

Matrix implementation of Grover's algorithm

Define, diffusion operator ($n \times n$ matrix)

$$D_{ij} = \begin{cases} -1 + \frac{2}{N} & \text{if } i=j \\ \frac{2}{N} & \text{if } i \neq j \end{cases}$$

$N=2$

$$D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

~~N=3~~

$$\boxed{D = -I + \frac{2J}{N}}$$

J is a matrix whose each element is 1

e.g. $N=2$

$$D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + \frac{2}{N=2} \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}}_{J} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\left(\frac{J}{N}\right)^2 = \frac{J}{N} \qquad P^2 = P$$

$\Rightarrow \frac{J}{N}$ is a projection operator

J is an $N \times N$ matrix with each element unity

$$D \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} = \left(-I + \frac{2J}{N} \right) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix}$$

$$= \begin{pmatrix} -a_1 + 2\bar{a} \\ -a_2 + 2\bar{a} \\ \\ -a_N + 2\bar{a} \end{pmatrix} \qquad |\psi\rangle = \sum a_x |x\rangle$$

$$\Rightarrow \boxed{D|\psi\rangle = \sum_x (2\bar{a} - a_x)|x\rangle}$$

We can implement the action of U_s by a matrix D

$$\boxed{D = WRW}$$

W is the Walsh-Hadamard transformation
R is the selective phase rotation

W is simply an extension of the Hadamard operation on a single qubit to the case of n qubit.

$$\boxed{H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_K (-1)^{x \cdot K} |K\rangle}, \quad N = 2^n$$

bitwise product

The matrix elements for W

$$W_{ij} = \frac{1}{\sqrt{N}} (-1)^{i.j}$$

The matrix element for R_{ij} is

$$R_{ij} = (2\delta_{i0} - 1)\,\delta_{ij}$$

Steps in Grover's algorithm

1. Generate the standard state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

2. The $(n+1)$th qubit is initialized to $\boxed{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}$

3. Loop is applied m-times (i.e. apply Grover operation m-times)

U_W (a) Apply the oracle (T-operation)

$$|s\rangle|y\rangle \longrightarrow \sum_{x=0}^{N-1} a_x |x\rangle (-1)^{f(x)} |y\rangle$$

U_S (b) Apply Diffusion operators

$$D = WRW$$

(c) Apply steps (a) and (b) $O(\sqrt{N})$ number of times

4. Measure the first register. With a very high probability, we can identify the marked state w.

5. The algorithm may fail to yield result, the probability of that is $O\left(\frac{1}{N}\right)$ Then go to step number 1