Grover's algorithm

Having <u>not sorted</u> array of elements, the taske is to find certain element (which we will call the „winner").

<u>Illustrative example</u>: having phone number find the name of the person in phone book.

$$\{x_i\} \quad i = 0, 1, 2, \ldots, N-1$$

N elements

w – winner, which we look for

We have also function (so called <u>oracle</u>) which for given element answers if it is a winner or not:

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

- Number of calls to function f is the complexity of the algorithm.
- Classically, since the array is <u>unsorted</u>, statistically we need $N/2$ calls, which means complexity is $O(N)$

- such oracle functions are very popular in quantum algorithms
- having function $f(x)$ we can use the following form of oracle as an operator:

$$\boxed{\hat{O}|x\rangle \equiv (-1)^{f(x)}|x\rangle} \quad (2)$$

Let's consider the situation where states $|x_0\rangle, |x_1\rangle, \ldots, |x_{N-1}\rangle$ are basis states in some Hilbert space of dimension N.

We can construct such Hilbert space using n qubits : $N = 2^n$

Let's consider following state:

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle \Rightarrow |\alpha\rangle \perp |w\rangle \quad (3)$$

↑ as $|\alpha\rangle$ does not contain $|w\rangle$

Let's consider also state $|\psi\rangle$ being a linear combination of all basis states:

$$|\psi\rangle \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = H^{\otimes n}|0^{\otimes n}\rangle \quad (4)$$

We have

$$|\psi\rangle = \frac{1}{\sqrt{N}}\left(\sum_{x\neq w}|x\rangle + |w\rangle\right) = \frac{1}{\sqrt{N}}\sum_{x\neq w}|x\rangle + \frac{1}{\sqrt{N}}|w\rangle =$$

$$= \left\{ \text{from (3): } \sum_{x\neq w}|x\rangle = \sqrt{N-1}\,|\alpha\rangle \right\} = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|w\rangle =$$

$$= \sqrt{1-\frac{1}{N}}\,|\alpha\rangle + \sqrt{\frac{1}{N}}\,|w\rangle \qquad (5)$$

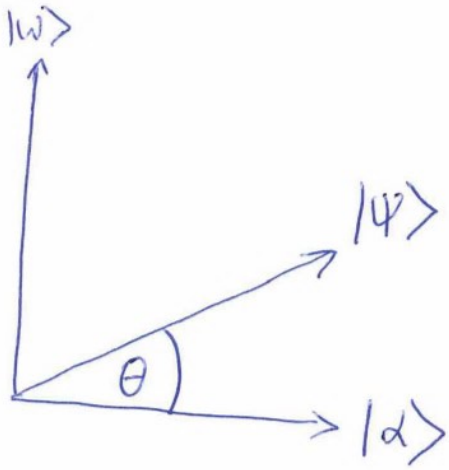
Now by analogy to $\sin\theta$ and $\cos\theta$):

$$\sin^2\theta + \cos^2\theta = 1 \Rightarrow \sqrt{1-\sin^2\theta} = \sqrt{\cos^2\theta} \qquad (6)$$

We see, that there is always such θ, that

$$\boxed{|\psi\rangle = \cos\theta\,|\alpha\rangle + \sin\theta\,|w\rangle}$$

Graphically:



$\boxed{\sin\theta = \frac{1}{\sqrt{N}}}$ => for large N, θ is small

If we have state $|\psi\rangle$ let's see what effect has acting on it with oracle operator $\hat{O}$:

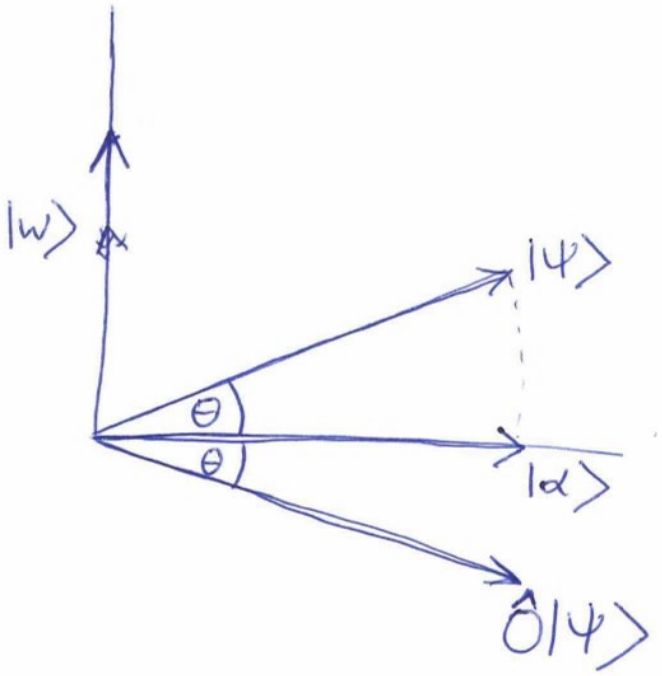
$$\hat{O}|\psi\rangle = \hat{O}\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \frac{1}{\sqrt{N}}\hat{O}\left(|x_0\rangle + |x_1\rangle + \dots |w\rangle + \dots |x_{N-1}\rangle\right)$$

$$= \frac{1}{\sqrt{N}}\left(\hat{O}|x_0\rangle + \hat{O}|x_1\rangle + \dots \hat{O}|w\rangle + \dots + \hat{O}|x_{N-1}\rangle\right) =$$

$$= \left\{\begin{array}{l}\text{based on (2)}\\ \text{and (1)}\end{array}\right\} = \frac{1}{\sqrt{N}}\left(|x_0\rangle + |x_1\rangle + \dots \boxed{-|w\rangle} + \dots + |x_{N-1}\rangle\right)$$

$$\Downarrow$$

$\hat{O}|\psi\rangle$ does not change any of the amplitudes except the one of $|w\rangle$ which is flipped

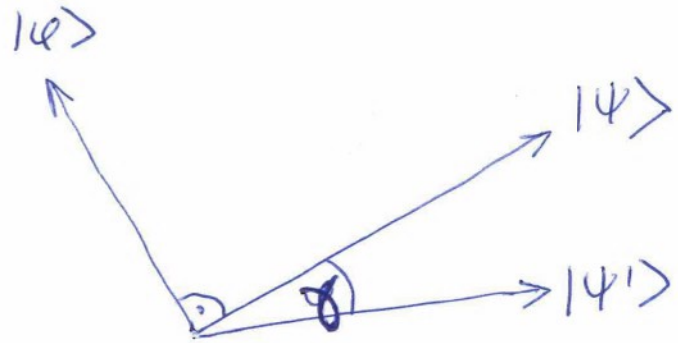


Now, let's consider the following operator:

$$\hat{D} \equiv 2|\psi\rangle\langle\psi| - \underline{1\!\!1}$$

Reflection operator (or diffuser)

and consider following states in our Hilbert space:



where $|\varphi\rangle$ is state orthogonal to $|\psi\rangle$ and so $|\varphi\rangle$ and $|\psi\rangle$ project a hyperplane which means they are basis states for any other state on this plane. For example state $|\psi'\rangle$ can be expressed as:

$$|\psi'\rangle = \eta_1|\psi\rangle + \eta_2|\varphi\rangle$$

↓

Now, let's act with operator $\hat{D}$ on state $|\psi'\rangle$:

$$\hat{D}|\psi'\rangle = \hat{D}(\eta_1|\psi\rangle + \eta_2|\varphi\rangle) =$$

$$= (2|\psi\rangle\langle\psi| - \mathbb{1})(\eta_1|\psi\rangle + \eta_2|\varphi\rangle) =$$

$$= 2\eta_1|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{=1} + 2\eta_2|\psi\rangle\underbrace{\langle\psi|\varphi\rangle}_{=0} - \eta_1|\psi\rangle - \eta_2|\varphi\rangle$$

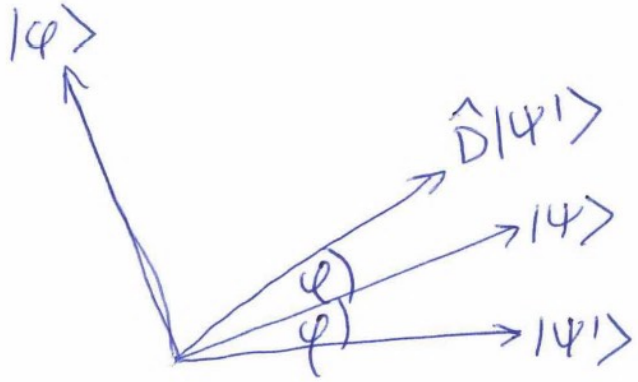
($=0$ based on definition of $|\varphi\rangle$)

$$= 2\eta_1|\psi\rangle - \eta_1|\psi\rangle - \eta_2|\varphi\rangle =$$

$$= \eta_1|\psi\rangle - \eta_2|\varphi\rangle$$

$\Downarrow$

$\hat{D}$ flips the „$|\varphi\rangle$ coordinate" of any state to opposite one:



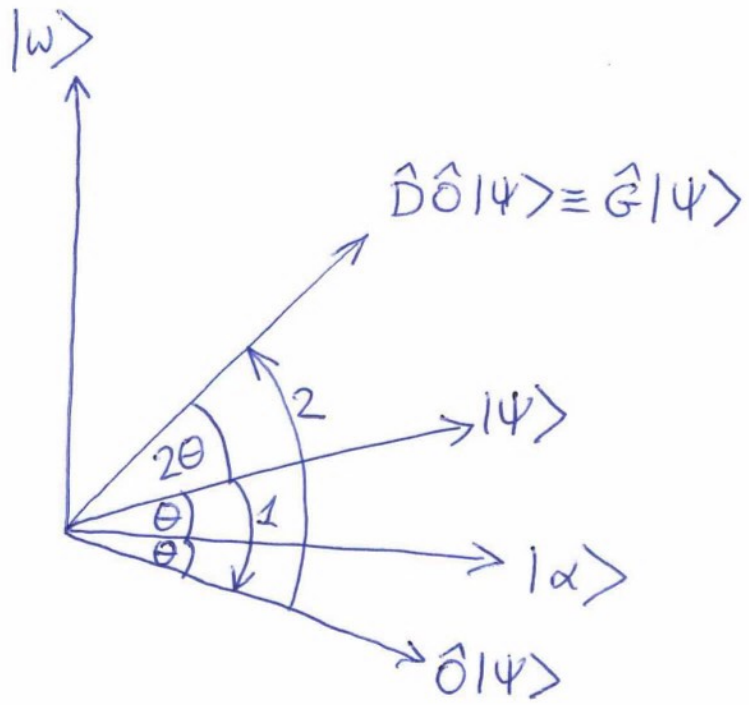
Now, our final Grover operator is defined as:

$$\hat{G} \equiv \underbrace{(2|\psi\rangle\langle\psi| - \mathbb{1})}_{\hat{D}}\hat{O}$$

or

$$\hat{G} \equiv \hat{D}\hat{O}$$

and it's effect can be graphically represented as:



- we only know $|\psi\rangle$ at the beginning (superposition of all states - H gates on all qubits), and have operator $\hat{O}$
- $\hat{D}$ is a constant operator, not depending on the problem

- having just this, we can perform operations ($\hat{O}$ and $\hat{D}$, so effectively $\hat{G}$) moving initial state $|\psi\rangle$ to state $\hat{G}|\psi\rangle$ which we know is closer to our searched state $|w\rangle$
- being „closer" to $|w\rangle$ means, that when we measure the state we will have bigger probability of getting $|w\rangle$ as the result.
- now, we can perform Grover operation $\hat{G}$ multiple times getting us closer and closer to $|w\rangle$

How many times should we apply Grover operator?

- one application of $\hat{G}$ rotates our state by 2θ in direction of $|w\rangle$
- from (5) and (6) we see, that

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

- for large N, $\frac{1}{\sqrt{N}}$ is small, which means, that ↓

$$\sin\theta \approx \theta$$

$$\Downarrow$$

$$\theta \approx \frac{1}{\sqrt{N}} \quad / \cdot 2\sqrt{N}$$

$$2\theta \cdot \sqrt{N} \approx 2$$

let's assume, that we need to rotate by $\frac{\pi}{2}$:

as $|\psi\rangle = \cos\theta|\alpha\rangle + \sin\theta|w\rangle$
we want $|\psi\rangle = |w\rangle$
$\cos\theta = 0 \Rightarrow \theta = \frac{\pi}{2}$

$$2\theta \cdot \sqrt{N} \approx 2 \quad / \cdot \frac{\pi}{4}$$

$$\frac{\pi\sqrt{N}}{4} \cdot \underbrace{2\theta}_{\text{rotation in one iteration}} \approx \underbrace{\frac{\pi}{2}}_{\text{total rotation angle}}$$

$\frac{\pi\sqrt{N}}{4}$: number of iterations

$$\Downarrow$$

We need approximately

$$\boxed{\frac{\pi}{4}\sqrt{N} \text{ iterations}}$$

to align our initial state $|\psi\rangle$ with $|w\rangle$ which we look for.

$$\downarrow$$

This means we need $O(\sqrt{N})$ calls to our oracle $\hat{O}$ (and so function $f(x)$)

$$\Downarrow$$

$O(N)$ classically $\longrightarrow$ $O(\sqrt{N})$ with Grover algorithm

- accounting for quantum gates, the total number of operations is $\approx \sqrt{N} \ln N$
- it can be shown, that Grover algorithm is optimal

Summary:

$$|0\rangle^{\otimes n} \longrightarrow H^{\otimes n} \longrightarrow \underbrace{\hat{D}\hat{O} \rightarrow \hat{D}\hat{O} \rightarrow \ldots \rightarrow \hat{D}\hat{O}}_{\sim \frac{\pi}{4}\sqrt{N} \text{ times}} \longrightarrow \text{measure}^{\otimes n}$$

$$\hat{O}|x\rangle \equiv (-1)^{f(x)}|x\rangle$$

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

$$\hat{D} \equiv 2|\psi\rangle\langle\psi| + \mathbb{1}$$

$$|\psi\rangle \equiv \frac{1}{\sqrt{N}} \sum^{N-1} |x\rangle = H^{\otimes n}|0^{\otimes n}\rangle$$

Grover algorithm example on 3 qubits

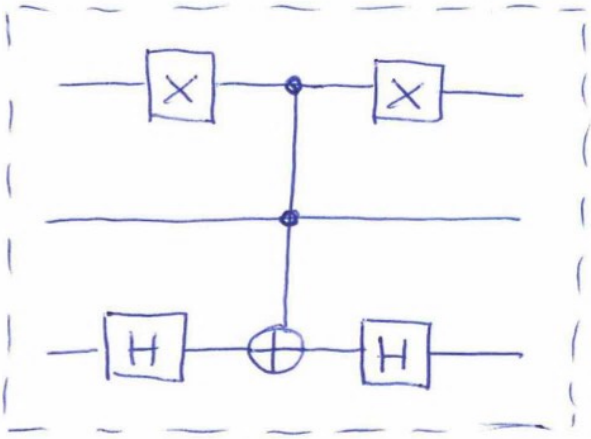
3 qubits can represent 8 states:

$$|000\rangle, |001\rangle, |010\rangle, \ldots, |111\rangle$$

Let's choose for our winner $|w\rangle$ the following state:

$$|w\rangle \equiv |110\rangle = |6\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

How to construct Oracle?

$\hat{O} =$ 

→ it can be proven experimentally :)

where

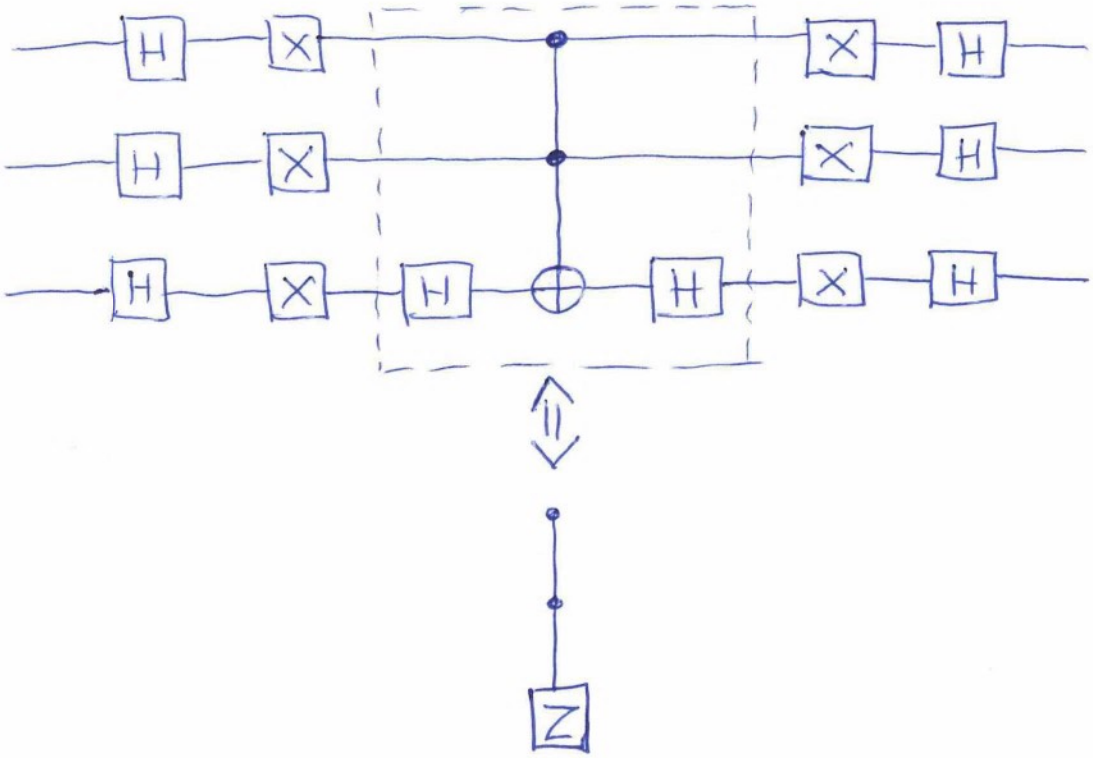
is so called Toffoli gate, which is a CNOT but with one additional control qubit

↓

Toffoli gate flips last qubit only if first two are $|1\rangle$

Now, how to construct diffuser?

$\hat{D} =$



- the diffuser is fixed, not dependent on the problem