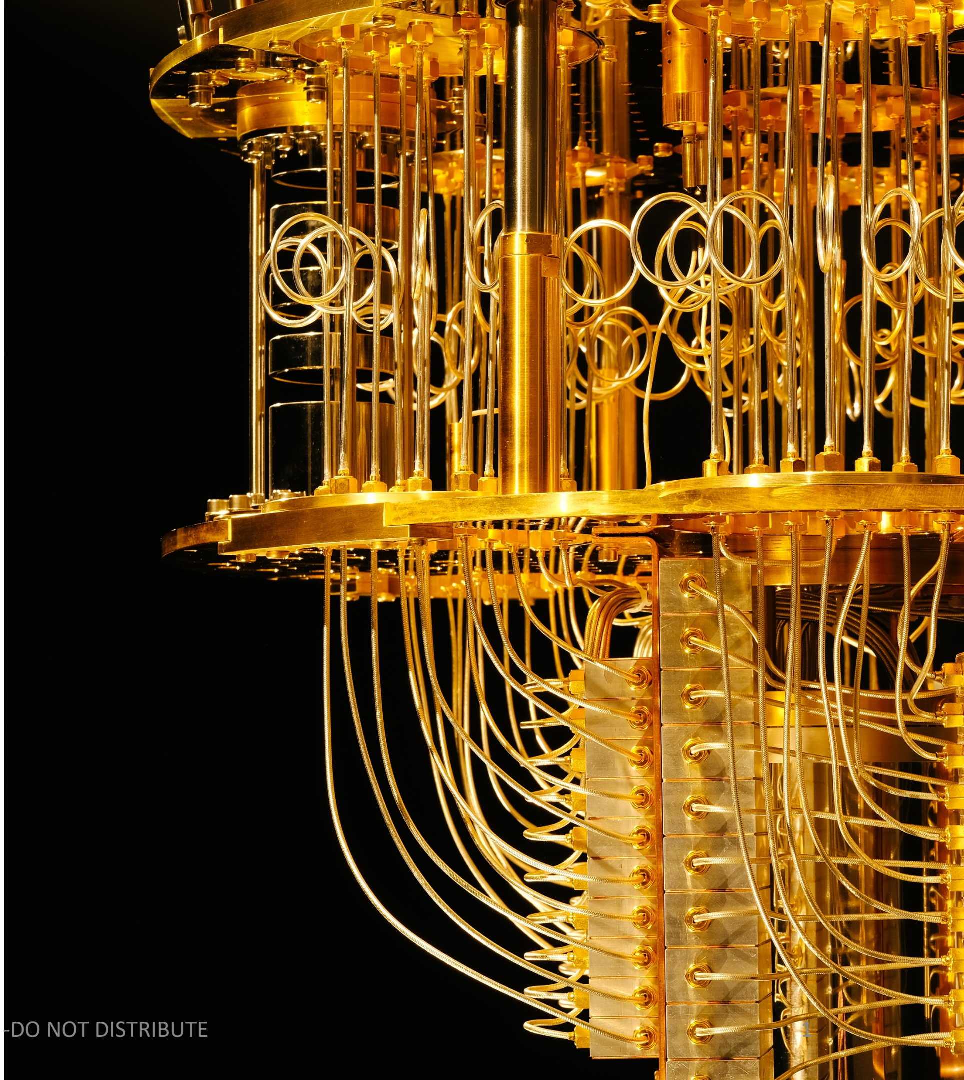
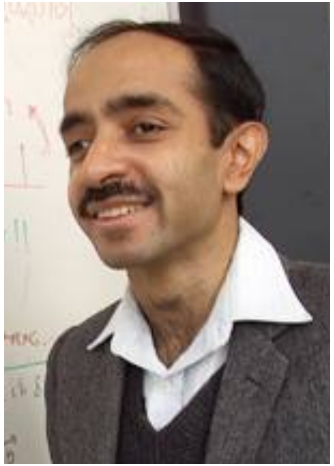
An Introduction to Grover's Search Algorithm

M. Grossi – IBM Quantum

In collaboration with F. Tramonto



Grover’s Search Algorithm

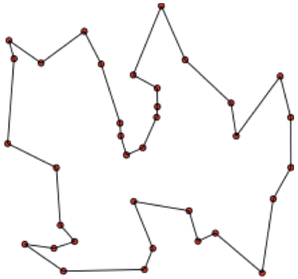


Lov Grover

Applications

- Searches in a non–ordered list
    - Example: Search a phone book for a specifc number

- Travelling salesman problem (TSP)



Speedup?

Classical search: $O(N)$ steps

Grover’s Algorithm search: $O(\sqrt{N})$ steps

The problem

Given a boolean function $f(x)$

$$f(x):\ \{0,1\}^n \rightarrow \{0,1\}, \qquad f(x) = \begin{cases} 1, & \text{if } x = x^* \\ 0, & \text{if } x \neq x^* \end{cases}$$

find the value of x such that $f(x) = 1$, that is find x^*.

A remind: $\mathrm{x} \in \{0,1\}^n \leftrightarrow \mathrm{x} = 0, 1, 2, \ldots N - 1$ in binary with $N = 2^n$ (i.e. $n = \log_2 N$)

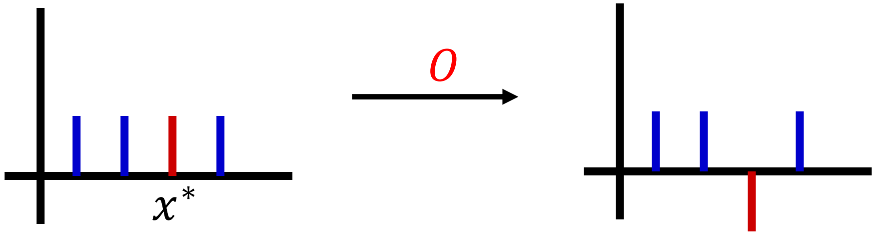
Classically: worst case → N steps

on average → $N/2$ steps $\Longrightarrow \mathrm{O}(N)$ steps

The idea…

Step 0) Initial state: equal superpostion of the $N = 2^n$ basis states $|0\rangle, |1\rangle, |2\rangle, \dots |N-1\rangle$

equal amplitudes

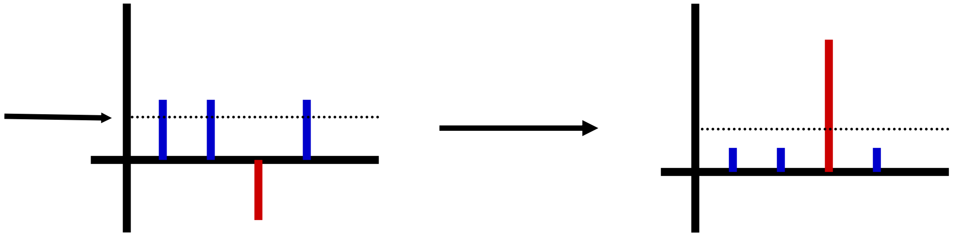


Step 1)
A *black box* operator, the Oracle O marks $|x^*\rangle$ with a minus sign

If we measure now ⟶ equal probability for all states

$\Longrightarrow$ we have to amplify $|x^*\rangle$ to have higher probability. How?

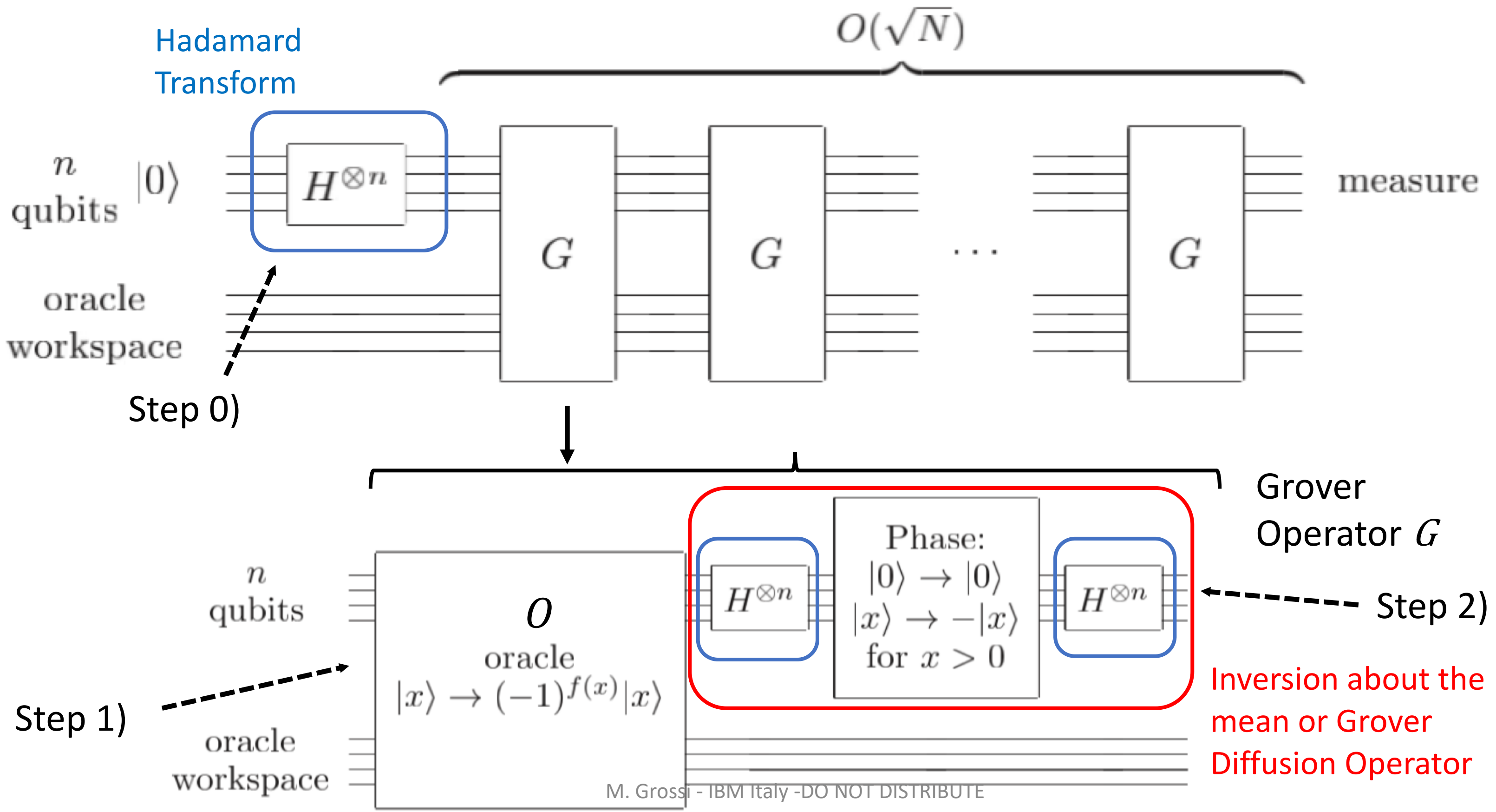
average of all amplitudes



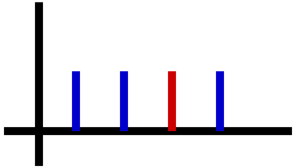
Step 2)
Inversion about the mean

Repeat step 1) and 2) M times

Schematic Circuit



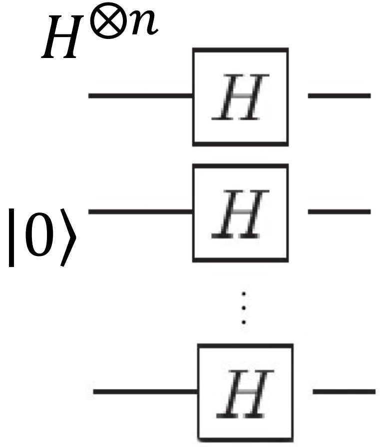
Hadamard Transform



Step 0) Prepare all the basis states with equal amplitude, by applying the

Hadamard transform to the initial state $|0\rangle = |000\ldots0\rangle = |0\rangle^{\otimes n}$

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{N-1}|x\rangle \equiv |\psi_0\rangle$$



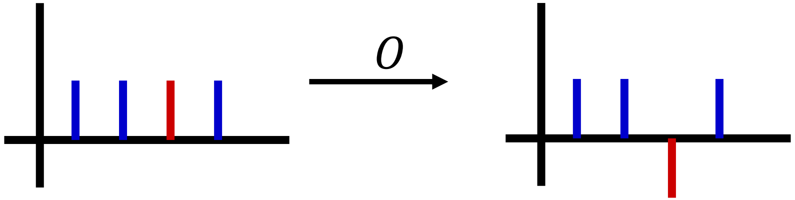
$$H^{\otimes n}|0\rangle = (H|0\rangle)^{\otimes n} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{N-1}|x\rangle$$

Example with 2 qubits:

$$H^{\otimes 2}|00\rangle = (H|0\rangle)\otimes(H|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =$$

$$= \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2^2}}\,(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

The Oracle



Oracle operator O associated to the function $f(x)$ *marks* the state $|x^*\rangle$ with a minus

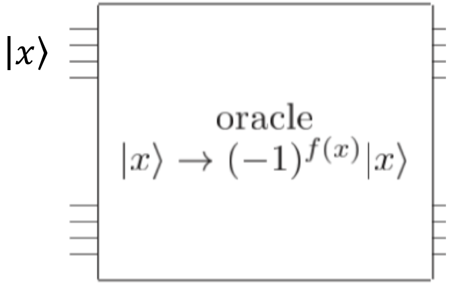
$$O|x^*\rangle = -|x^*\rangle$$

and leaves the other states unchanged

$$O|x\rangle = |x\rangle \quad \text{if } x \neq x^*$$

or more compactly

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



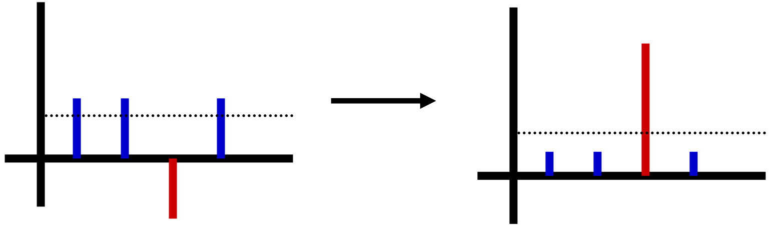
How? A way is by using an Oracle operator that exploits an ancilla qubit defined as

ancilla qubit

$$|x\rangle|a\rangle \xrightarrow{O} |x\rangle|a \oplus f(x)\rangle$$

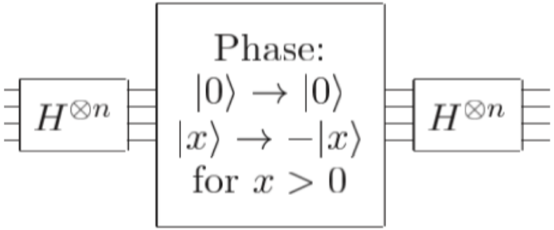
$$|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{O} |x\rangle \begin{cases} \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle), & \text{if } f(x) = 1 \ (x = x^*) \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \text{if } f(x) = 0 \ (x \neq x^*) \end{cases} = (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Inversion around the mean (or Grover diffusion)



3 steps:

1) Hadamard Transform $H^{\otimes n}$
2) Conditional phase shift: $|x\rangle \rightarrow -(-1)^{\delta_{x,0}}|x\rangle$
3) Hadamard Transform $H^{\otimes n}$



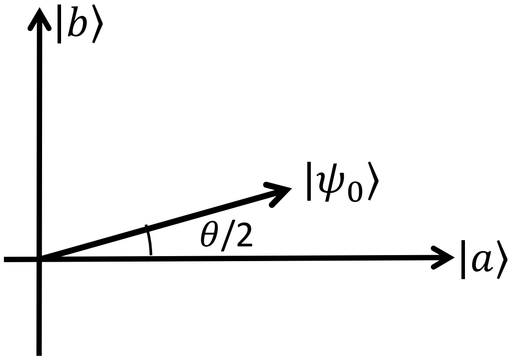
step 2: the operator $2|0\rangle\langle 0| - I$ → applied to $|0\rangle$ it gives $|0\rangle$

and to $|x\rangle$ it gives $-|x\rangle$, if $x \neq 0$

Combining all 3 steps: $H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi_0\rangle\langle\psi_0| - I$

With the Oracle → the Grover operator $\mathrm{G} \equiv (2|\psi_0\rangle\langle\psi_0| - I)O$

Geometric representation



$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{x, f(x)=0} |x\rangle$ sum of states that aren't solution

$|b\rangle = \frac{1}{\sqrt{M}} \sum_{x, f(x)=1} |x\rangle$ sum of states that are solution

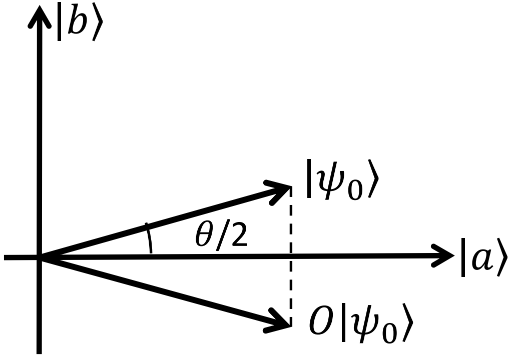
$|a\rangle$ and $|b\rangle$ generate a 2-dimensional subspace S and $|\psi_0\rangle$ belong to S :

$$|\psi_0\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle$$

$$|\psi_0\rangle = \cos\frac{\theta}{2}|a\rangle + \sin\frac{\theta}{2}|b\rangle$$

If apply O to a state of S:

$$O(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta|b\rangle$$



the sign of the $|b\rangle$ component changes

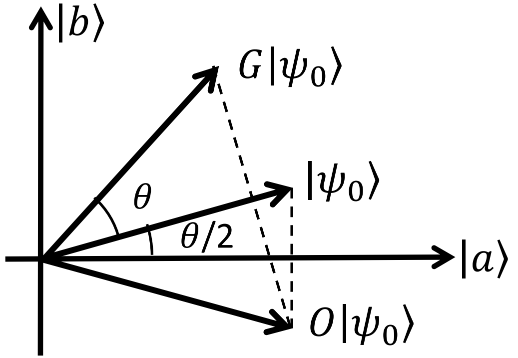
Geometric representation 2

By applying G $G|\psi_0\rangle$ goes to an angle $\left(\frac{\theta}{2}+\theta\right)$ respect to $|a\rangle$

at each iteration G add an angle θ :

$$G|\psi_0\rangle = \cos\left(\frac{\theta}{2}+\theta\right)|a\rangle + \sin\left(\frac{\theta}{2}+\theta\right)|b\rangle$$

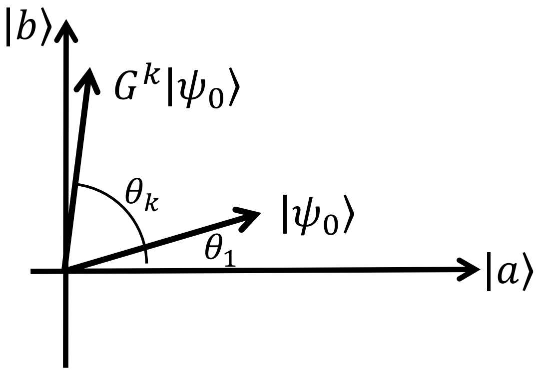
$$G^k|\psi_0\rangle = \cos\theta_k\,|a\rangle + \sin\theta_k\,|b\rangle, \qquad \theta_k = \left(k+\tfrac{1}{2}\right)\theta$$



When stop the iterations?

Nearer possible to $|b\rangle$ $\longrightarrow \theta_k \simeq \frac{\pi}{2}$ $\longrightarrow k \simeq \frac{1}{2}\left(\frac{\pi}{\theta}-1\right)$

$$\longrightarrow \quad k = \mathrm{CI}\left[\frac{1}{2}\left(\frac{\pi}{\theta}-1\right)\right] = O\left(\sqrt{N/M}\right)$$



For calculation details see, for example,

Nielsen, Chuang – *Quantum Computation and Quantum Information*

Now let's apply the algorithm…

2. Example: 2 Qubits

Let's first have a look at the case of Grover's algorithm for $N = 4$ which is realized with 2 qubits. In this particular case, only **one rotation** is required to rotate the initial state $|s\rangle$ to the winner $|w\rangle$[3]:

1. Following the above introduction, in the case $N = 4$ we have

$$\theta = \arcsin \frac{1}{2} = \frac{\pi}{6}.$$

2. After t steps, we have

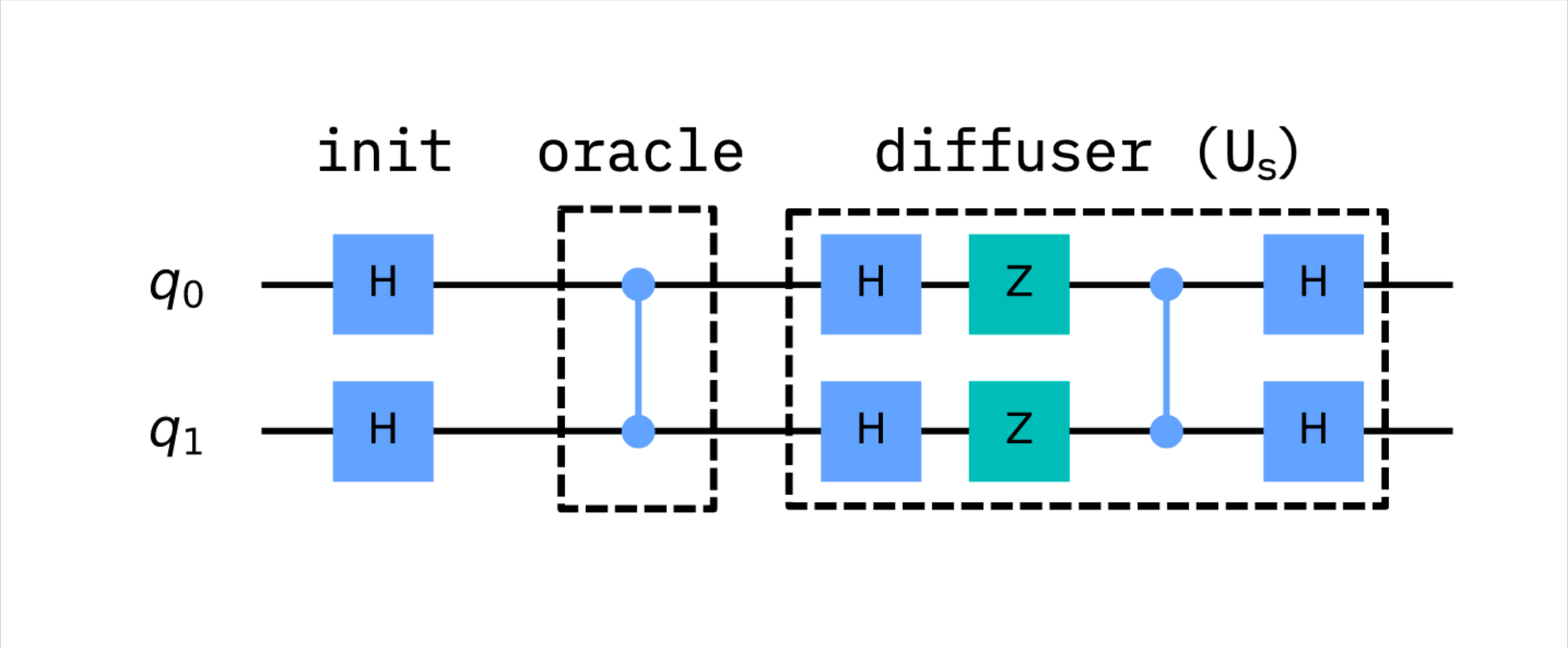
$$(U_s U_\omega)^t |s\rangle = \sin \theta_t |\omega\rangle + \cos \theta_t |s'\rangle,$$

where

$$\theta_t = (2t + 1)\theta.$$

3. In order to obtain $|\omega\rangle$ we need $\theta_t = \frac{\pi}{2}$, which with $\theta = \frac{\pi}{6}$ inserted above results to $t = 1$. This implies that after $t = 1$ rotation the searched element is found.

Example: 2 Qubits



$$|x\rangle|a\rangle \xrightarrow{O} |x\rangle|a \oplus f(x)\rangle$$

If $|a\rangle = |0\rangle$

$$|x\rangle|0\rangle \xrightarrow{O} |x\rangle|f(x)\rangle = |x\rangle \begin{cases} |1\rangle, & \text{if } f(x) = 1 \ (x = x^*) \\ |0\rangle, & \text{if } f(x) = 0 \ (x \neq x^*) \end{cases}$$

If $|a\rangle = |1\rangle$

$$|x\rangle|1\rangle \xrightarrow{O} |x\rangle|1 \oplus f(x)\rangle = |x\rangle \begin{cases} |0\rangle, & \text{if } f(x) = 1 \ (x = x^*) \\ |1\rangle, & \text{if } f(x) = 0 \ (x \neq x^*) \end{cases}$$

If $|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{O} |x\rangle \begin{cases} \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle), & \text{if } f(x) = 1 \ (x = x^*) \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \text{if } f(x) = 0 \ (x \neq x^*) \end{cases} = (-1)^{f(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$