GROVER'S ALGORITHM

Solves the problem of "unstructured search" in the "black-box query model"

UNSTRUCTURED SEARCH PROBLEM:

Given database $X = \{x_1, x_2 \dots x_N\}$

and $f : X \to \{0,1\}$

find $x \in X$ satisfying $f(x) = 1$.

BLACK-BOX QUERY MODEL:

Algorithm only accesses f via input/output queries

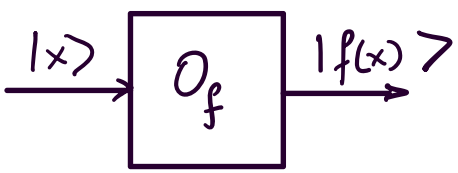
Doesn't rely on any details of circuit implementing f.

Q: How many queries to f will solve unstructured search?

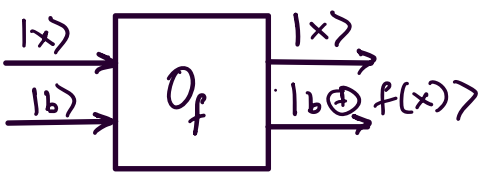
A: Classically, need N queries worst case.

Quantumly, only need $O(\sqrt{N})$ queries!

SETTING:



not reversible



reversible implementation

"PHASE KICKBACK"

Given access to O_f, implement $|x\rangle \to (-1)^{f(x)}|x\rangle$

Query O_f on $|x\rangle \otimes |-\rangle$

$$= |x0\rangle - |x1\rangle$$

$$O_f(|x0\rangle - |x1\rangle) = |x\, f(x)\rangle - |x\, \overline{f(x)}\rangle$$

$$= |x0\rangle - |x1\rangle = |x\rangle \otimes |-\rangle \quad \text{if } f(x)=0$$

$$= |x1\rangle - |x0\rangle = -|x\rangle \otimes |-\rangle \quad \text{if } f(x)=1$$

$$O_f(|x\rangle \otimes |-\rangle) \longrightarrow (-1)^{f(x)}|x\rangle \otimes |-\rangle$$

Assume gate $O_{f\pm} : |x\rangle \longrightarrow (-1)^{f(x)}|x\rangle$

GROVER SEARCH :

Simplifying assumption : $\exists$ unique x^* s.t. $f(x)=0$ if $x=x^*$, $=1$ otherwise

and $N = 2^n$

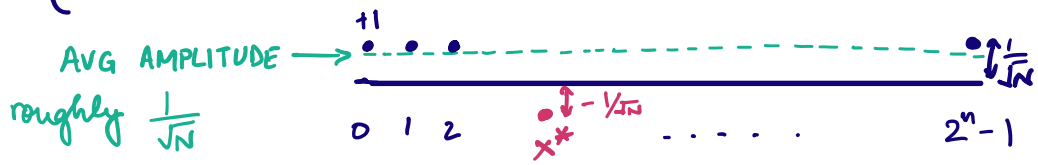
General strategy to build Quantum algorithms

① Prepare a uniform superposition of inputs

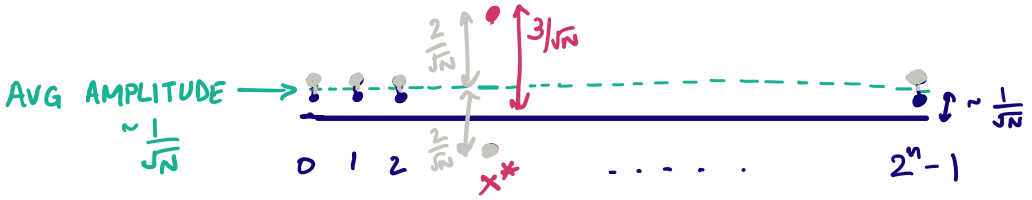
Apply $H^{\otimes n}|0^n\rangle \longrightarrow \sum_{x\in\{0,1\}^n} |x\rangle$

② Query the function in superposition

$$O_{f\pm}\left(\sum_{x\in\{0,1\}^n} |x\rangle\right) \longrightarrow \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$$

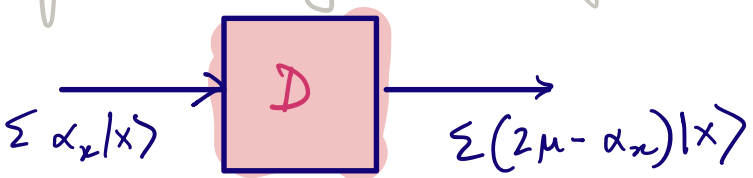


③ Flip amplitudes about the average



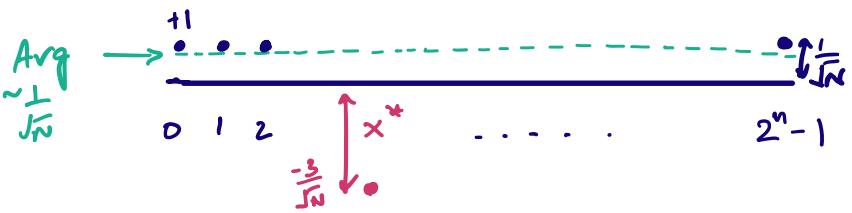
The state is roughly: $|\psi_1\rangle \approx \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (2f(x)+1)|x\rangle$

[Our goal is to bring it to roughly $|x^*\rangle$]

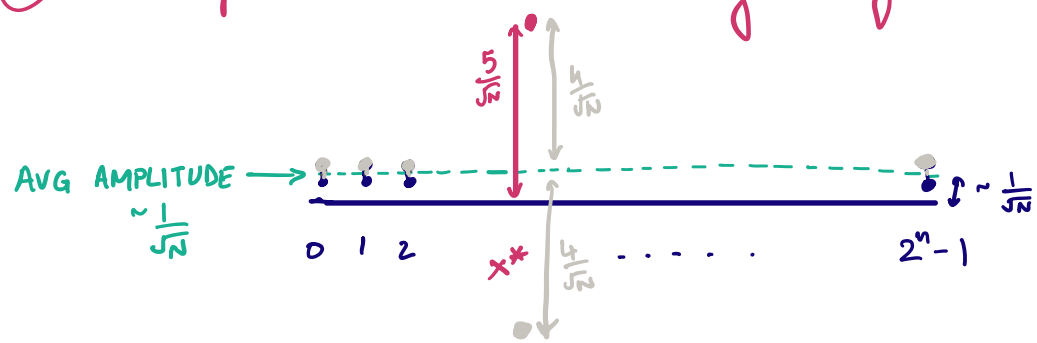


(4) Query the function again, on $|\psi_1\rangle$

$$O_{f\pm}\left(\sum_{x\in\{0,1\}^n}(2f(x)+1)|x\rangle\right) \longrightarrow \sum_{x\in\{0,1\}^n}(-1)^{f(x)}(2f(x)+1)|x\rangle$$



(5) Flip around the average again



Repeat $O(\sqrt{N})$ times : a) Query $O_{f\pm}$

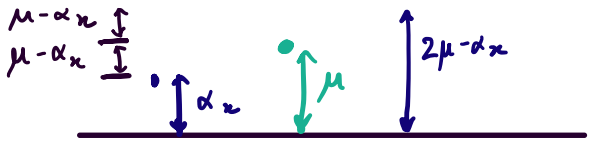
b) Flip around the average

Roughly, each time amplitude on x^* ↑ by $> \frac{1}{\sqrt{N}}$

After sufficiently many tries, amplitude on $x^* \sim 1$.

IMPLEMENTING D:

Goal:



Convert $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \longrightarrow \sum_{x\in\{0,1\}^n} (2\mu-\alpha_x)|x\rangle$

Is there a unitary that achieves this?

$-\mathbb{I}\left(\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\right) \longrightarrow -\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$

$\langle +^n| = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} \langle x|$

$\langle +^n| \left(\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\right) \longmapsto \frac{\sum_{x\in\{0,1\}^n} \alpha_x}{\sqrt{N}} = \frac{\mu N}{\sqrt{N}} = \mu\sqrt{N}$

$2|+^n\rangle\left(\langle +^n| \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\right) \longmapsto 2\left(\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle\right) \mu\sqrt{N}$

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

$\left(2|+^n\rangle\langle +^n| - \mathbb{I}\right)\left(\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\right) \longmapsto \sum_{x\in\{0,1\}^n} 2\mu-\alpha_x |x\rangle$

D: efficient unitary implementation?

Let $Z_0 = 2|0^n\rangle\langle 0^n| - I$

What does this do?

$Z_0|x\rangle = 2|0^n\rangle\langle 0^n|x\rangle - |x\rangle$

When $|x\rangle = |0^n\rangle$, then $Z_0|x\rangle = |0^n\rangle = |x\rangle$

When $|x\rangle \neq |0^n\rangle$, then $Z_0|x\rangle = -|x\rangle$

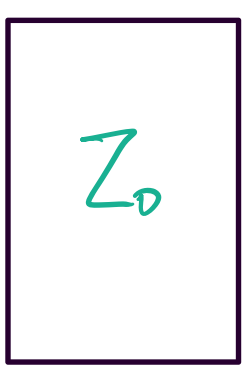
So Z_0 does nothing when $x = 0^n$
and flips the phase whenever $x \neq 0^n$.

There is a classical circuit for this:

Output x if $OR(x_1, x_2 \ldots, x_n) = 0$

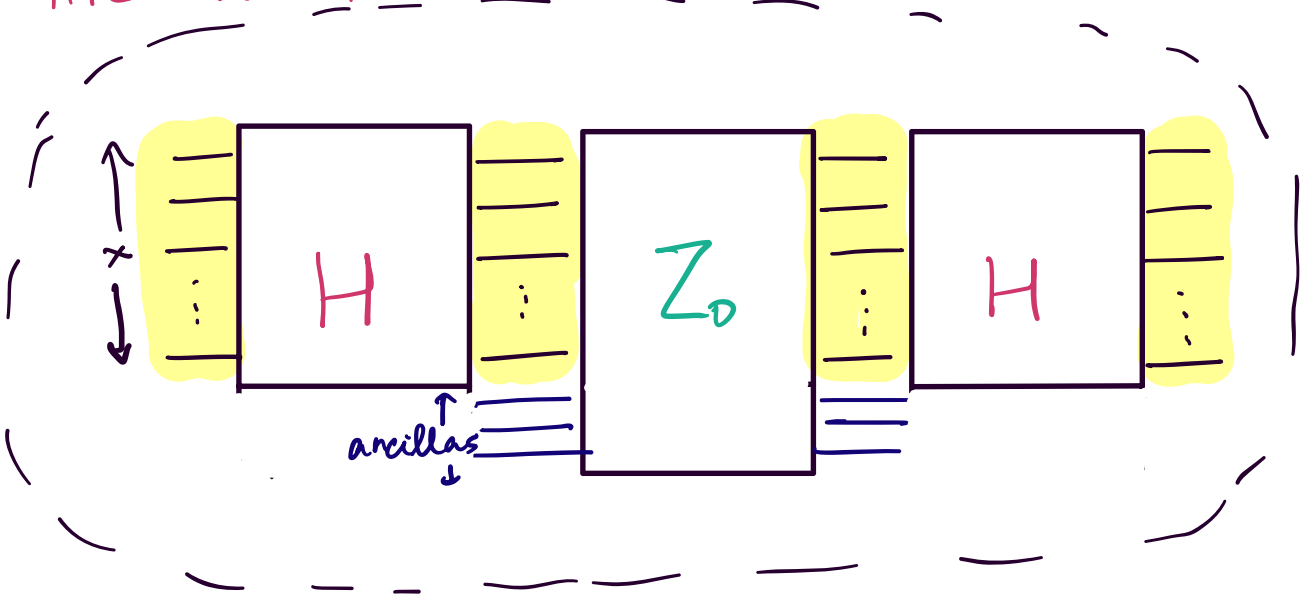
$-x$ otherwise

You already know to convert this to reversible quantum circuit



$\otimes$ is same as Z_0, except in Hadamard basis,
i.e. do nothing when $x = |+^n\rangle$
and flip phase on all other Had. basis states

THE $\otimes$ GATE



Let us check

$$H^{\otimes n} Z_0 H^{\otimes n}$$

$$= H^{\otimes n} \left(2|0^n\rangle\langle 0^n| - \mathbb{I}\right) H^{\otimes n}$$

$$= \left(2 H^{\otimes n}|0^n\rangle\langle 0^n| - H^{\otimes n}\right) H^{\otimes n}$$

$$= 2|+^n\rangle\langle +^n| - \mathbb{I}$$

How many iterations ?

In each step, apply $O_{f\pm}$ followed by D.

Let $\alpha^{(t)}$ = Amplitude on x^* after t^{th} step

$\beta^{(t)}$ = Amplitude on $x \neq x^*$ after t^{th} step

$\mu^{(t)}$ = Avg amplitude after $O_{f\pm}$ in t^{th} step

$$= -\alpha^{(t)} + \frac{N-1}{N}\beta^{(t)}$$

$$\alpha^{(0)} = \beta^{(0)} = \frac{1}{\sqrt{N}}$$

After $O_{f\pm}$, x^* has amplitude $\left(\frac{-1}{\sqrt{N}}\right)$

Avg. amplitude $\mu^{(1)} = \frac{1}{N}\left(\frac{N-1}{\sqrt{N}} + \frac{(-1)}{\sqrt{N}}\right) = \frac{N-2}{N\sqrt{N}}$

After D, x^* has amplitude $2\mu^{(1)} - \left(\frac{-1}{\sqrt{N}}\right)$

$$\alpha^{(1)} = 2\mu^{(1)} + \alpha^{(0)}$$

CLAIM 1:

For any t, $a^{(t+1)} \leq \alpha^{(t)} + \frac{2}{\sqrt{N}}$

Proof

Since Sum of squares of amplitudes $= 1$

$$\Rightarrow (N-1)\left(\beta^{(t)}\right)^2 \leq 1 \Rightarrow \beta^{(t)} \leq \frac{1}{\sqrt{N-1}}$$

$$\mu^{(t)} = \alpha^{(t)} + \frac{N-1}{N}\beta^{(t)} \leq \frac{N-1}{N}\beta^{(t)} = \frac{\sqrt{N-1}}{N}$$

$$\alpha^{(t+1)} = 2\mu^{(t)} + \alpha^{(t)}$$

$$= \frac{2\sqrt{N-1}}{N} + \alpha^{(t)}$$

$$\leq \frac{2}{\sqrt{N}} + \alpha^{(t)}$$

CLAIM 2:

Suppose $\alpha^{(t)} \leq \frac{1}{2}$, $N \geq 4$.

Then, $\alpha^{(t+1)} \geq \alpha^{(t)} + \frac{1}{\sqrt{N}}$

Proof. Since sum of squares of amplitudes is 1,

$$\left(\alpha^{(t)}\right)^2 + (N-1)\left(\beta^{(t)}\right)^2 = 1$$

$$\left(\beta^{(t)}\right)^2 = \frac{1-\left(\alpha^{(t)}\right)^2}{N-1} \geq \frac{3}{4(N-1)}$$

$$\mu^{(t)} = \frac{-\alpha^{(t)}}{N} + \frac{(N-1)}{N}\beta^{(t)}$$

$$\geq -\frac{1}{2N} + \left(\frac{N-1}{N}\right)\sqrt{\frac{3}{4(N-1)}}$$

$$\geq -\frac{1}{2N} + \frac{\sqrt{N-1}}{2N}\cdot\sqrt{3} \geq \frac{1}{2\sqrt{N}} \quad \text{for } N \geq 4$$

$$\alpha^{(t+1)} = 2\mu^{(t)} + \alpha^{(t)} \geq \frac{1}{\sqrt{N}} + \alpha^{(t)}$$

Claims 1 and 2 together tell us that for $\alpha^{(t)} \leq \frac{1}{2}$, $N > 4$,

$$\frac{1}{\sqrt{N}} + \alpha^{(t)} \leq \alpha^{(t+1)} \leq \frac{2}{\sqrt{N}} + \alpha^{(t)}$$

$\alpha^{(0)} = \frac{1}{\sqrt{N}}$. For $t \leq \frac{\sqrt{N}}{8}$, by

$$\alpha^{(t+1)} \leq \frac{2}{\sqrt{N}} \cdot \frac{\sqrt{N}}{8} + \alpha_0$$

$$\leq \frac{1}{\sqrt{N}} + \frac{1}{4} < \frac{1}{2}$$

So, $\alpha^{(t+1)} \geq \alpha^{(t)} + \frac{1}{\sqrt{N}}$ for $t \leq \frac{\sqrt{N}}{8}$

$$\Rightarrow \alpha^{(\sqrt{N}/8)} \geq \frac{1}{\sqrt{N}} \cdot \frac{\sqrt{N}}{8} > \frac{1}{8}$$

So, measuring in computational basis after $\frac{\sqrt{N}}{8}$ steps gives 0.125 prob. of finding x^*.

Repeat 100 times!