Grover's Algorithm

$N = 2^n$ bit strings length n

Consider

$$f(x) = 0 \text{ for all but one input}$$
$$= 1 \text{ for the special input } x^*$$

$$f: \{0,1\}^n \to \{0,1\}$$

Find secret x^*

Unstructured search - No particular ordering of the domain
If $f(x)=0$ no info is given about where to look next

Examples
- Needle in hay stack
- Linux pw
- Setting of n switches combo lock

Classically takes $O(N)$ queries

$$x \longrightarrow \boxed{\begin{matrix} O_f \\ \text{oracle} \\ f \end{matrix}} \longrightarrow 0 \text{ or } 1$$

We assume each takes constant time

Example
Linux pw

$g(x)$ one-way
find private $x \mid g(x) = y$
public

$$f(x) = 1 \quad \text{if } g(x) = y$$
$$= 0 \quad \text{otherwise}$$

Very general setting, like VQE

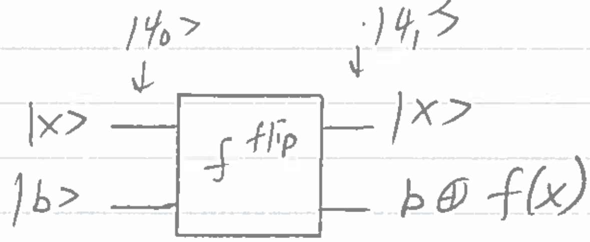
Grover's alg finds x^* with high prob using $\Theta(\sqrt{N})$ queries (iterations of a quantum process) and $O(\sqrt{N} \lg N)$ gates in the "unrolled" circuit

→ running time ~ $\sqrt{N}$

Note N is 2^n some power of 2
We view inputs an n-bit string
We assume only one x^* is valid as the secret

Makins O_f quantum gate

O_f is not reversible, so try



This can work

We want to "call out", distinguish $f(x^*)$

$$f(x) = 0 \quad \text{for almost all } x$$
$$= 1 \quad \text{for } x^*$$

Let's use the phase kickback idea to change the phase when $f(x) = 1$ and leave it alone when $f(x) = 0$

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

We've seen this trick before

Let $b = |-\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$

Input

$$|\psi_0\rangle = |x\rangle \otimes |-\rangle =$$

$$|x\rangle \otimes \tfrac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$\tfrac{1}{\sqrt{2}} (|x0\rangle - |x1\rangle)$$

Apply gate f^{flip}

$$|\psi_1\rangle = \tfrac{1}{\sqrt{2}} \left(|x\rangle|f(x)\rangle - |x\rangle|1-f(x)\rangle \right)$$

2 cases $f(x) = 0$

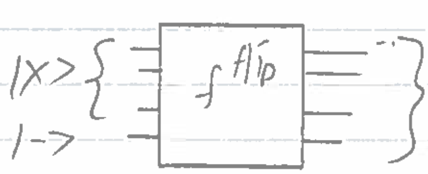
$$|\psi_1\rangle = \tfrac{1}{\sqrt{2}} (|x0\rangle - |x1\rangle) = |\psi_0\rangle$$

$$f(x) = 1$$

$$|\psi_1\rangle = \tfrac{1}{\sqrt{2}} (|x1\rangle - |x0\rangle)$$

$$= -|\psi_0\rangle$$

So $|\psi_1\rangle = (-1)^{f(x)} (|x\rangle \otimes |-\rangle)$

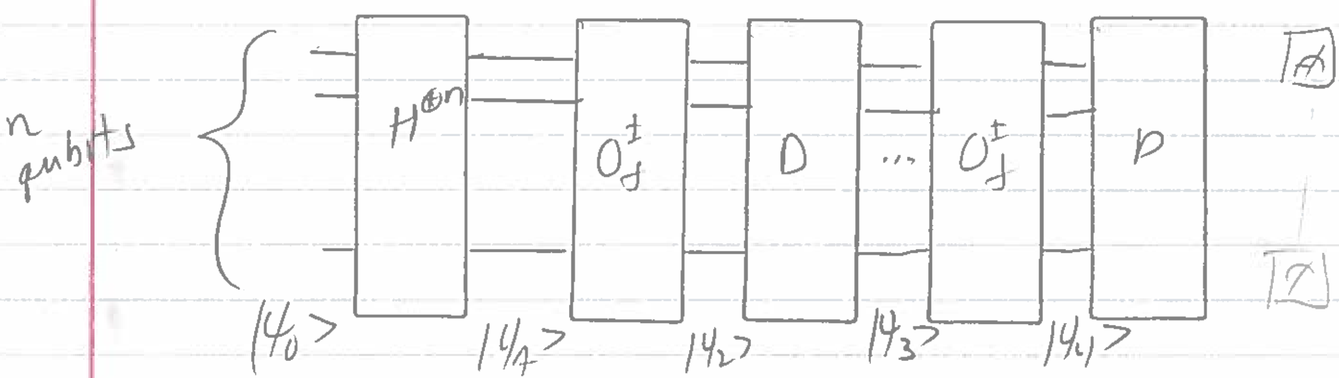


$$(-1)^{f(x)} \left[|x\rangle \otimes |-\rangle \right]$$

In concept we view this as

$$|x\rangle - \boxed{O_f^{\pm}} - (-1)^{f(x)}|x\rangle$$

the algorithm

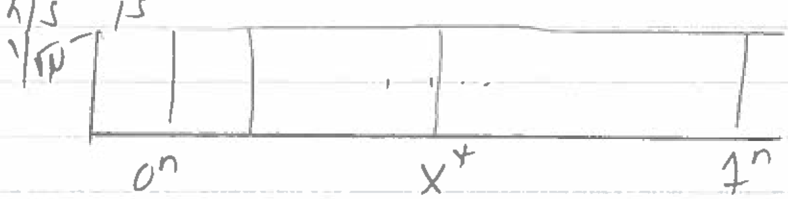


$$|\psi_0\rangle = |0^n\rangle$$

$$|\psi_1\rangle = \sum_x 1/\sqrt{N}\, |x\rangle \quad \text{as before}$$

uniform superposition of all $|x\rangle$

This is

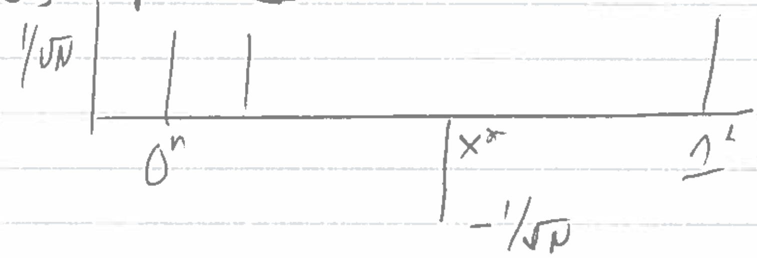


Define $\alpha^{(t)}$ amplitude of $|x^*\rangle$ at time t

$\beta^{(t)}$ amplitude of all other $|x\rangle$

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

$O_f^{\pm}$ produces



$$|\psi_2\rangle = -1/\sqrt{N}\,|x^*\rangle + \sum_{x \neq x^*} 1/\sqrt{N}\,|x\rangle$$

We need a way to "boost" the amplitude for x^*.

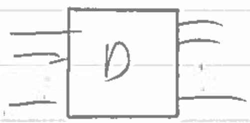
Consider the mean

$$\mu = \frac{(N-1)\,1/\sqrt{N} - 1/\sqrt{N}}{N}$$

$$= \frac{N-2}{\sqrt{N}} \Big/ N$$

N large $\approx \frac{N}{\sqrt{N}} \Big/ N = 1/\sqrt{N}$

We can make a gate D

$|\psi_2\rangle$  $|\psi_3\rangle$

$|\psi_2\rangle$ is $-1/\sqrt{N}\,|x^*\rangle + \sum\limits_{x \neq x^*} 1/\sqrt{N}\,|x\rangle$

Given input amplitude a
D produces amplitude $2\mu - a$

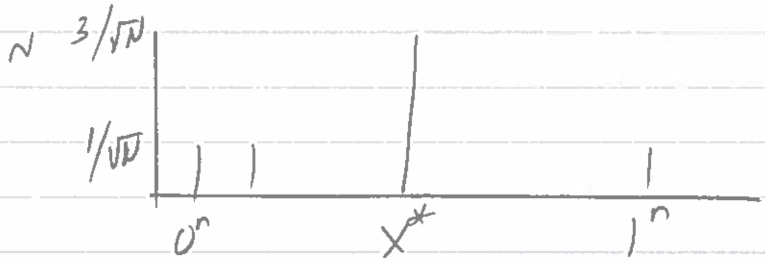
So $\mu = 1/\sqrt{N}$ the amplitude of x^*

$$-1/\sqrt{N} \rightarrow 2\,1/\sqrt{N} - -1/\sqrt{N}$$

$$\rightarrow 3/\sqrt{N}$$

All others

$$1/\sqrt{N} \rightarrow 2\,1/\sqrt{N} - 1/\sqrt{N} = 1/\sqrt{N}$$



Now

$$\alpha^{(1)} \cong 3/\sqrt{N} \qquad \beta^{(1)} \cong 1/\sqrt{N}$$

Let's do this again

$$|\psi_3\rangle \cong -3/\sqrt{N}\,|x^*\rangle + \sum_{x \neq x^*} 1/\sqrt{N}$$

$|\psi_4\rangle$

$$\mu = \frac{(N-1)\,1/\sqrt{N} - 3/\sqrt{N}}{N}$$

$$= \frac{N-4}{\sqrt{N}} \Big/ N \approx N/\sqrt{N}/N$$

$$= 1/\sqrt{N}$$ same slightly less

$|\psi_5\rangle =$

$$\alpha^{(2)} = \frac{2}{\sqrt{N}} - -3/\sqrt{N} \cong 5/\sqrt{N}$$

$$\beta^{(2)} \cong 1/\sqrt{N}$$

	0	1	2
α	$1/\sqrt{N}$	$3/\sqrt{N}$	$5/\sqrt{N}$

to make α some const value
we must continue $\sqrt{N}$ times

Generally

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

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

$$\mu^{(t)} = \frac{-\alpha^{(t)} + N-1}{N} \beta^{(t)}$$ [mistake in paper]

1) α grows significantly if not already too large

[Fear: μ goes negative
because α is so large
& this causes in turn
α to decrease
]

Suppose $\alpha^{(t)} \leq 1/2$ & $N \geq 4$ $(n \geq 2)$

Claim $\alpha^{(t+1)} \geq \alpha^{(t)} + 1/\sqrt{N}$

α grows by at least $1/\sqrt{N}$

Proof

At t amplitudes^2 sum to $\underline{1}$

$$\underbrace{\left(\alpha^{(t)}\right)^2}_{\le 1/2} + (N-1)\left(\beta^{(t)}\right)^2 = \underline{1}$$

so $1 \le 1/4 + (N-1)\left(\beta^{(t)}\right)^2$

$$\frac{1-1/4}{N-1} \le \left(\beta^{(t)}\right)^2$$

$$\beta^{(t)} \ge \sqrt{3/4(N-1)}$$

What does this do to $m^{(t)}$ the mean?

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

$$\ge \frac{-1/2 + (N-1)\sqrt{3/4(N-1)}}{N}$$

$$= \frac{-\frac{1}{2} + \frac{1}{2}(N-1)\sqrt{3/(N-1)}}{N}$$

$$= \frac{\frac{1}{2}\left[-1 + \sqrt{\frac{(N-1)^2 3}{N-1}}\right]}{N}$$

$$= \frac{\frac{1}{2}\left[-1 + \sqrt{3(N-1)}\right]}{N}$$

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

$$N \geq 4 \rightarrow \sqrt{3N-3} - 1 \geq \sqrt{N}$$

[they are equal at $N=4$]

$$m^{(t)} \geq \frac{1}{2}\,\frac{\sqrt{N}}{N} = \frac{1}{2}\,\frac{1}{\sqrt{N}}$$

$$\begin{aligned} \alpha^{(t+1)} &= 2m^{(t)} + \alpha^{(t)} \\ &\geq 2\,\frac{1}{2}\,\frac{1}{\sqrt{N}} + \alpha^{(t)} \\ &\geq 1/\sqrt{N} + \alpha^{(t)} \end{aligned} \qquad \square$$

Now we must show $\alpha^{(t)}$ never gets too large — stays at/under $1/2$

Claim

For any t $\quad \alpha^{(t+1)} \le \alpha^{(t)} + 2/\sqrt{N}$

grows by at most $2/\sqrt{N}$ each iteration

$1/\sqrt{2} \quad 3/\sqrt{N} \quad 5/\sqrt{N}$ — we've seen this empirically

$\alpha^{(t)} \ge 0$ always so

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

also $(N-1)(\beta^{(t)})^2 \le 1$

$$\rightarrow \underline{\beta^{(t)} \le 1/\sqrt{N-1}}$$

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

$$\le 2\frac{N-1}{N}\underline{\beta^{(t)}} + \alpha^{(t)}$$

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

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

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

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

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

For t steps

$$\alpha^{(t)} \leq \alpha^{(0)} + 2/\sqrt{N}\; t$$

$$\leq 1/\sqrt{N} + 2t/\sqrt{N}$$

If we take at most $t = \sqrt{N}/8$ steps

$$\alpha^{(t)} \leq 1/\sqrt{N} + 1/4$$

$N \geq 16 \quad \alpha^{(t)} \leq 1/2$

Let's show $\alpha^{(t)} > .1$ in this process

$N < 16 \quad \alpha^{(0)} = 1/\sqrt{16} \geq 1/4$ done

$N \geq 16 \quad t \leq \sqrt{N}/8$

$$\alpha^{(\sqrt{N}/8)} = \frac{\sqrt{N}}{8}\frac{1}{\sqrt{N}} = 1/8 > 0.1$$

We can achive $\alpha^{(t)} \geq 0.1$ in $\sqrt{N}/8$ steps

$\Pr[\text{see } x^* \text{ in measurement}] = \left(\alpha^{(\sqrt{N}/4)}\right)^2$

$\geq .01$

low but

Try 110 times, test each time

$P[\text{one result is } x^*] = 1 - \Pr[\text{Not}]^{110}$

$\geq 1 - .99^{110}$

$\geq 2/3$

You can make this arbitrarily better!