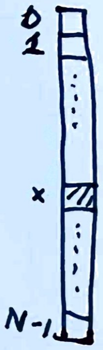
Unstructured Quantum Search (Grover's algorithm)

(Lecture notes of O'Donnel and Vazirani)

1

Looking for a needle in a haystack!



- classically search every entry : $O(N)$
- classically (randomly) $\sim \frac{N}{2}$ expected time

NP-complete problems: (hard to solve, easy to verify)

$\longleftrightarrow$ Satisfiability problem : finding a solution to satisfiability problem can be viewed as a search problem:

$$(x_1 \vee \neg x_2 \vee \neg x_3) \wedge (x_3 \vee x_5 \vee \neg x_6) \wedge \dots$$

Q: is there a configuration of $x_1, x_2, \dots x_n$ that satisfy the above formula?

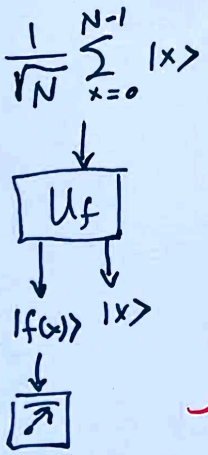
(There are $N = 2^n$ possible configurations)

Quantum solution: Grover's search (1996) can solve such problems in $O(\sqrt{n})$ time. (Thm. any quantum algorithm must take at least $\sqrt{n}$ time)

(Not exponential but quadratic speedup)

The main idea: "Use the fact that we can put n qubits and put them in equal superposition and probe these 2^n entries in parallel in quantum parallel universes" - by Umesh Vazirani

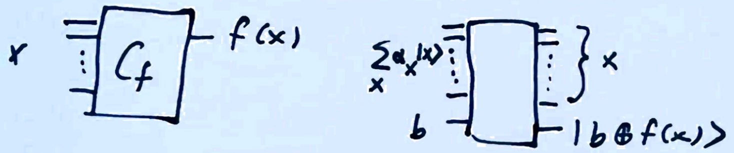
- put n-qubits in equal superposition:



This is not better than probing the list.

What we do in quantum computing is not only using the superposition of states, but getting constructive/destructive interference

Problem: Given $f:\{0,1,\dots,N-1\}\to\{0,1\}$, find x s.t. $f(x)=1$. (hardest case is when there is one x s.t. $f(x)=1$)

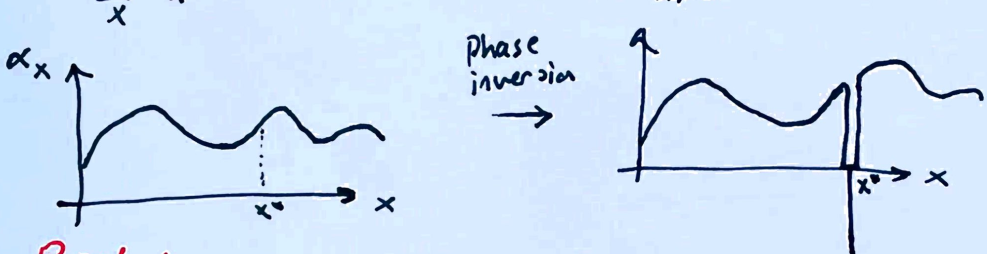


Two primitives

1) **Phase inversion**:

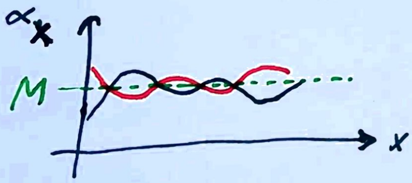
$f(x^*)=1$

$$\sum_x \alpha_x|x\rangle \longrightarrow \sum_{x\neq x^*}\alpha_x|x\rangle - \alpha_{x^*}|x^*\rangle$$



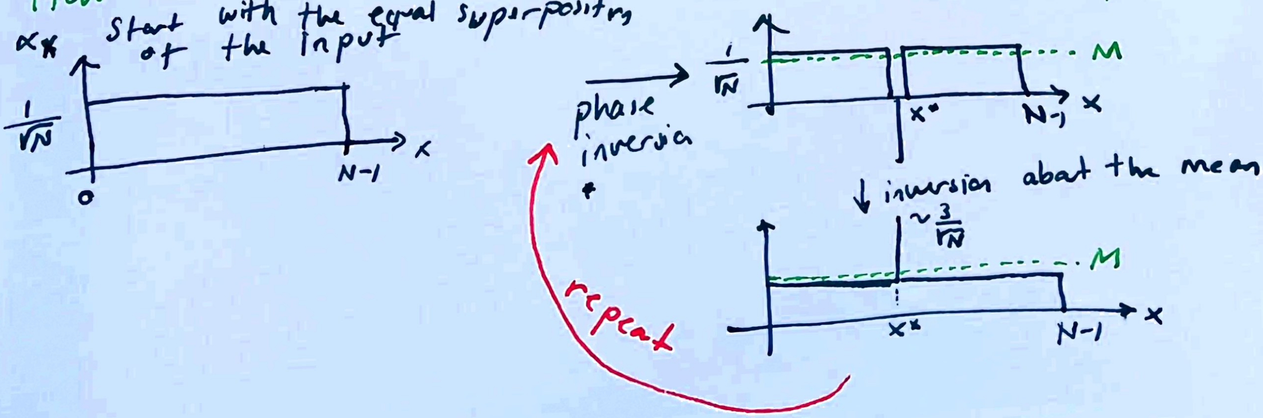
2) ~~Inversion~~ **Reflection about mean**

$$\sum_x \alpha_x|x\rangle \to \sum_x (2M-\alpha_x)|x\rangle$$



How do we solve the problem using these primitives?

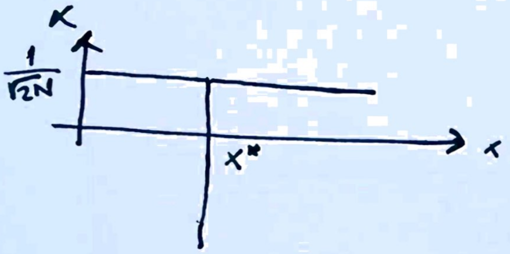
Start with the equal superposition of the input



3

$\alpha^* = \frac{1}{\sqrt{N}} \to \sim \frac{3}{\sqrt{N}} \to \sim \frac{5}{\sqrt{N}} \to \sim \frac{7}{\sqrt{N}} \to \cdots\cdots \to \frac{2T+1}{\sqrt{N}}$ after T iters.

When $\alpha^* = \frac{1}{\sqrt{2}}$ (50% probability) the rest have an amplitute $\sim \frac{1}{\sqrt{2N}}$.



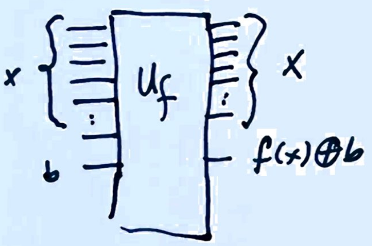
at this step the improvement is $\sim 2 * \frac{1}{\sqrt{2N}} = \frac{\sqrt{2}}{\sqrt{N}}$

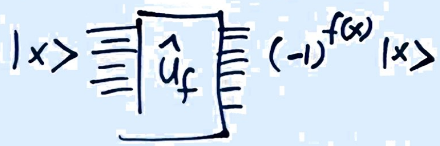
Therefore one can reach $\frac{1}{\sqrt{2}}$ in $\sim \frac{1/\sqrt{2}}{\sqrt{2}/\sqrt{N}} = \frac{\sqrt{N}}{2}$ steps.

In fact, as shown by Boyer, Brassard, Høyer, Tapp, "Tight bounds on Quantum Searching", 1998, $\alpha^* \approx 1$ after $\frac{\pi}{4}\sqrt{N}$ iterations!

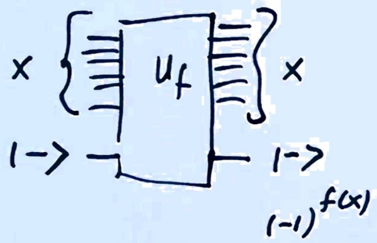
Created with Scanner Pro

Phase inversion :





$$\sum_x \alpha_x |x\rangle \longrightarrow \sum_x (-1)^{f(x)} \alpha_x |x\rangle$$



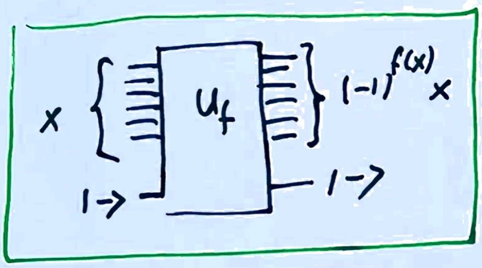
$$|-\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$$

Case 1: $f(x) = 0$

$$|-\rangle \longrightarrow |-\rangle$$

Case 2: $f(x) = 1$

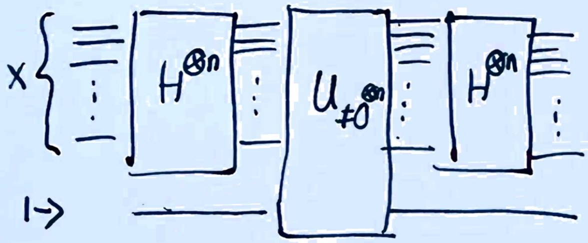
$$|-\rangle \longrightarrow \frac{1}{\sqrt{2}} |1\rangle - \frac{1}{\sqrt{2}} |0\rangle = -|-\rangle$$



$\longrightarrow$ Phase inversion quantum circuit

Reflection about mean:

$$\sum_x \alpha_x |x\rangle \longrightarrow \sum_x (2M - \alpha_x)|x\rangle$$



$$g(x) = \begin{cases} 0 & \text{if } x = 00\cdots0 \\ 1 & \text{otherwise} \end{cases}$$

Reflection about the mean is the same as doing reflection about $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$

$$H^{\otimes n} \begin{pmatrix} 1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ 0 & & & -1 \end{pmatrix} H^{\otimes n}$$

$$= H^{\otimes n} \left[\begin{pmatrix} 2 & 0 & 0 \\ & \ddots & \\ 0 & & 0 \end{pmatrix} - \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \right] H^{\otimes n}$$

$$= H^{\otimes n} \begin{pmatrix} 2 & & 0 \\ & 0 \ddots & \\ 0 & & 0 \end{pmatrix} H^{\otimes n} - \underbrace{H^{\otimes n} I H^{\otimes n}}_{I}$$

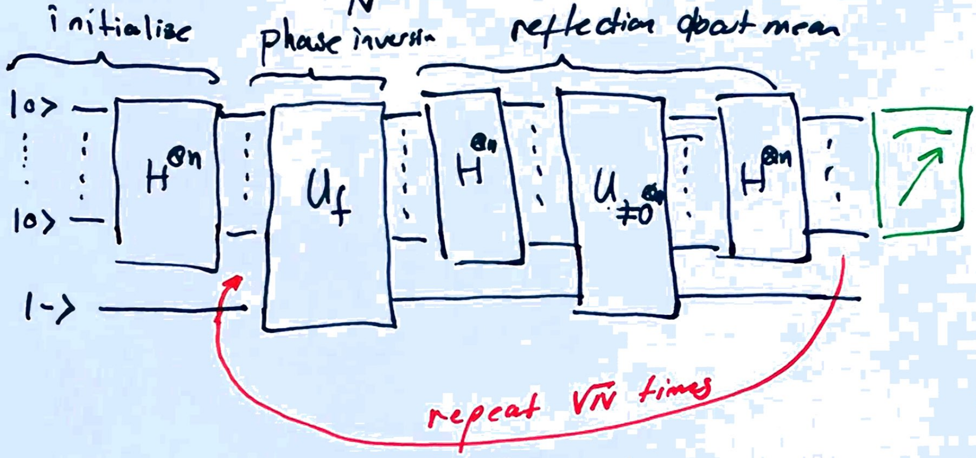
$$= \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & & & \\ \frac{2}{N} & \cdots & & \frac{2}{N} \end{pmatrix} - I$$

$$= \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & & \ddots & \\ \frac{2}{N} & & & \frac{2}{N}-1 \end{pmatrix}$$

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N} & \frac{2}{N}-1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} 2M-\alpha_0 \\ 2M-\alpha_1 \\ \vdots \\ 2M-\alpha_{N-1} \end{pmatrix}$$

$\sum_x \alpha_x |x\rangle$

Where $2M = \frac{2}{N}(\alpha_0 + \alpha_1 + \cdots + \alpha_{N-1})$



* if too many iterations are done, grover's algorithm might uncompute the result.