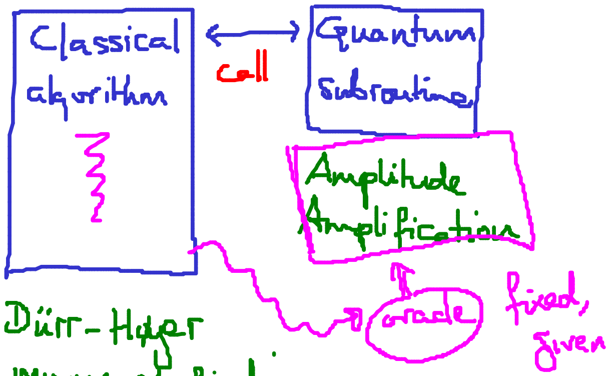
6/26/18

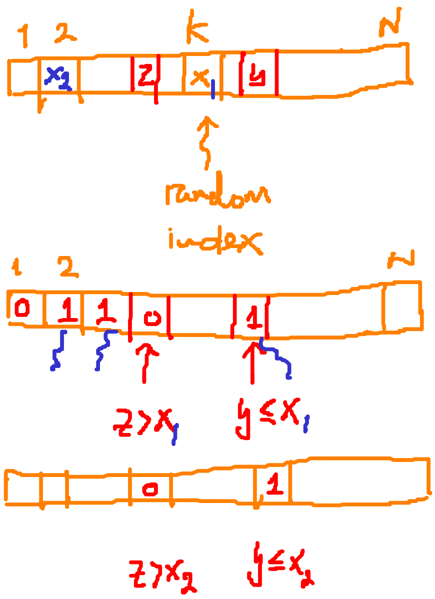


Dürr-Høyer MINIMUM finding algorithm

MINIMUM

Input: An array of N integers

Output: The smallest integer.

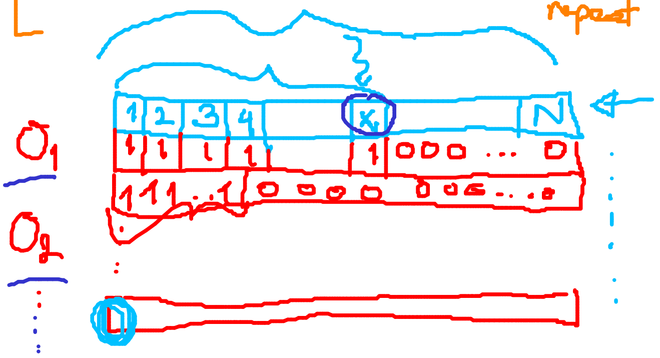


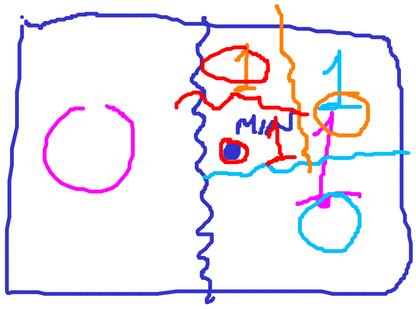
Run $\boxed{AA}$ on oracle:

return a random position where oracle is 1 (O_1)

cost is $\sqrt{N}$ queries

repeat





$\sqrt{N}$

$\sqrt{N/2}$

$\sqrt{N/4}$

$\vdots$

$+$

$$\sqrt{N}\underbrace{\left(1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{4}}+\frac{1}{\sqrt{8}}+\cdots\right)}_{\text{constant}}$$

Must dynamically create new oracles

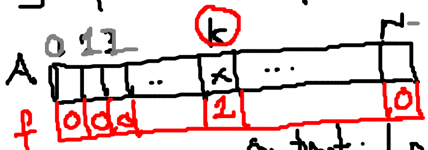
Grover (revisited): SEARCHING an array of size N for item x

$f : \{0, 1, \ldots, N-1\} \to \{0, 1\}$

$\boxed{N = 2^n}$ wlog

classical test

$$f(j) = \begin{cases} 1 & \text{if } A[j] = x \\ 0 & \text{if } A[j] \neq x \end{cases}$$

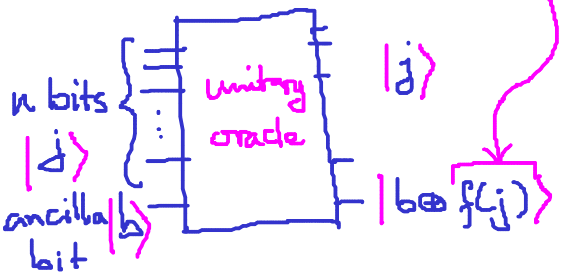


Output: Location/index where x occurs

Say k

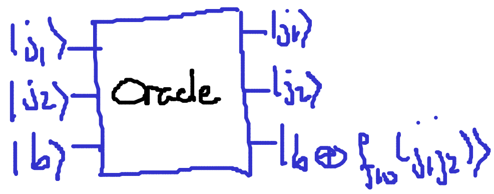
f can be computed classically (reversibly) [Bennett, ...]

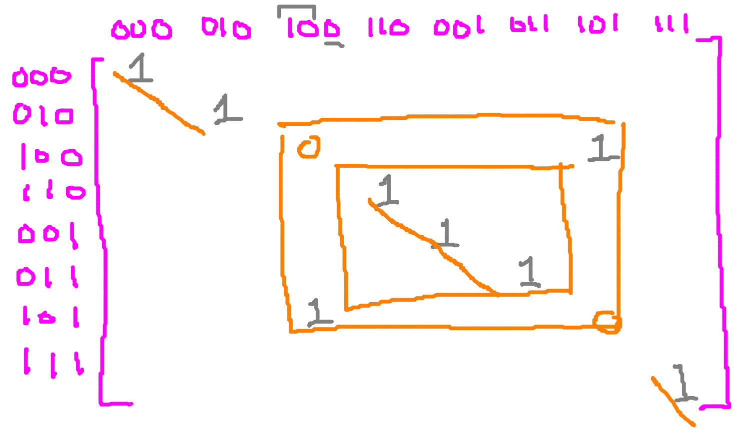
use the classical reversible circuit for computing f



example: $n = 2$ $\quad N = 4$ $\quad$ indices $\{0, 1, 2, 3\}$ (00 01 10 11)

oracle encodes x in position $2 = 10_2$ $\quad f_{10}$



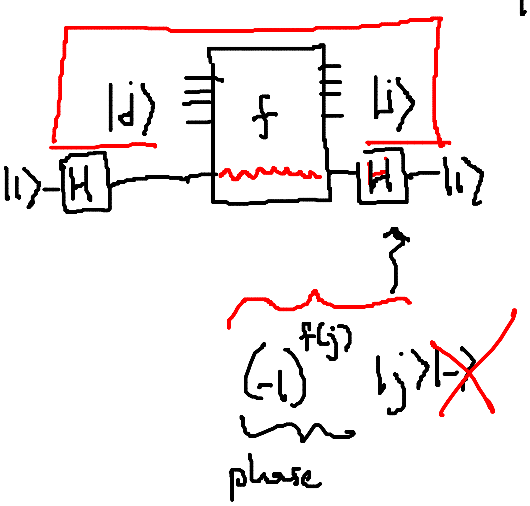


$|j\rangle|b\rangle \xrightarrow[\text{ancilla}]{f} |j\rangle|b \oplus f(j)\rangle$

equivalent

$|j\rangle \xrightarrow[\text{no ancilla}]{\tilde{f}} (-1)^{f(j)} |j\rangle$

→ Eigenvalue Kickback method: [Cleve, Ekert, Mosca, Machiavello]



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

$\xrightarrow{f} \frac{1}{\sqrt{2}}|j\rangle|f(j)\rangle - \frac{1}{\sqrt{2}}|j\rangle|\overline{f(j)}\rangle$

$$\to \begin{cases} \frac{1}{\sqrt{2}}|j\rangle|0\rangle - \frac{1}{\sqrt{2}}|j\rangle|1\rangle & \text{if } f(j) = 0 \\ \quad (-1)^{f(j)}\left[\frac{1}{\sqrt{2}}|j\rangle|0\rangle - \frac{1}{\sqrt{2}}|j\rangle|1\rangle\right] & \\ \frac{1}{\sqrt{2}}|j\rangle|1\rangle - \frac{1}{\sqrt{2}}|j\rangle|0\rangle & \text{if } f(j) = 1 \end{cases}$$

$$= (-1)^{f(j)}\left[\frac{1}{\sqrt{2}}|j\rangle|0\rangle - \frac{1}{\sqrt{2}}|j\rangle|1\rangle\right]$$

Grover (continued):

phase oracle (reflection) R_f:

$$R_f|j\rangle = \begin{cases} -|j\rangle & \text{if } f(j)=1 \\ |j\rangle & \text{if } f(j)=0 \end{cases}$$

reflection R_0:

$$R_0|j\rangle = \begin{cases} -|j\rangle & \text{if } j=0 \\ |j\rangle & \text{if } j\neq 0 \end{cases}$$

Grover iteration:

$$G = \underbrace{(H^{\otimes n} R_0 H^{\otimes n})}R_f \quad \xrightarrow{\text{amplitude amplification}} \quad G = -A R_0 A^{-1} R_f$$

[Høyer]

$A = H^{\otimes n}$ $\qquad$ A = arbitrary unitary operator

$$R_0 = I - 2|0\rangle\langle 0| \qquad HH = I \qquad H^\dagger = H$$

$$\underbrace{-H^{\otimes n} R_0 H^{\otimes n}}_{R_{H_n}} = H^{\otimes n}(I - 2|0\rangle\langle 0|)H^{\otimes n} = I - 2\,H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}$$

$$\underbrace{H^{\otimes n}\,|0\rangle^{\otimes n}} = (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{N}}\sum_j |j\rangle \quad \text{uniform superposition}$$

$$= I - \frac{2}{N}\begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix} = \begin{bmatrix} 1-\frac{2}{N} & & -\frac{2}{N} \\ & 1-\frac{2}{N} & \\ & & \ddots \\ -\frac{2}{N} & & 1-\frac{2}{N} \end{bmatrix}$$

inversion around mean

$$\frac{1}{N}\underbrace{\sum_{jk}|j\rangle\langle k|}_{\text{all-one matrix}} = \frac{1}{N}\begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix}$$

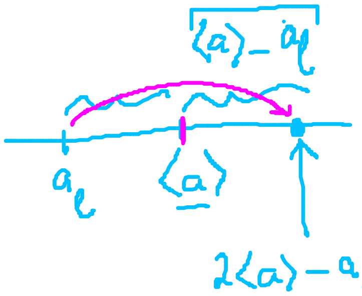
$|\psi\rangle \doteq \sum_\ell a_\ell|\ell\rangle$ $\quad$ arbitrary state

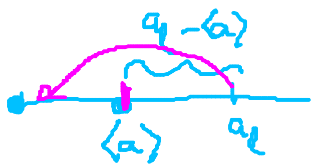
$$R_{H_n}|\psi\rangle = \left(I - \frac{2}{N}\underbrace{\sum_{jk}|j\rangle\langle k|}\right)|\psi\rangle = \sum_\ell a_\ell|\ell\rangle - \frac{2}{N}\sum_{j,k}|j\rangle\langle k|\sum_\ell a_\ell|\ell\rangle$$

$$= \sum_\ell a_\ell|\ell\rangle - \frac{2}{N}\sum_j |j\rangle\left[\sum_k a_k\right]$$

$$= \sum_\ell a_\ell|\ell\rangle - 2\sum_\ell \underbrace{\left[\frac{1}{N}\sum_k a_k\right]}_{\langle a\rangle}|\ell\rangle$$

$$= \sum_\ell \underbrace{(a_\ell - 2\langle a\rangle)}_{\Downarrow\ 2\langle a\rangle - a_\ell}|\ell\rangle$$

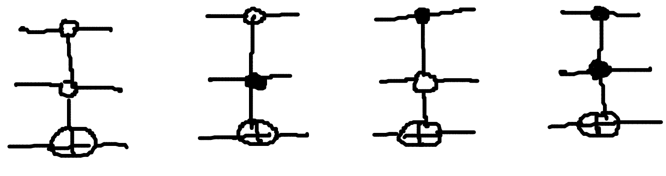




$$\langle a\rangle - (a_\ell - \langle a\rangle) = 2\langle a\rangle - a_\ell$$

Grover (continued): $n=2$, $N=4$ Nielsen-Chuang

possible oracles (exactly one 1)



00 01 10 11

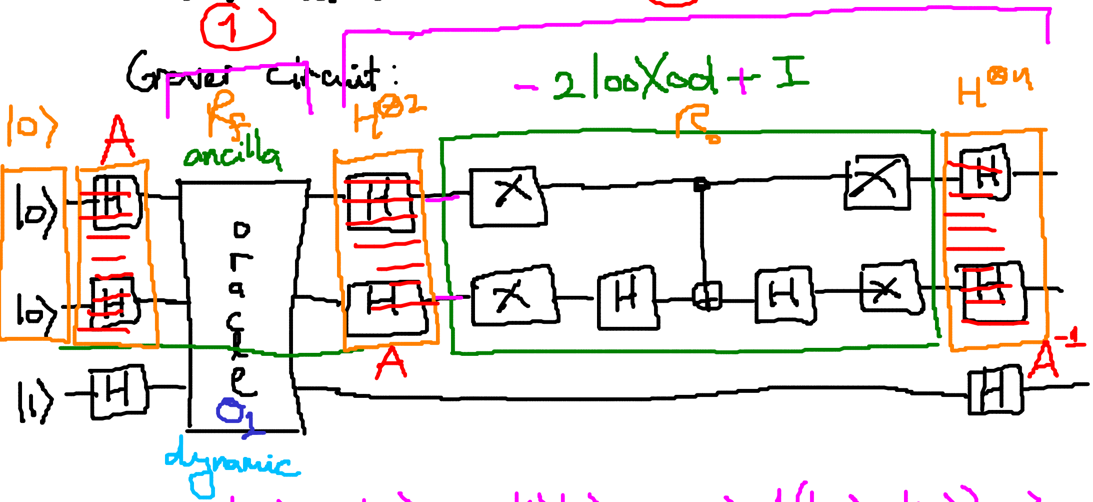
eigenvalue $\rightsquigarrow$ kickback

R_f

phase oracles ① ② ①②

ancilla-based oracles ① ②

Grover circuit:



repeat

$\sqrt{N}$ times

with O_1

$|00\rangle \to |11\rangle \to |1\rangle|-\rangle \longrightarrow \frac{1}{\sqrt{2}}(|11\rangle - |10\rangle) \to -|1\rangle|1\rangle \to -|0\rangle|0\rangle$

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

$|01\rangle \to |10\rangle \to |1\rangle|+\rangle \longrightarrow |1\rangle|+\rangle \longrightarrow |1\rangle|0\rangle \to |01\rangle$

$= \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$

$|10\rangle \to |10\rangle$

$|11\rangle \to |11\rangle$

Goal: * Implement Dürr-Høyer's algorithm in Quipper (or some other options)