Introduction to Quantum Information Processing

Michele Mosca

Overview

- Quantum Searching
- Quantum Counting
- Searching when you don't know the number of elements

QUANTUM SEARCHING

Searching problem

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

Given $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$

find an x satisfying $f(x) = 1$.

Application

Consider a 3-SAT formula

$$\Phi = C_1 \wedge C_2 \wedge \cdots \wedge C_M$$

$$C_j = (y_{j,1} \vee y_{j,2} \vee y_{j,2})$$

$$y_{j,k} \in \{x_1, x_2, \cdots, x_n, \overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n\}$$

For a given assignment $\mathrm{x} = \mathrm{x}_1 \mathrm{x}_2 \cdots \mathrm{x}_n$

$$f_\Phi(\mathrm{x}) = \begin{cases} 1 & \text{if x satisfies } \Phi \\ 0 & \text{otherwise} \end{cases}$$

Some ideas

For simplicity, let's start by assuming that $f(x) = 1$ has exactly one solution, $x = w$.

IDEA: Prepare

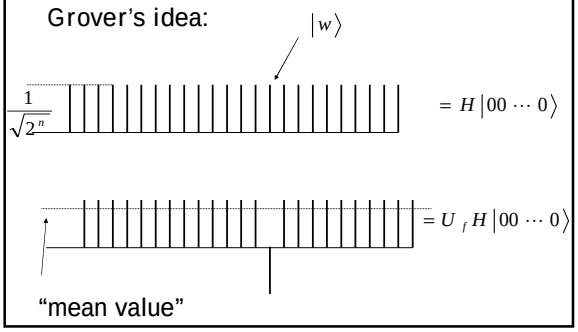
$$\sum_x \frac{1}{\sqrt{2^n}} |x\rangle = \frac{1}{\sqrt{2^n}} |w\rangle + \left(\sum_{x \neq w} \frac{1}{\sqrt{2^n}} |x\rangle \right)$$

Keep this — "Re-scramble" this

Repeat roughly $\sqrt{2^n}$ times.

Must do this with legal quantum operations

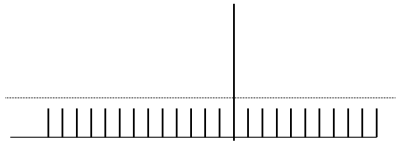
Grover's idea:



"mean value"

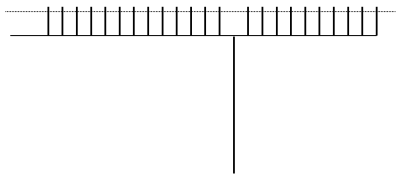
Must do this with legal quantum operations

"invert about the mean"



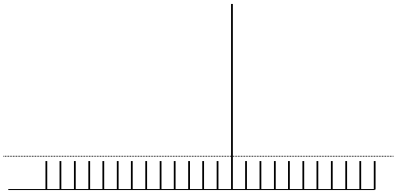
$$= (-HU_0 H)U_f H|00\cdots 0\rangle$$
$$= -U_{H|0\rangle}U_f H|00\cdots 0\rangle$$

Repeat



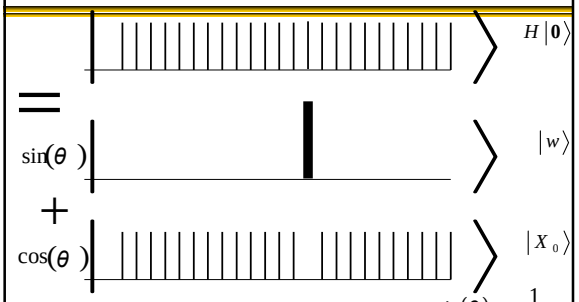
$$= U_f(-HU_0 H)U_f H|00\cdots 0\rangle$$

Repeat



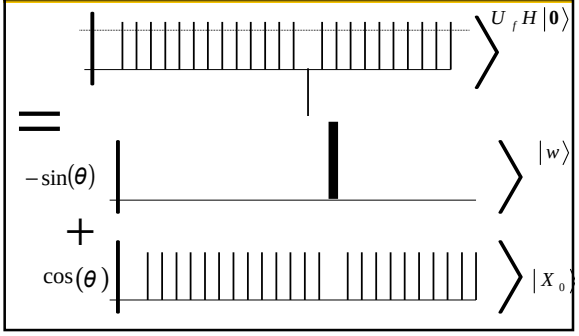
$$= (-HU_0H)U_f(-HU_0H)U_fH|00\cdots0\rangle$$

A nice way to analyze this

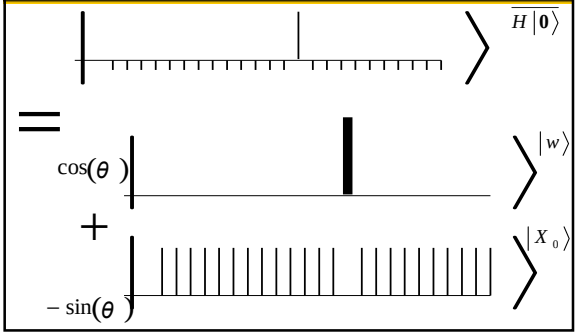


$$\sin(\theta) = \frac{1}{\sqrt{2^n}}$$

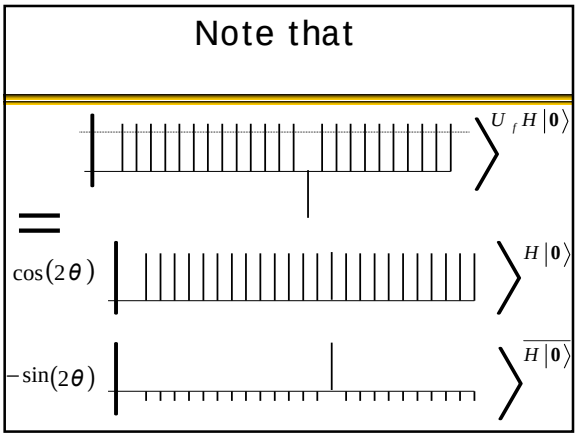
A nice way to analyze this



Definition



Note that



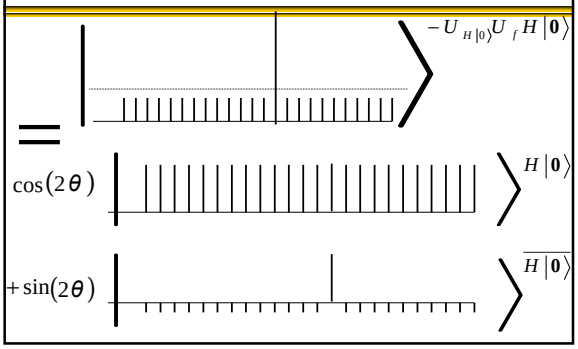
Verify that

$$-\sin(\theta)|w\rangle + \cos(\theta)|X_0\rangle$$

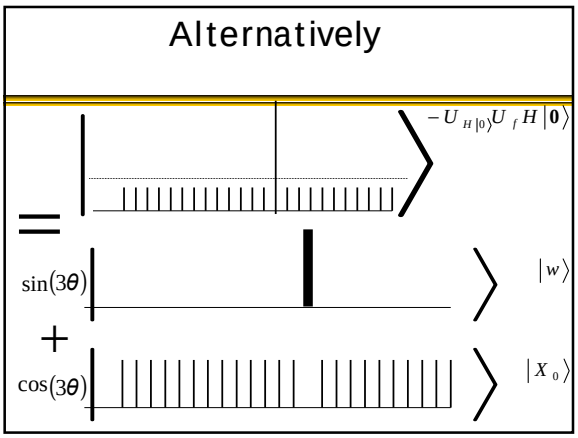
$$=$$

$$\cos(2\theta)\, H|\mathbf{0}\rangle \; -\sin(2\theta)\, \overline{H|\mathbf{0}\rangle}$$

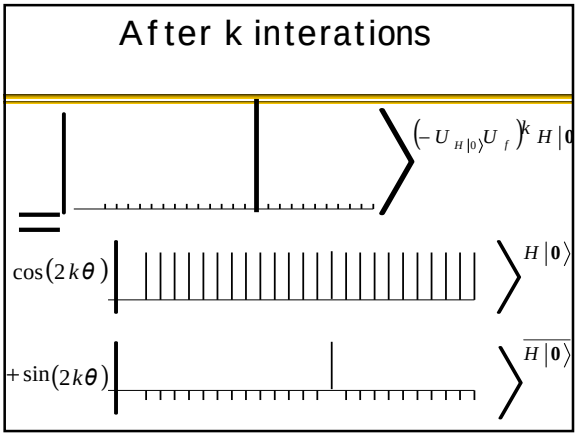
After “inversion”



Alternatively

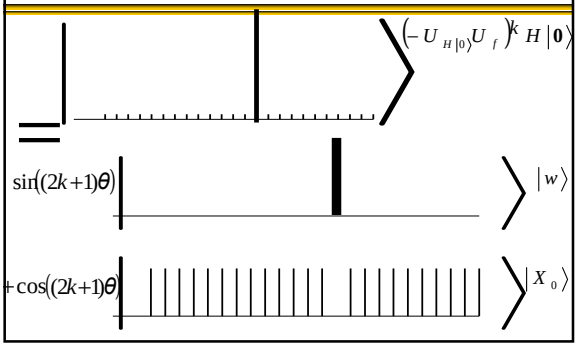


After k interations



(*formula found by BBHT)

Alternatively



Selecting parameters

So we need

$$\sin((2k+1)\theta) \approx 1$$

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx \frac{\pi\sqrt{2^n}}{4}$$

Square root speed-up! What if we don't know k? See [BBHT] (or [M98]) for a protocol that works in this case as well.

Generalization: Amplitude Amplification (BBHT,BH,BHT,G,BHMT,...)

Consider functions with t solutions

$X_1 = f^{-1}(1)$ $X_0 = f^{-1}(0)$ $t = |X_1|$

Consider any algorithm that works with non-zero probability

$$A|0\rangle = |\Psi\rangle \qquad |\Psi\rangle = \sin(\theta)|\Psi_1\rangle + \cos(\theta)|\Psi_0\rangle$$

$$|\Psi_1\rangle = \sum_{x\in X_1} \alpha_x |x\rangle \qquad \sum_{x\in X_1} |\alpha_x|^2 = 1$$

$$|\Psi_0\rangle = \sum_{y\in X_0} \alpha_y |y\rangle \qquad \sum_{y\in X_0} |\alpha_y|^2 = 1$$

Amplitude Estimation

- Given operators

$$A|0\rangle = |\Psi\rangle = \sin(\theta)|\Psi_1\rangle + \cos(\theta)|\Psi_0\rangle$$

$$U_f : |\Psi_1\rangle \mapsto -|\Psi_1\rangle$$
$$|\Psi_0\rangle \mapsto |\Psi_0\rangle$$

- Estimate $\sin^2(\theta)$

Application: Counting

- E.g. $A|0\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}|x\rangle$

$$|\Psi_1\rangle = \sum_{x\in X_1} \frac{1}{\sqrt{t}}|x\rangle \qquad |\Psi_0\rangle = \sum_{y\in X_0} \frac{1}{\sqrt{N-t}}|y\rangle$$

- So $A|0\rangle = \sqrt{\frac{t}{N}}|\Psi_1\rangle + \sqrt{\frac{N-t}{N}}|\Psi_0\rangle$
- So $\sin(\theta) = \sqrt{\frac{t}{N}}$

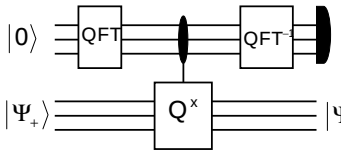
Eigenvectors of Q

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}|\Psi_0\rangle + \frac{i}{\sqrt{2}}|\Psi_1\rangle$$

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}|\Psi_0\rangle - \frac{i}{\sqrt{2}}|\Psi_1\rangle$$

$$Q|\Psi_+\rangle = e^{i2\theta}|\Psi_+\rangle \qquad Q|\Psi_-\rangle = e^{-i2\theta}|\Psi_-\rangle$$

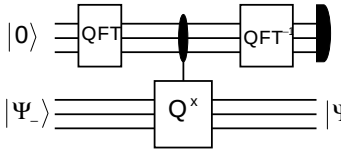
Amplitude Estimation ≈ Eigenvalue Estimation



$$\frac{2\pi y}{N} \approx 2\theta$$

$$\sin^2\left(\frac{\pi y}{N}\right) \approx \sin^2(\theta)$$

Amplitude Estimation ≈ Eigenvalue Estimation

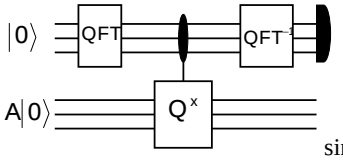


$$\frac{2\pi y}{N} \approx 2\pi - 2\theta$$

$$\sin^2\left(\frac{\pi y}{N}\right) \approx \sin^2(\theta)$$

Amplitude Estimation ≈ Eigenvalue Estimation

$$A|0\rangle = \frac{1}{\sqrt{2}} e^{i\theta} |\Psi_+\rangle + \frac{1}{\sqrt{2}} e^{-i\theta} |\Psi_-\rangle$$



$$\sin^2\left(\frac{\pi y}{N}\right) \approx \sin^2(\theta)$$

(BBHT discovered this in the Shor picture)

Application: Tight exact counting (BBHT,BHT,M,BHMT)

Using $A|0\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}|x\rangle$

we have $\sin(\theta_t) = \sqrt{\frac{t}{N}}$

To count exactly requires us to distinguish θ_t from θ_k , $k \neq t$

This requires precision $\Theta\left(\frac{1}{\sqrt{(t+1)(2^n - t + 1)}}\right)$

Application: Tight exact counting

QFT eigenvalue estimation techniques will give us this precision using $\Theta\left(\sqrt{(t+1)(2^n - t + 1)}\right)$ applications of Q

Black-box lower bounds imply that we need $\Omega\left(\sqrt{(t+1)(2^n - t + 1)}\right)$ calls to U_f

Searching when we don't know the number of solutions

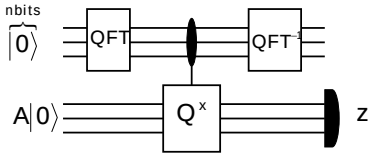
Note that the amplitude estimation network produces states

$$\frac{1}{\sqrt{2}} e^{i\theta} |\widetilde{\theta}\rangle |\Psi_+\rangle + \frac{1}{\sqrt{2}} e^{-i\theta} |\widetilde{2\pi - \theta}\rangle |\Psi_-\rangle$$

As the eigenvalue estimates become more orthogonal, the second register becomes closer and closer to an equal mixture of

$$\frac{1}{2}|\Psi_+\rangle\langle\Psi_+| + \frac{1}{2}|\Psi_-\rangle\langle\Psi_-| = \frac{1}{2}|\Psi_1\rangle\langle\Psi_1| + \frac{1}{2}|\Psi_0\rangle\langle\Psi_0|$$

Searching when we don't know the number of solutions



$$Prob(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$Prob(f(z)=1) \to \frac{1}{2}$$
$$n \to \infty$$

Searching when we don't know the number of solutions

So for each n=1,2,3,4,…, we try twice to find a satisfying x

This means that once $2^n > \frac{1}{\theta}$ we will find a satisfying x with probability in

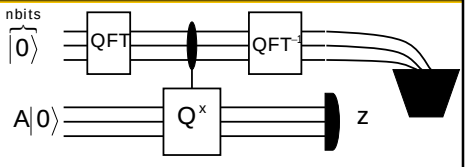
$$\frac{3}{4} - O\left(\frac{1}{2^n \theta}\right)$$

This means the expected running time is in

$$O\left(\frac{1}{\theta}\right)$$

The way BBHT do it

Notice

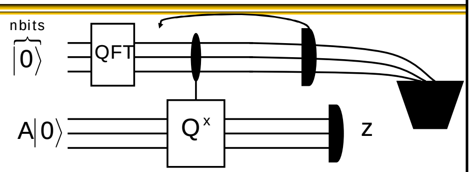


$$Prob(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$Prob(f(z)=1) \to \frac{1}{2}$$
$$n \to \infty$$

The way BBHT do it

Notice

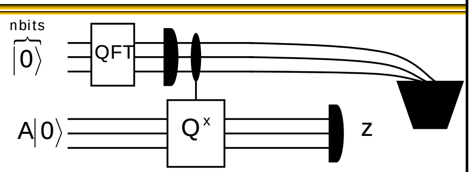


$$\text{Prob}(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$\text{Prob}(f(z)=1) \xrightarrow[n \to \infty]{} \frac{1}{2}$$

The way BBHT do it

Notice

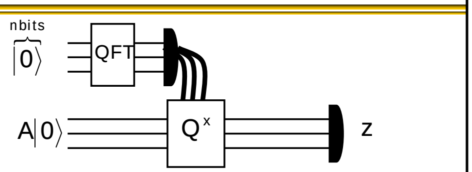


$$\text{Prob}(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$\text{Prob}(f(z)=1) \xrightarrow[n \to \infty]{} \frac{1}{2}$$

The way BBHT do it

Notice

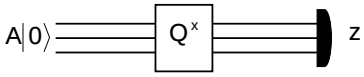


$$\text{Prob}(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$\text{Prob}(f(z)=1) \xrightarrow[n \to \infty]{} \frac{1}{2}$$

The way BBHT do it

Pick random $x \in \{0,1,\cdots,2^n-1\}$



$$\text{Prob}(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n \theta}\right)$$

$$\text{Prob}(f(z)=1) \to \frac{1}{2}$$
$$n \to \infty$$