Quantum Searching

Michele Mosca

Canada Research Chair in Quantum Computation

PIMS-MITACS Summer School on Quantum Information Science

June 2003

Overview

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

QUANTUM SEARCHING

Searching problem

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

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 $\mathrm{x} = \mathrm{x}_1 \mathrm{x}_2 \cdots \mathrm{x}_\mathrm{n}$

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

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

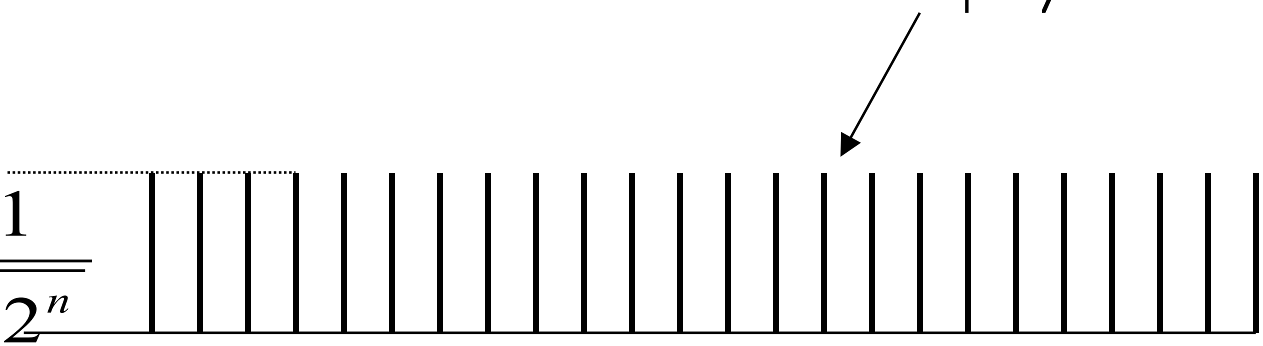
"Re-scramble" this

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

Must do this with legal quantum operations

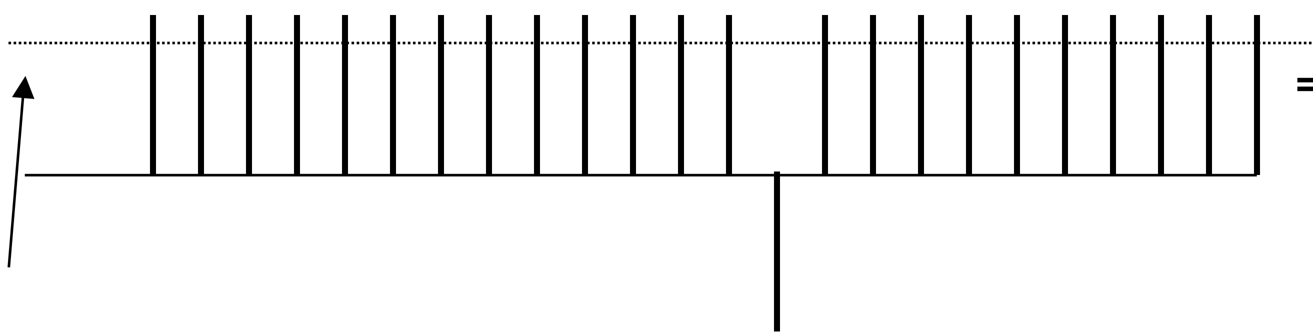
Grover's idea:

$|w\rangle$



$\frac{1}{\sqrt{2^n}}$

$= H|00\ldots0\rangle$

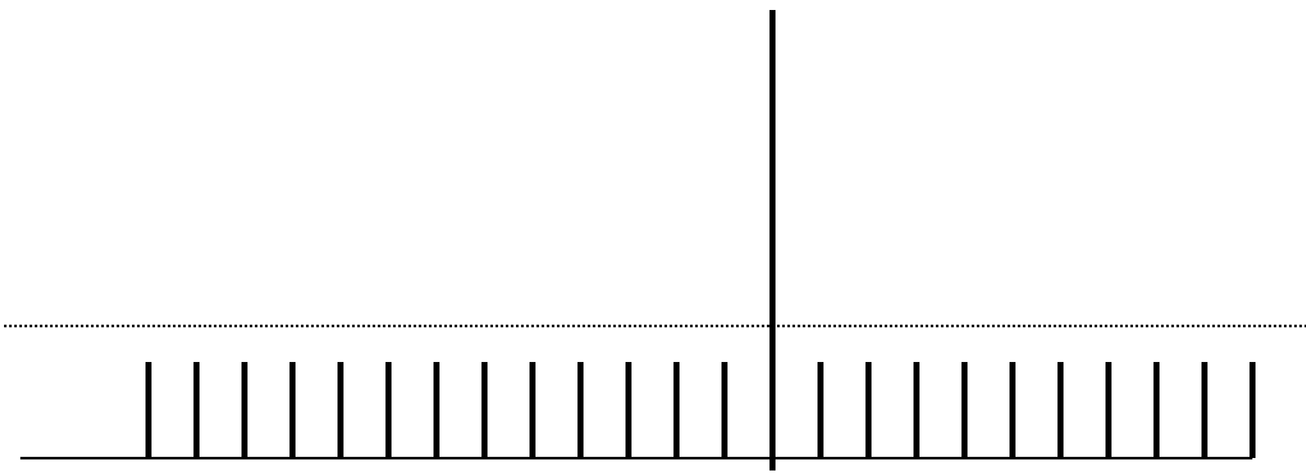


$= U_f H|00\ldots0\rangle$

"mean value"

Must do this with legal quantum operations

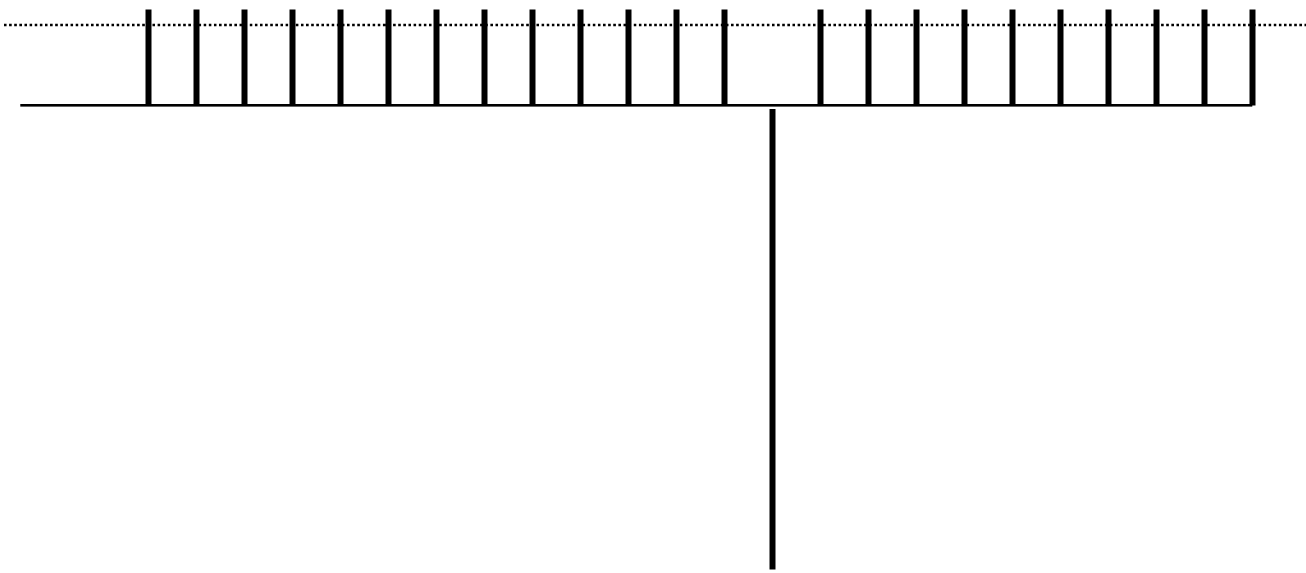
"invert about the mean"



$$= (-HU_0H)U_fH|00\ldots0\rangle$$

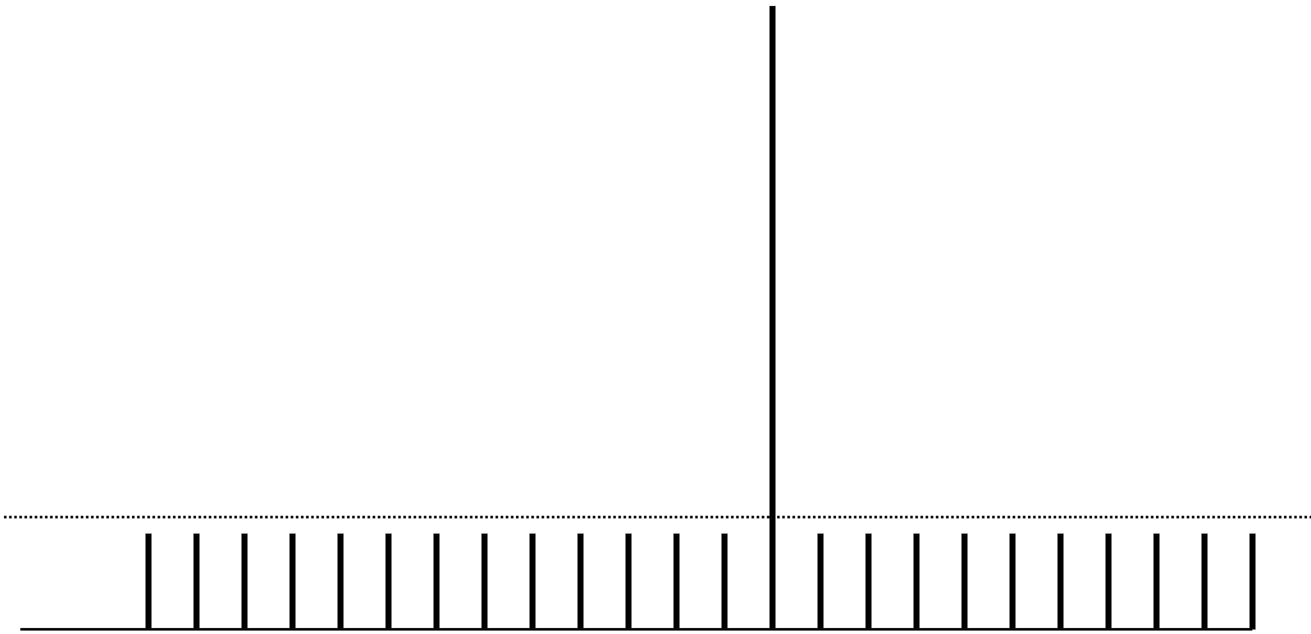
$$= -U_{H|0\rangle}U_fH|00\ldots0\rangle$$

Repeat



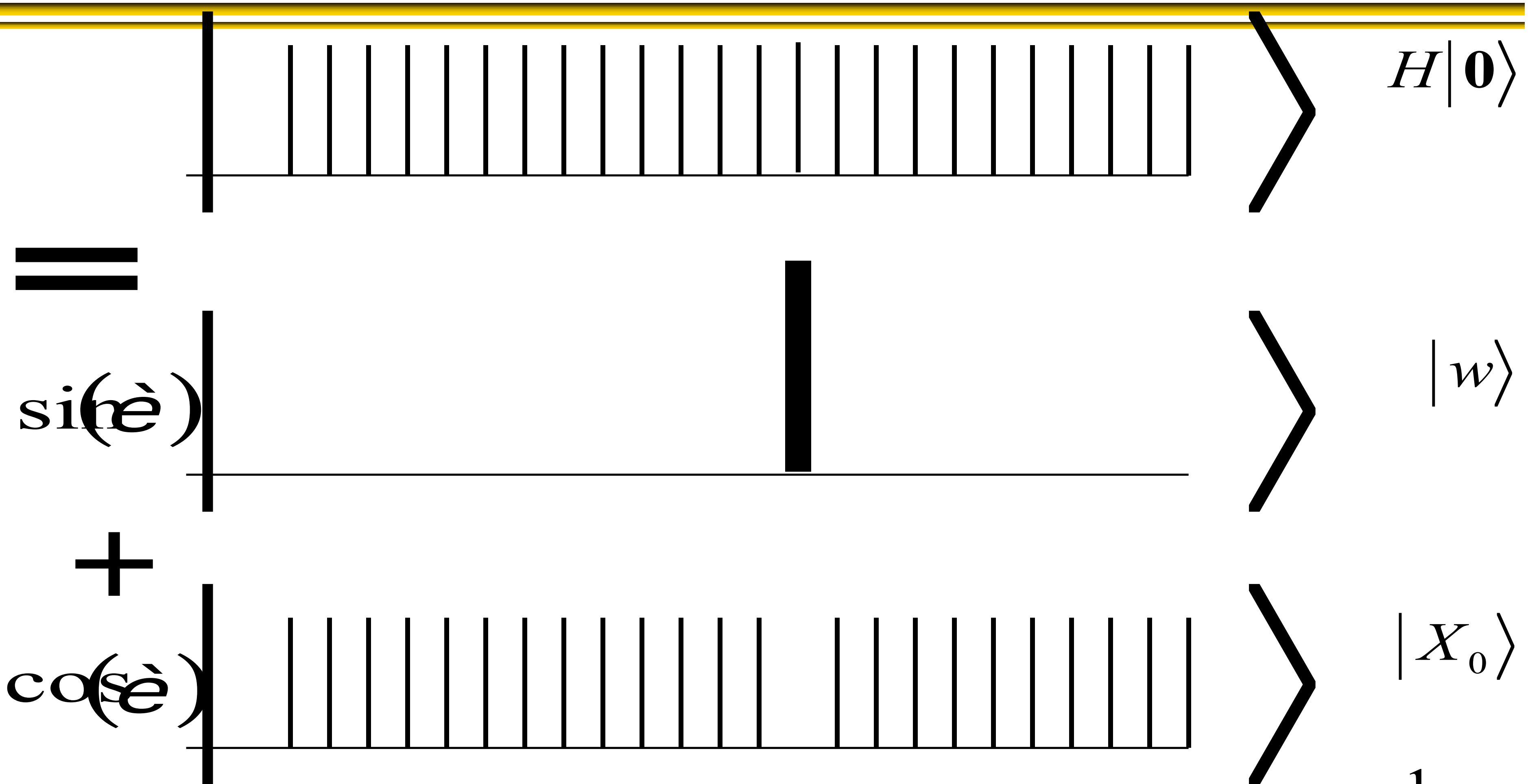
$$= U_f\left(\square\, H U_0 H\right) U_f H \left|00\ldots0\right\rangle$$

Repeat



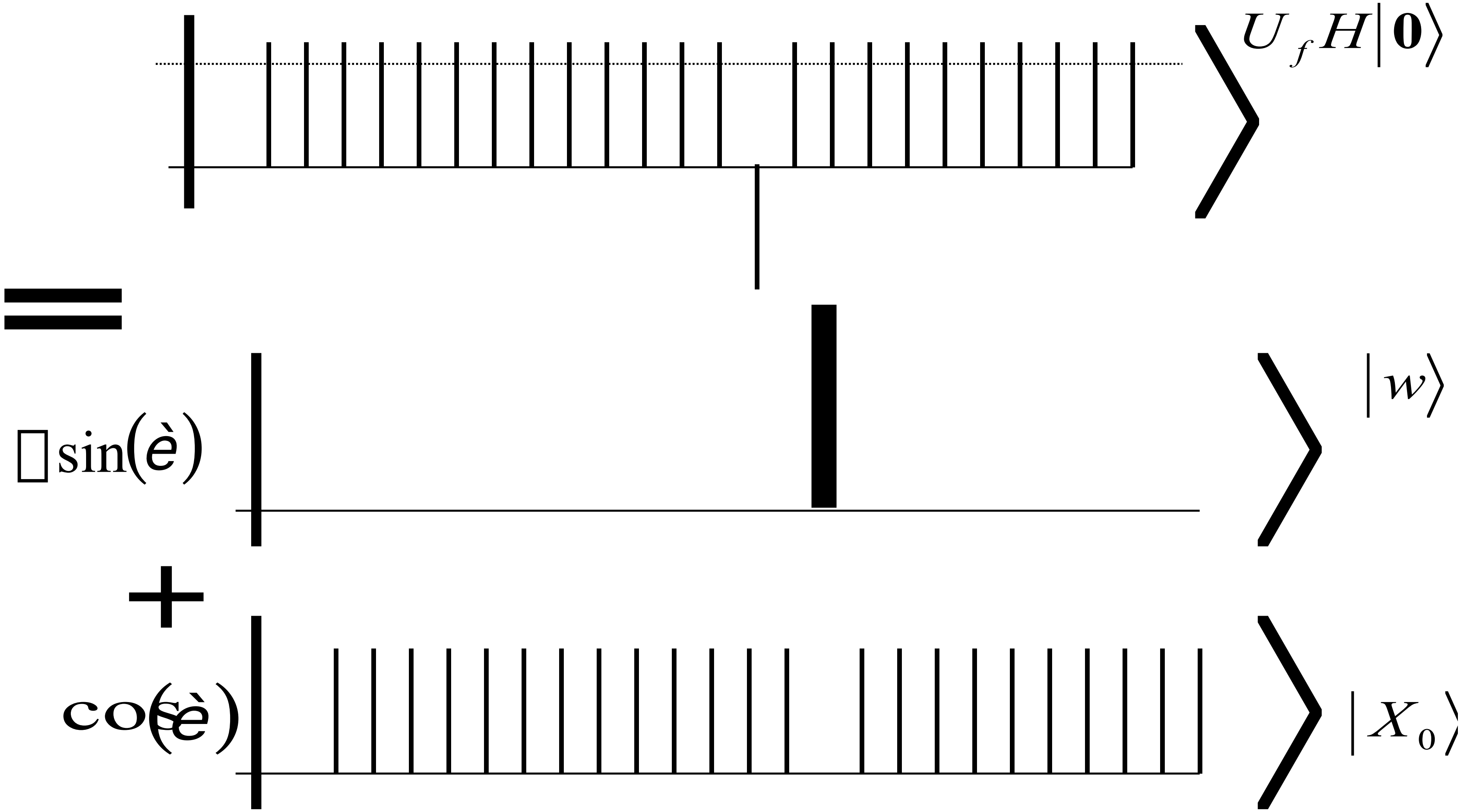
$$= \left(-HU_0H\right)U_f\left(-HU_0H\right)U_fH\left|00\ldots0\right\rangle$$

A nice way to analyze this

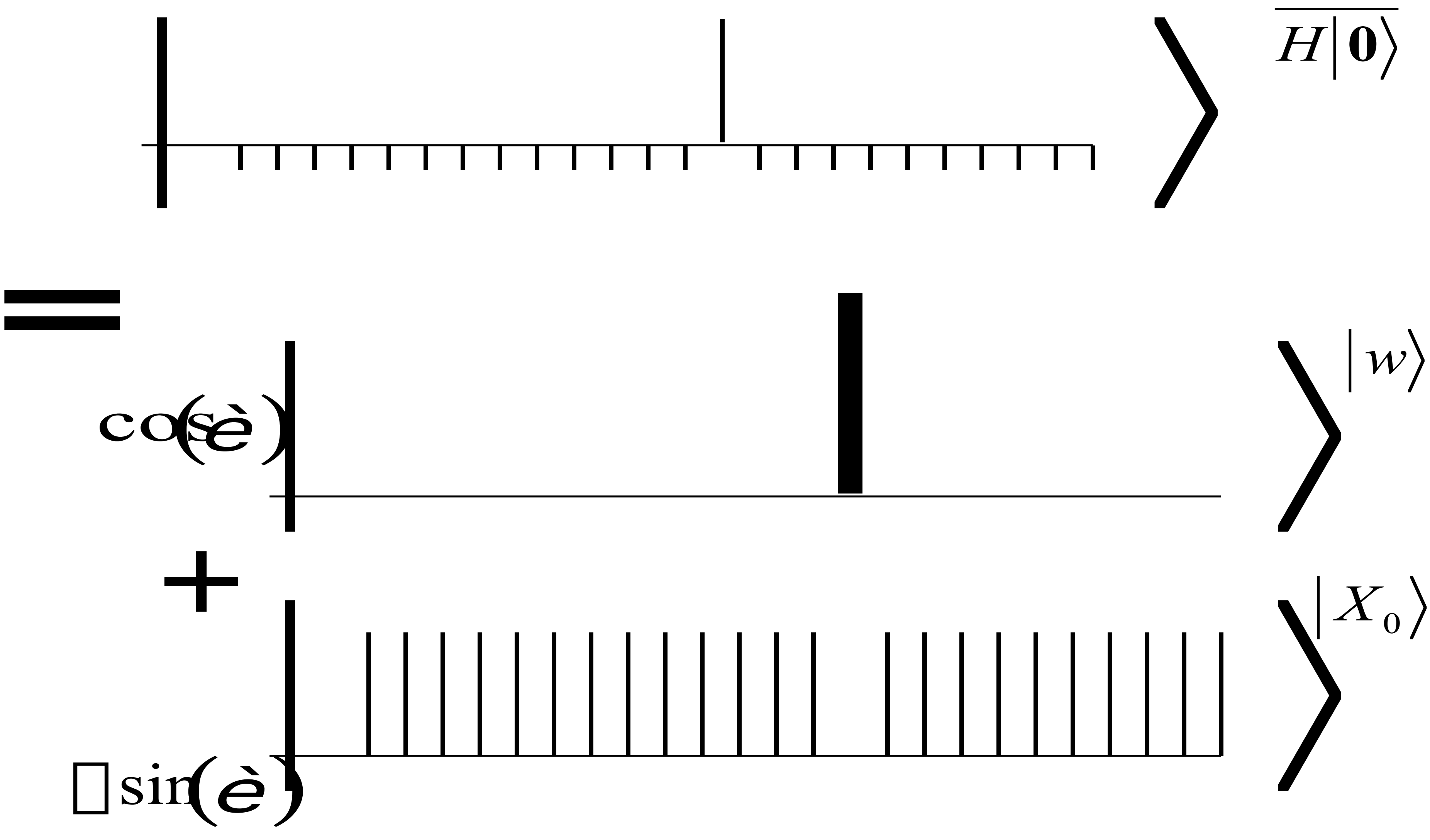


$$\sin(\theta) = \frac{1}{\sqrt{2^n}}$$

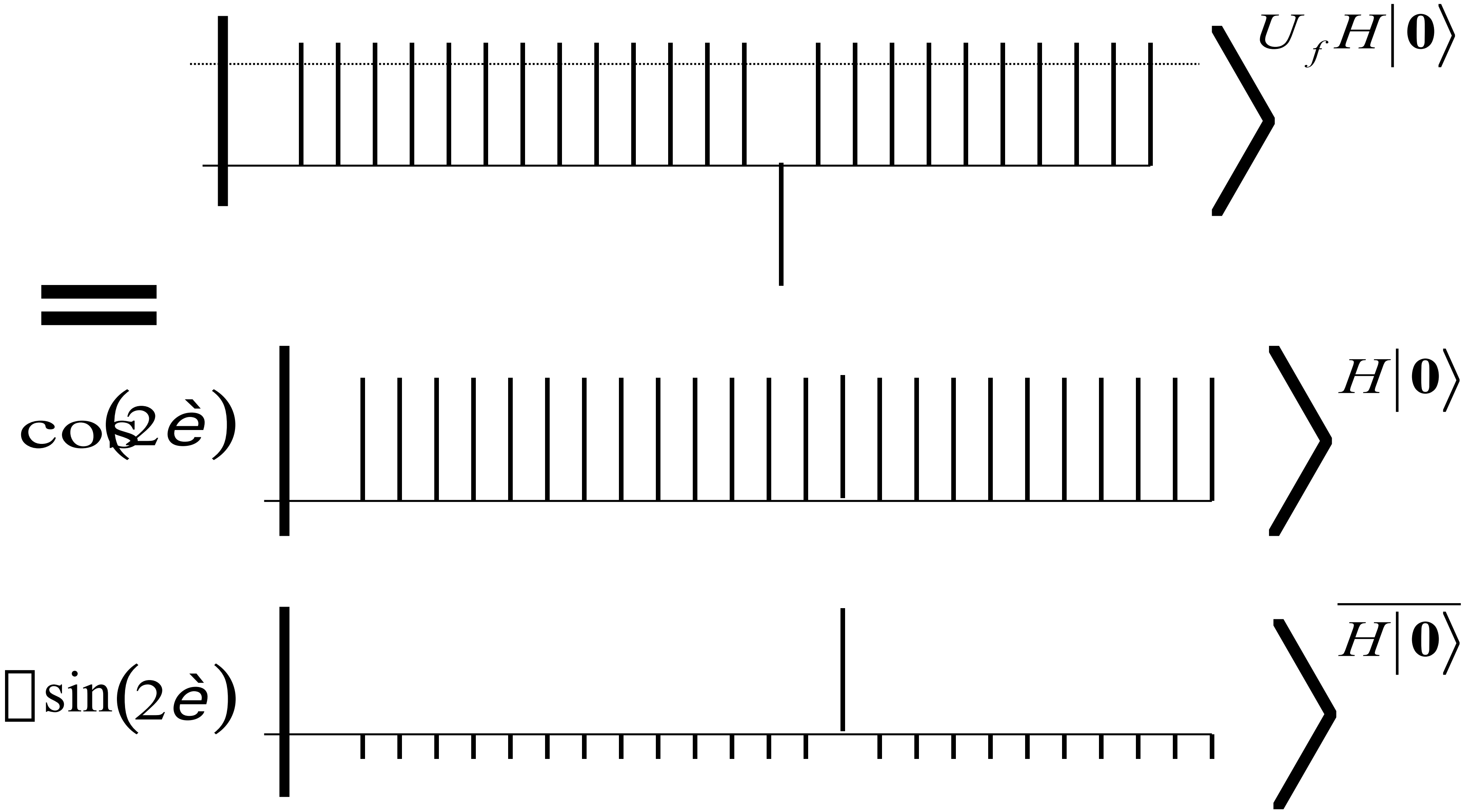
A nice way to analyze this



Definition



Note that


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

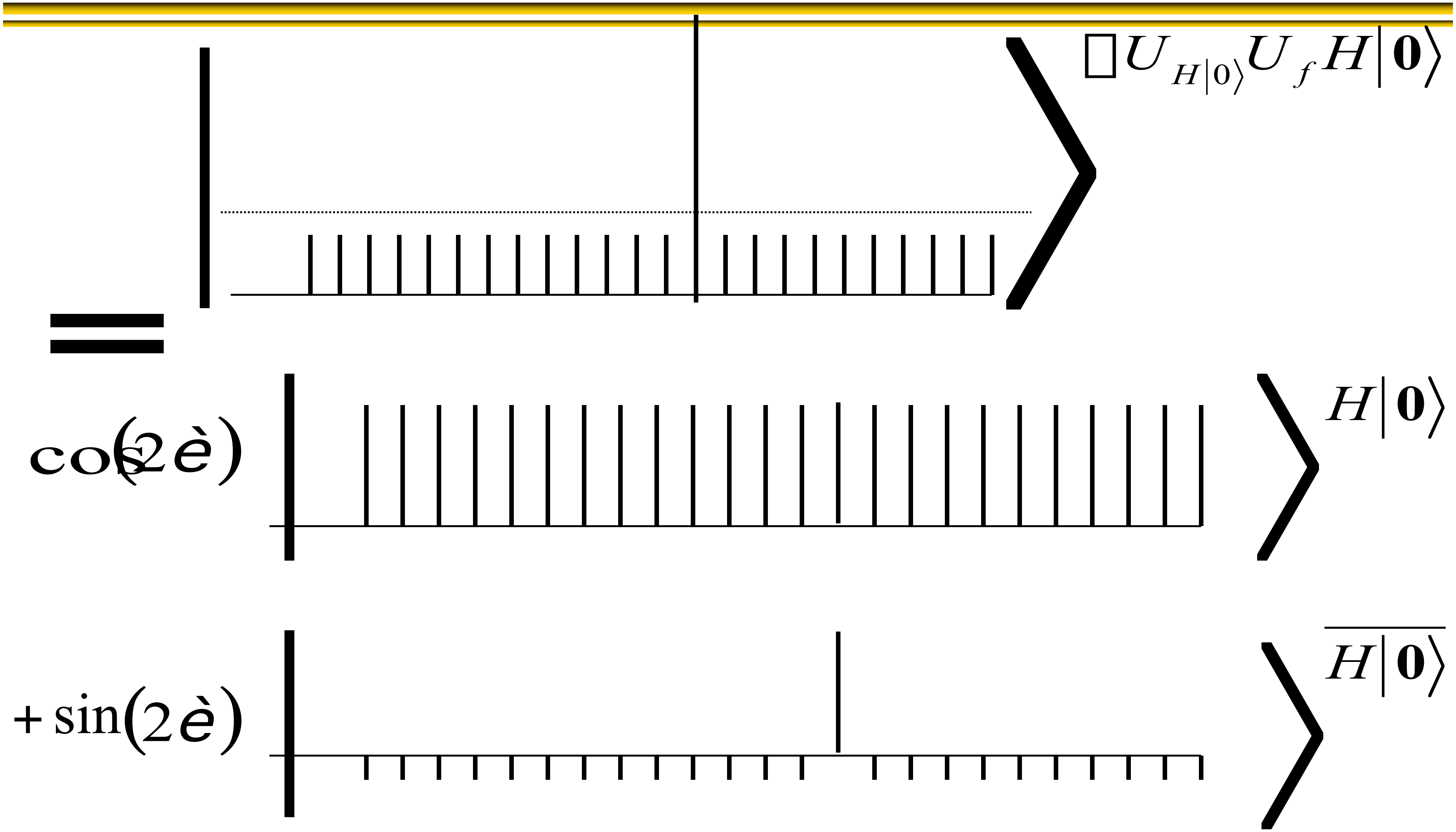
Verify that

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

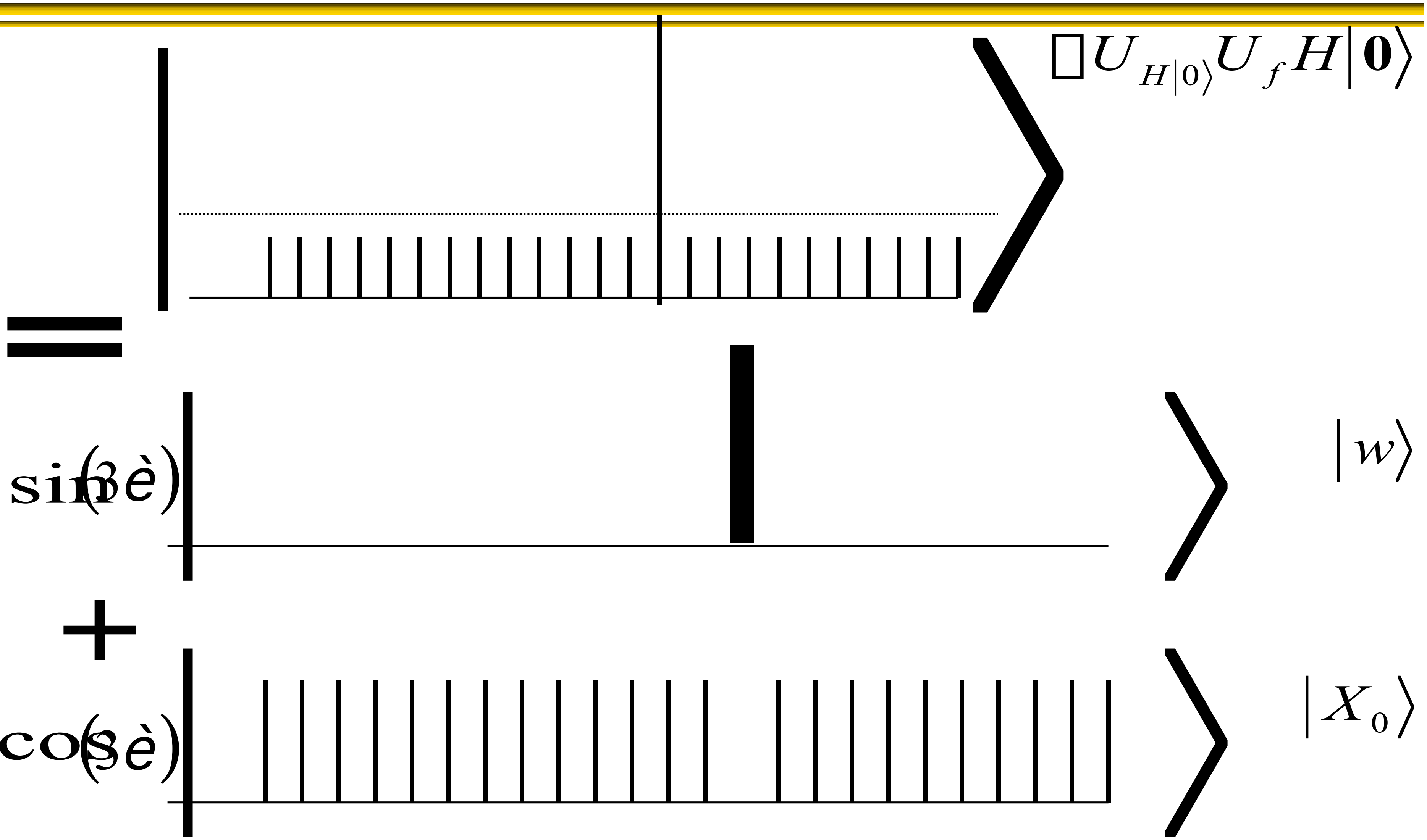
$$=$$

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

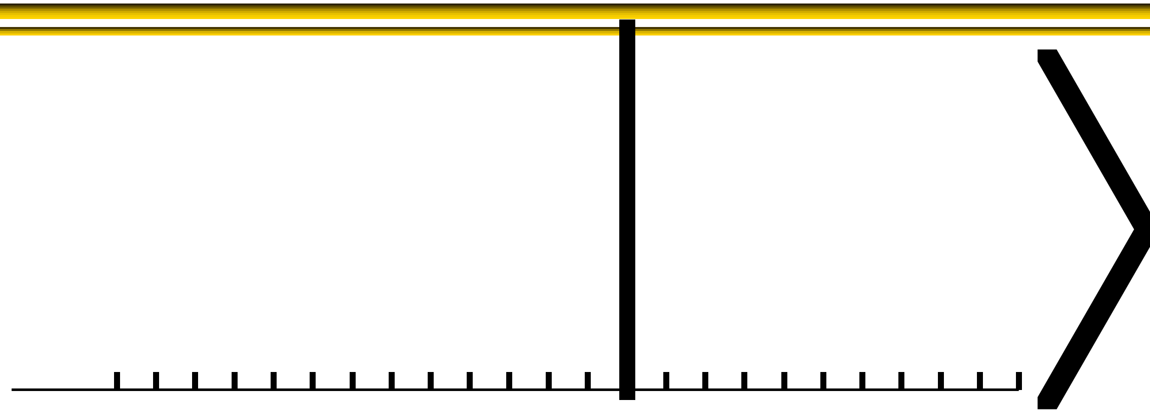
After "inversion"



Alternatively

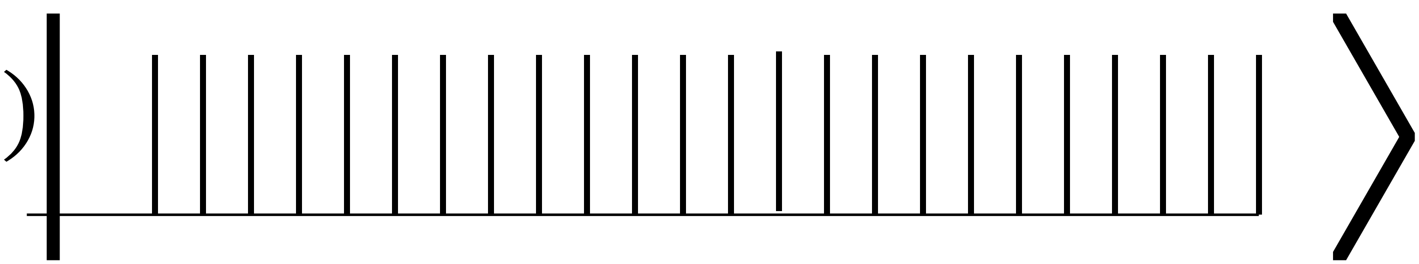


After k interations

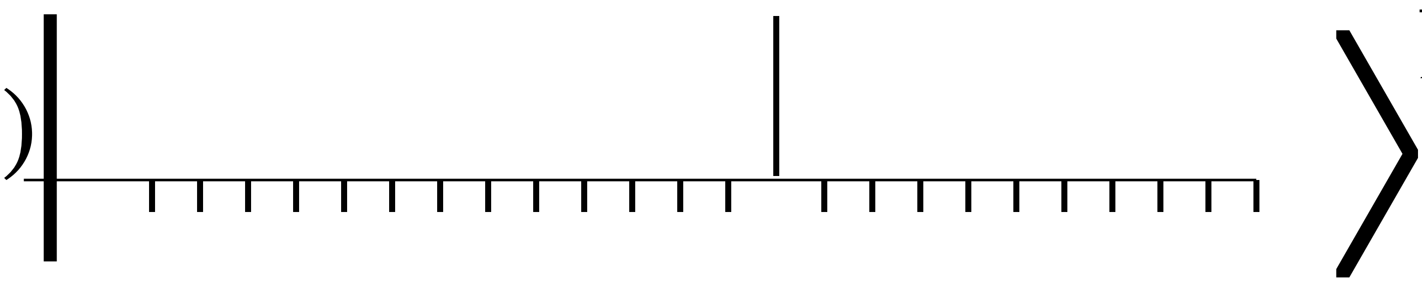


$$\left(-U_{H|0\rangle}U_f\right)^k H|\mathbf{0}\rangle$$

$=$



$$\cos(2k\theta)\, H|\mathbf{0}\rangle$$



$$+\sin(2k\theta)\, \overline{H|\mathbf{0}\rangle}$$

(*formula found by BBHT)

Alternatively

$$\left(-U_{H|0\rangle}U_f\right)^k H|\mathbf{0}\rangle = \sin\left((2k+1)\theta\right)|w\rangle + \cos\left((2k+1)\theta\right)|X_0\rangle$$

Selecting parameters

So we need

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

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

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

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

Consider any algorithm that works with non-zero probability

$$A|0\rangle = |\psi\rangle \qquad |\psi\rangle = \sin(\theta)|\psi_1\rangle + \cos(\theta)|\psi_0\rangle$$

$$|\psi_1\rangle = \sum_{x \in X_1} \alpha_x |x\rangle \qquad \sum_{x \in X_1} |\alpha_x|^2 = 1$$

$$|\psi_0\rangle = \sum_{y \in X_0} \beta_y |y\rangle \qquad \sum_{y \in X_0} |\beta_y|^2 = 1$$

Amplitude Estimation

- Given operators

$$A|0\rangle = |\text{Ø}\rangle = \sin(\text{è})|\text{Ø}_1\rangle + \cos(\text{è})|\text{Ø}_0\rangle$$

$$U_f : |\text{Ø}_1\rangle \text{ a } \square|\text{Ø}_1\rangle$$
$$|\text{Ø}_0\rangle \text{ a } |\text{Ø}_0\rangle$$

$$\sin^2(\text{è})$$

- Estimate

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 $\sin(\theta) = \sqrt{\frac{t}{N}}$

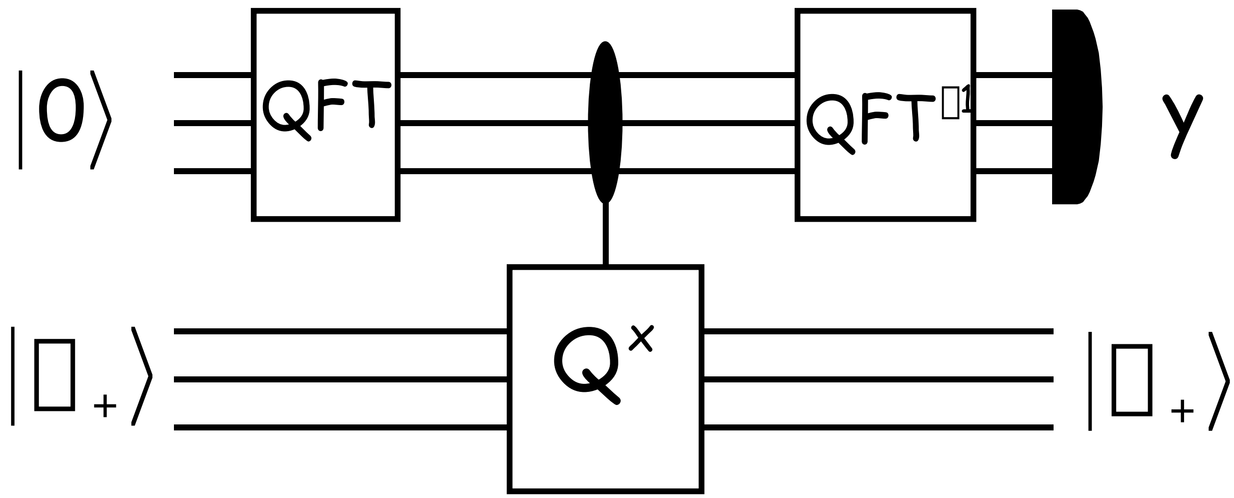
Eigenvectors of Q

$$\left|\phi_+\right\rangle = \frac{1}{\sqrt{2}}\left|\phi_0\right\rangle + \frac{i}{\sqrt{2}}\left|\phi_1\right\rangle$$

$$\left|\phi_-\right\rangle = \frac{1}{\sqrt{2}}\left|\phi_0\right\rangle - \frac{i}{\sqrt{2}}\left|\phi_1\right\rangle$$

$$Q\left|\phi_+\right\rangle = e^{i2\theta}\left|\phi_+\right\rangle \qquad Q\left|\phi_-\right\rangle = e^{-i2\theta}\left|\phi_-\right\rangle$$

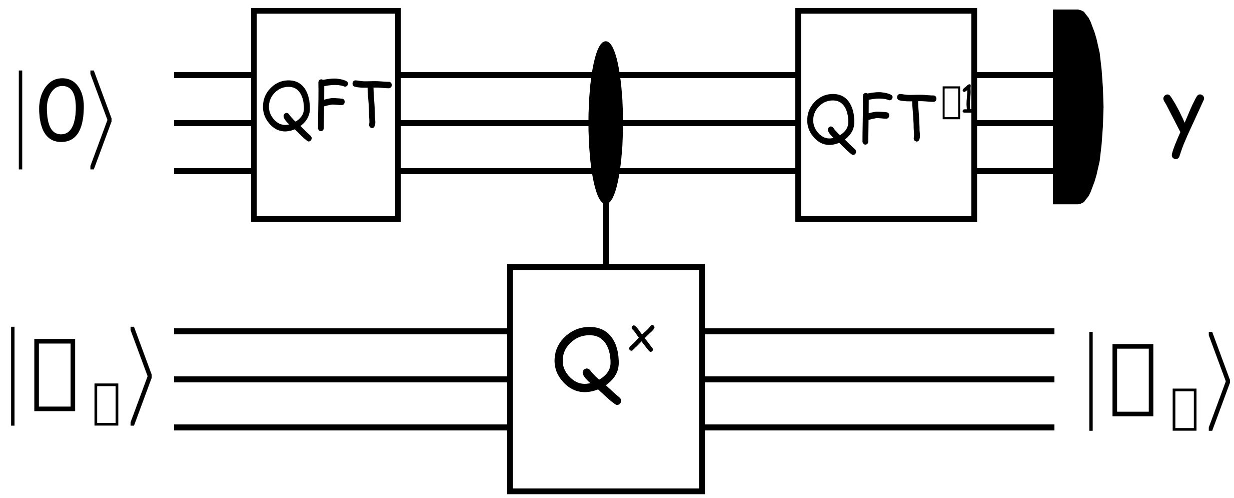
Amplitude Estimation
≈ Eigenvalue Estimation



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

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

Amplitude Estimation ⇒ Eigenvalue Estimation

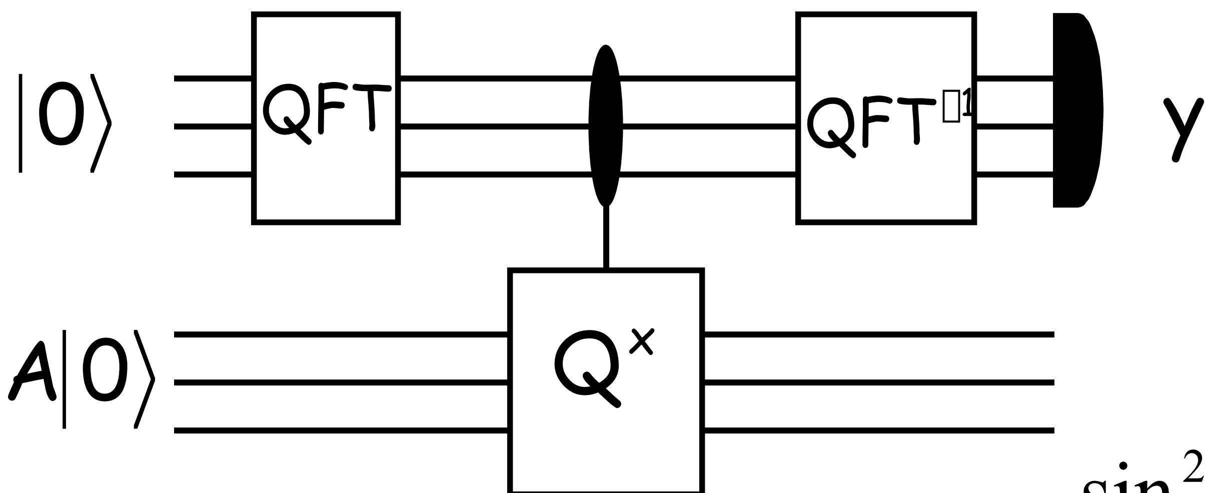


$$\frac{2\pi y}{N} \approx 2\pi \approx 2\theta$$

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

Amplitude Estimation □ Eigenvalue Estimation

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



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

(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 $$\Omega\left(\frac{1}{\sqrt{(t+1)(2^n - t + 1)}}\right)$$

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

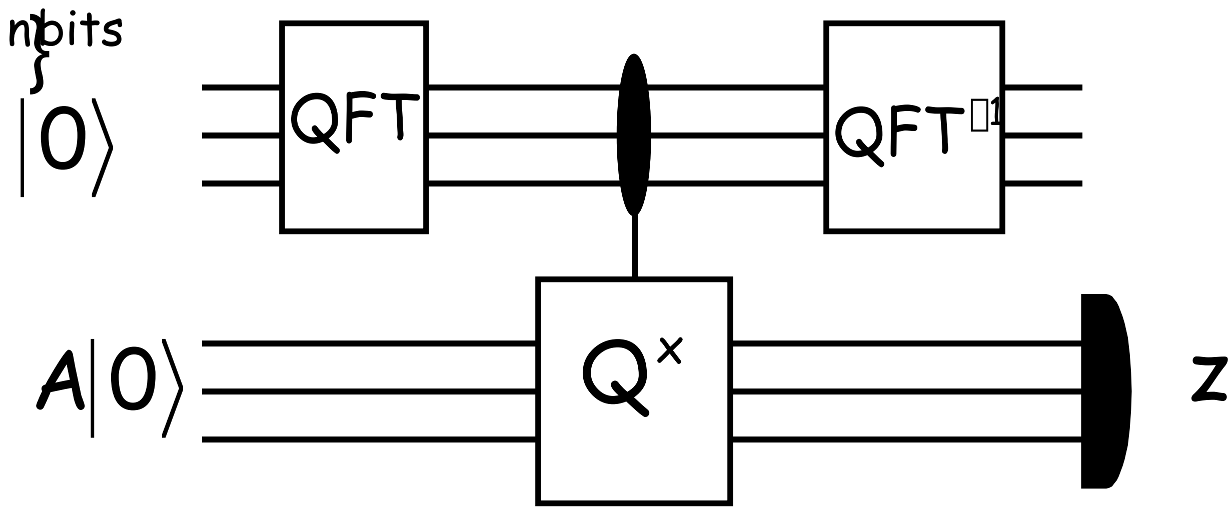
Note that the amplitude estimation network produces states

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

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

$$\frac{1}{2}\left|\psi_{+}\right\rangle\left\langle\psi_{+}\right| + \frac{1}{2}\left|\psi_{-}\right\rangle\left\langle\psi_{-}\right| = \frac{1}{2}\left|\psi_{1}\right\rangle\left\langle\psi_{1}\right| + \frac{1}{2}\left|\psi_{0}\right\rangle\left\langle\psi_{0}\right|$$

Searching when we don't know the number of solutions



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

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

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 $2^n > \frac{1}{\square}$ we will find a satisfying x with probability in

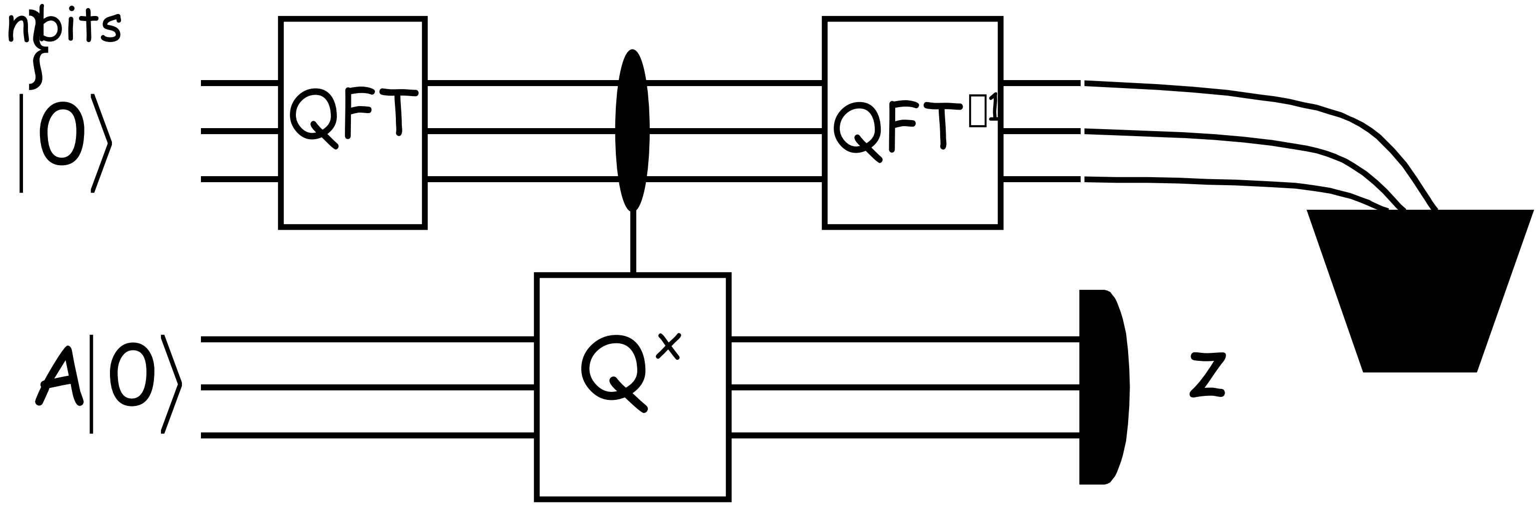
$$\frac{3}{4} \square O\left(\frac{1}{2^n \square}\right)$$

This means the expected running time is in

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

The way BBHT do it

Notice



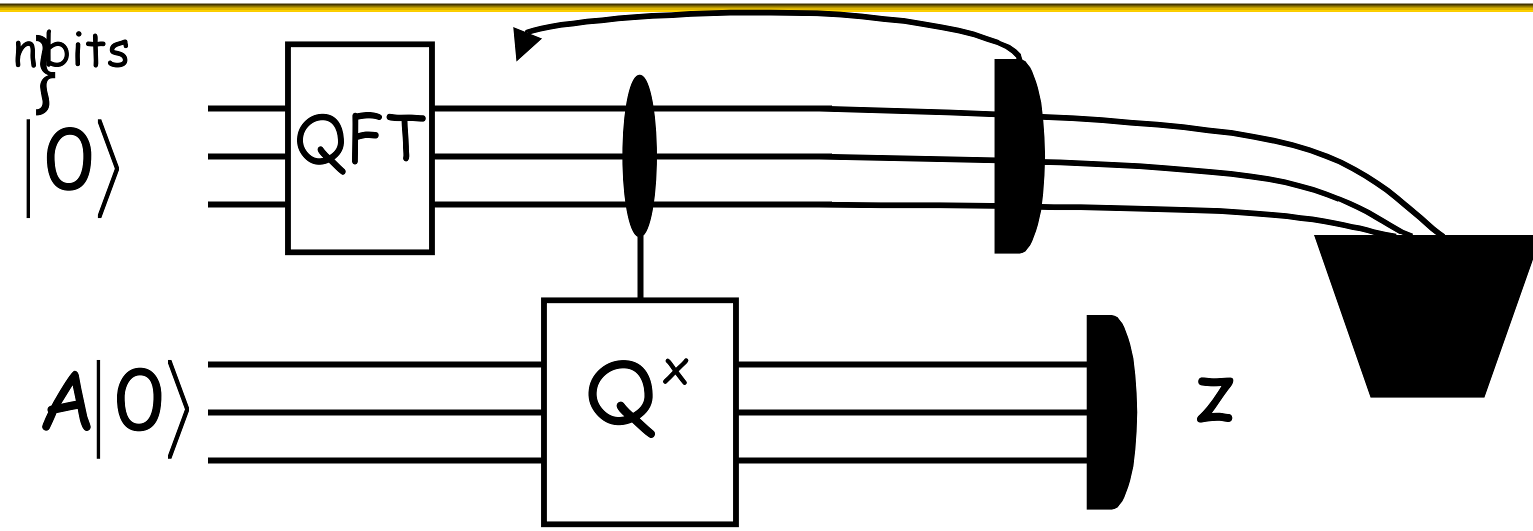
$$\mathrm{Prob}(f(z)=1) \geq \frac{1}{2} - O\left(\frac{1}{2^n}\right)$$

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

$$n \to \infty$$

The way BBHT do it

Notice



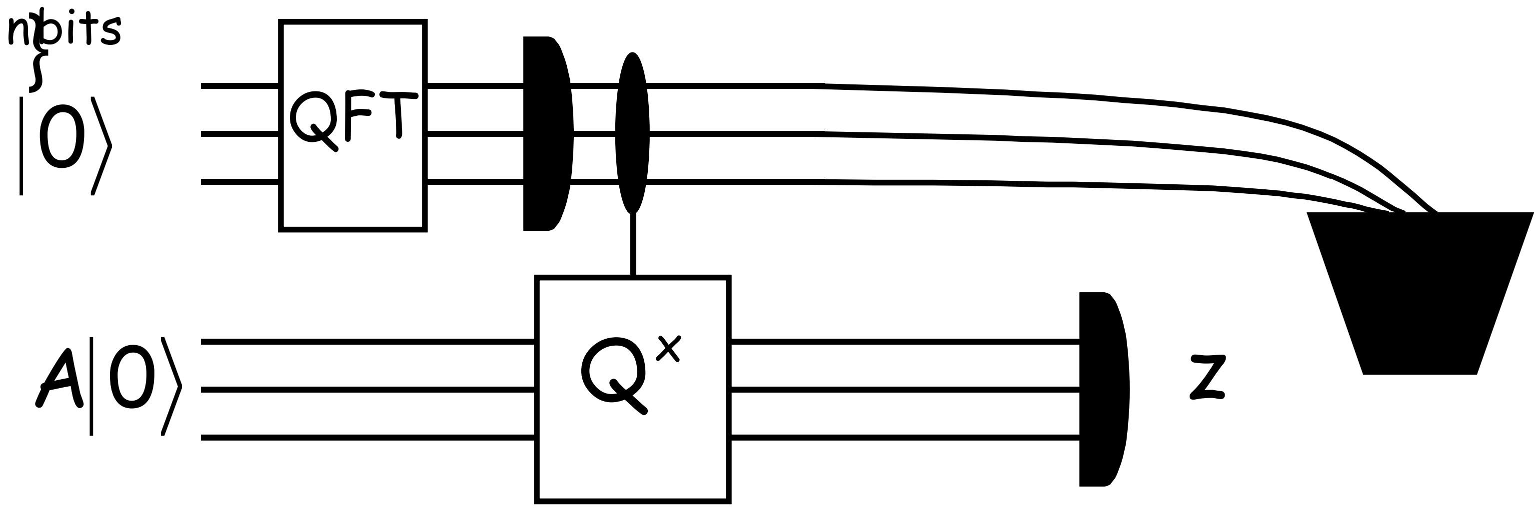
$$\mathrm{Prob}(f(z)=1) \approx \frac{1}{2} \pm O\left(\frac{1}{2^n}\right)$$

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

$$n \to \infty$$

The way BBHT do it

Notice



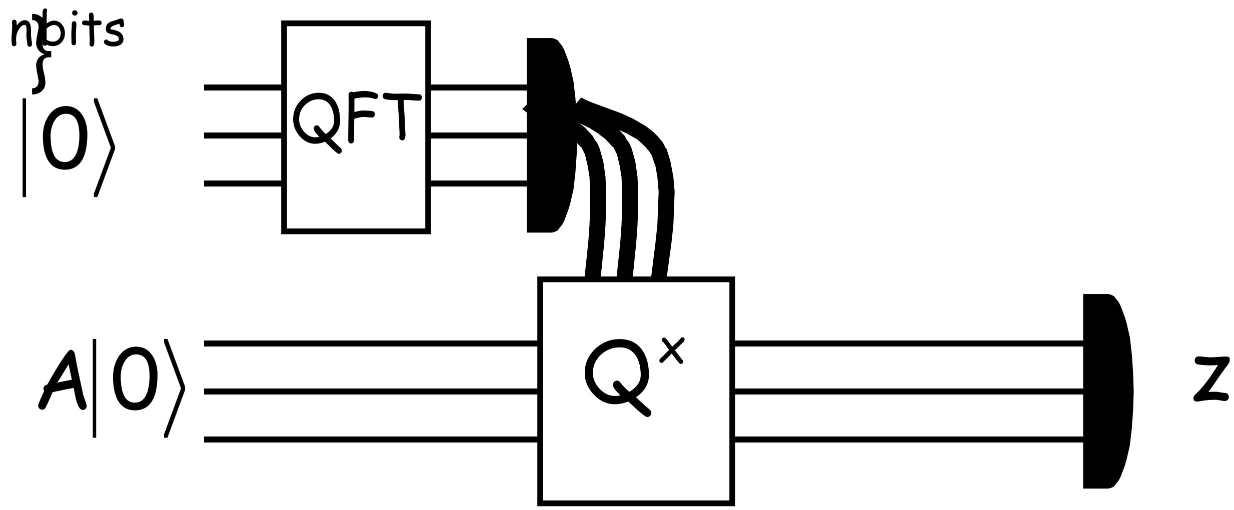
$$\text{Prob}(f(z)=1) \; \square \; \frac{1}{2} \; \square \; O\square \frac{1}{2^n \square} \square$$

$$\text{Prob}(f(z)=1) \; \square \; \frac{1}{2}$$

$$n \; \square$$

The way BBHT do it

Notice



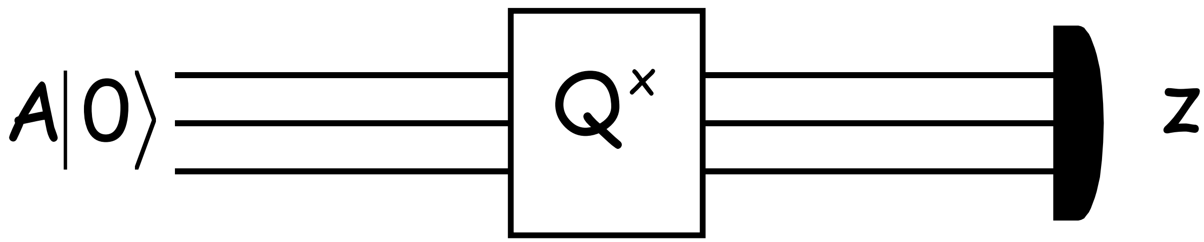
$$\mathrm{Prob}(f(z)=1) \Box \frac{1}{2} \Box O\Box\frac{1}{2^n}\Box\Box$$

$$\mathrm{Prob}(f(z)=1) \Box \frac{1}{2}$$

$$n \Box$$

The way BBHT do it

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



$$\mathrm{Prob}(f(z)=1) \, \square \, \frac{1}{2} \, \square \, O\left(\frac{1}{2^n \, \square}\right)$$

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