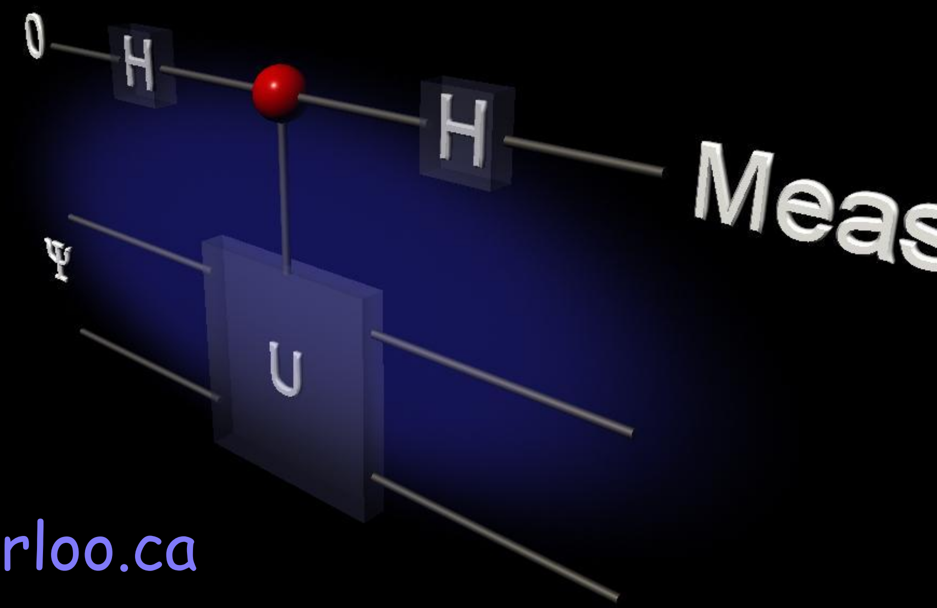
Introduction to Quantum Information Processing



CO481 CS467 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

Institute for Quantum Computing

UNIVERSITY OF WATERLOO

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

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

$$U_f : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$$

Find an x satisfying $f(x) = 1$

Can assume we have:

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

Application

Consider a 3-SAT formula

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

$$\boxed{\begin{array}{c} C_j = (y_{j,1} \vee y_{j,2} \vee y_{j,3}) \\ \\ y_{j,k} \in \{x_1, x_2, \cdots, x_n, \bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n\} \end{array}}$$

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

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

Some ideas

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

IDEA:

Prepare

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

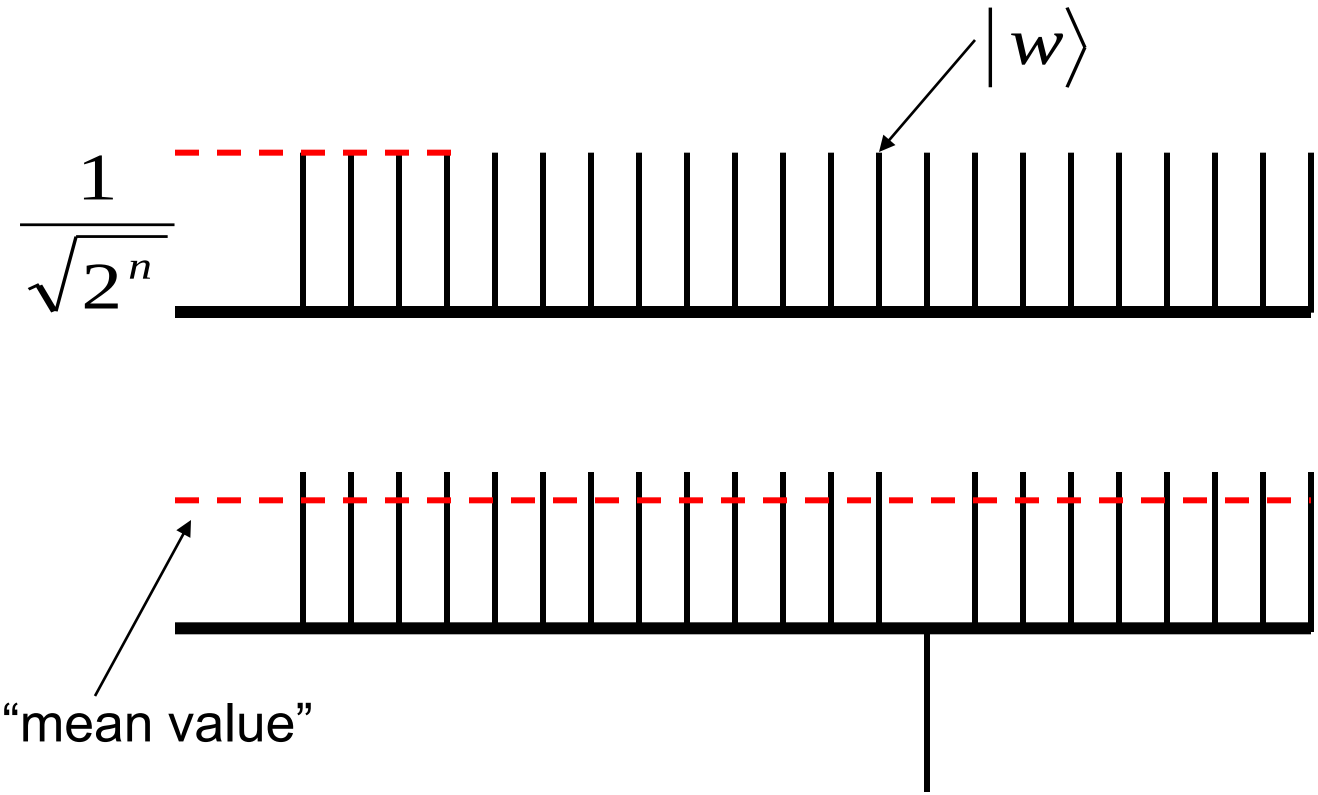
Keep this

"Re-scramble" this

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

! Must be done with legal quantum operation

Grover’s idea:



$$= H|00\cdots0\rangle$$

$$= U_f H|00\cdots0\rangle$$

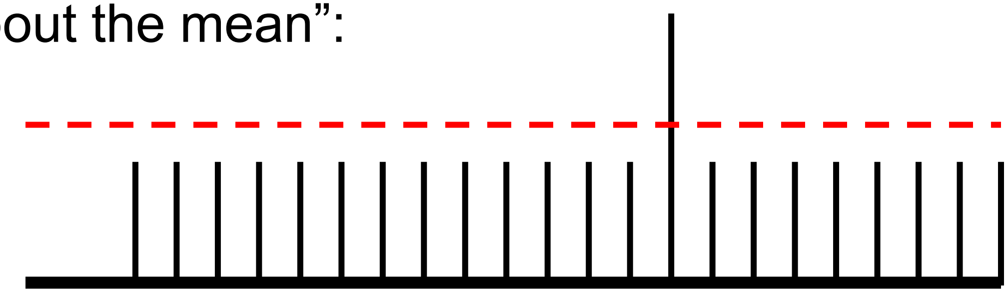
! Must be done with legal quantum operation

We define for an arbitrary quantum pure state $|\psi\rangle$

$$U_{|\psi\rangle} : |\omega\rangle \mapsto |\omega\rangle, \text{ if } |\omega\rangle \perp |\psi\rangle$$

$$|\psi\rangle \mapsto -|\psi\rangle$$

"invert about the mean":

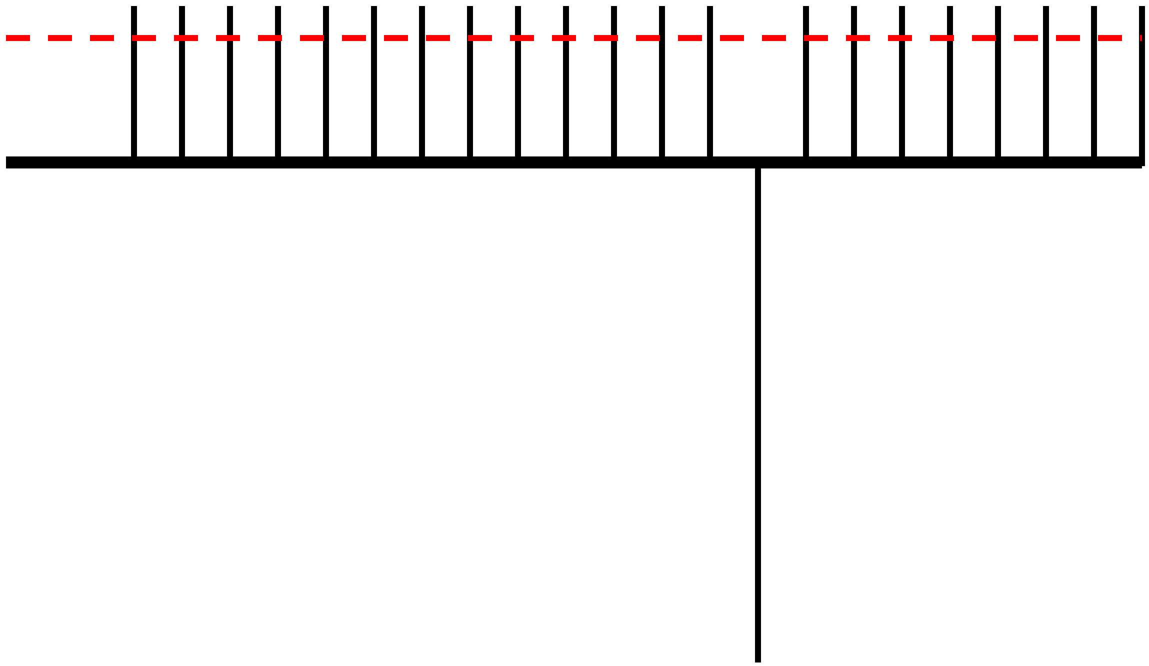


$$= \left(-HU_0 H\right) U_f H |00\cdots 0\rangle$$

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

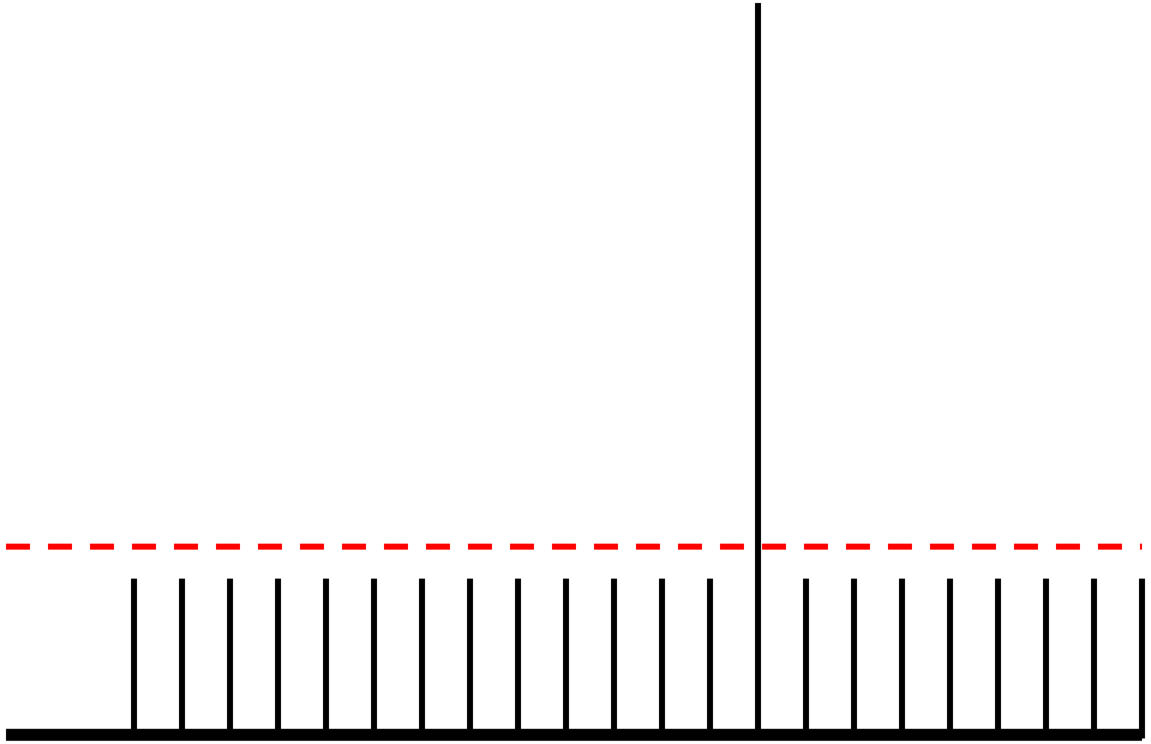
Repeat

$$= U_f \left(- H U_0 H \right) U_f H \left| 00 \cdots 0 \right\rangle$$

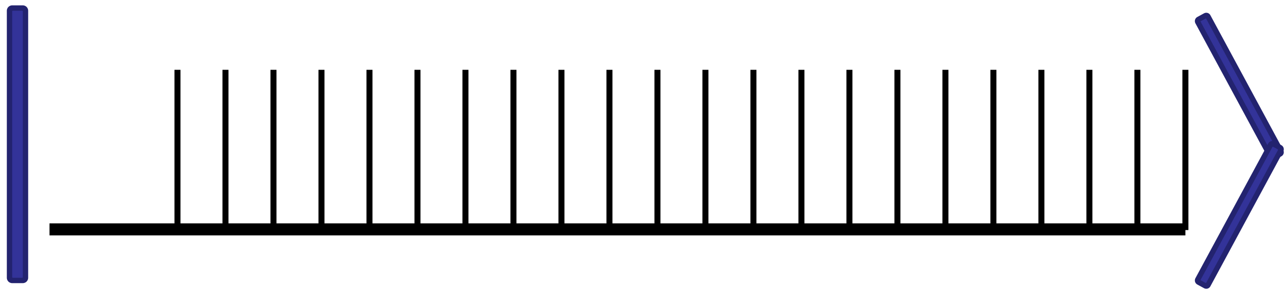


Repeat

$$= \left(-HU_0H\right)U_f\left(-HU_0H\right)U_f H\left|00\cdots0\right\rangle$$



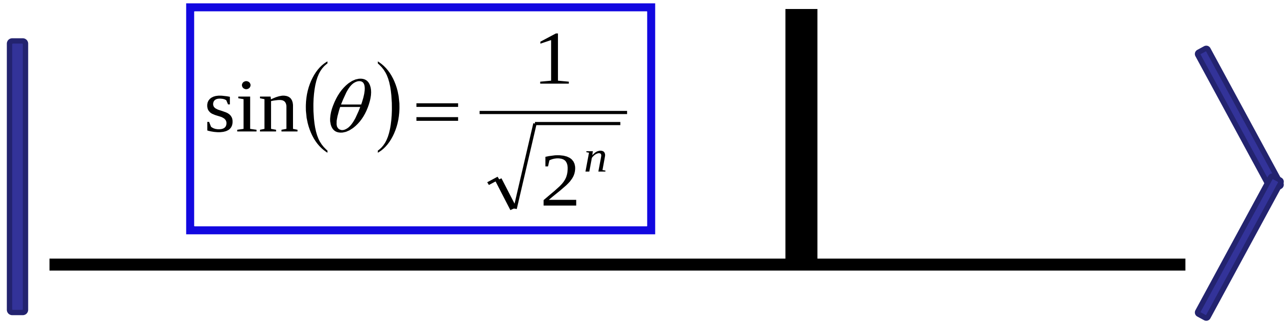
A nice way to analyze this



$$H|\mathbf{0}\rangle$$

$$=$$

$$\sin(\theta)$$

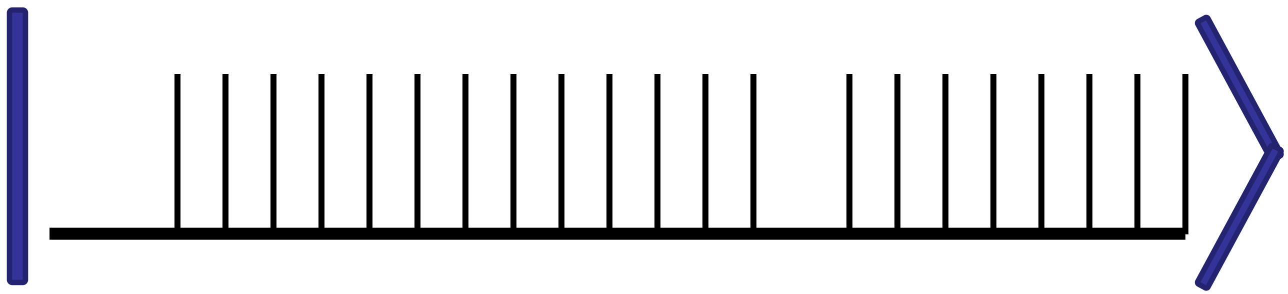


$$\sin(\theta)=\frac{1}{\sqrt{2^n}}$$

$$|w\rangle$$

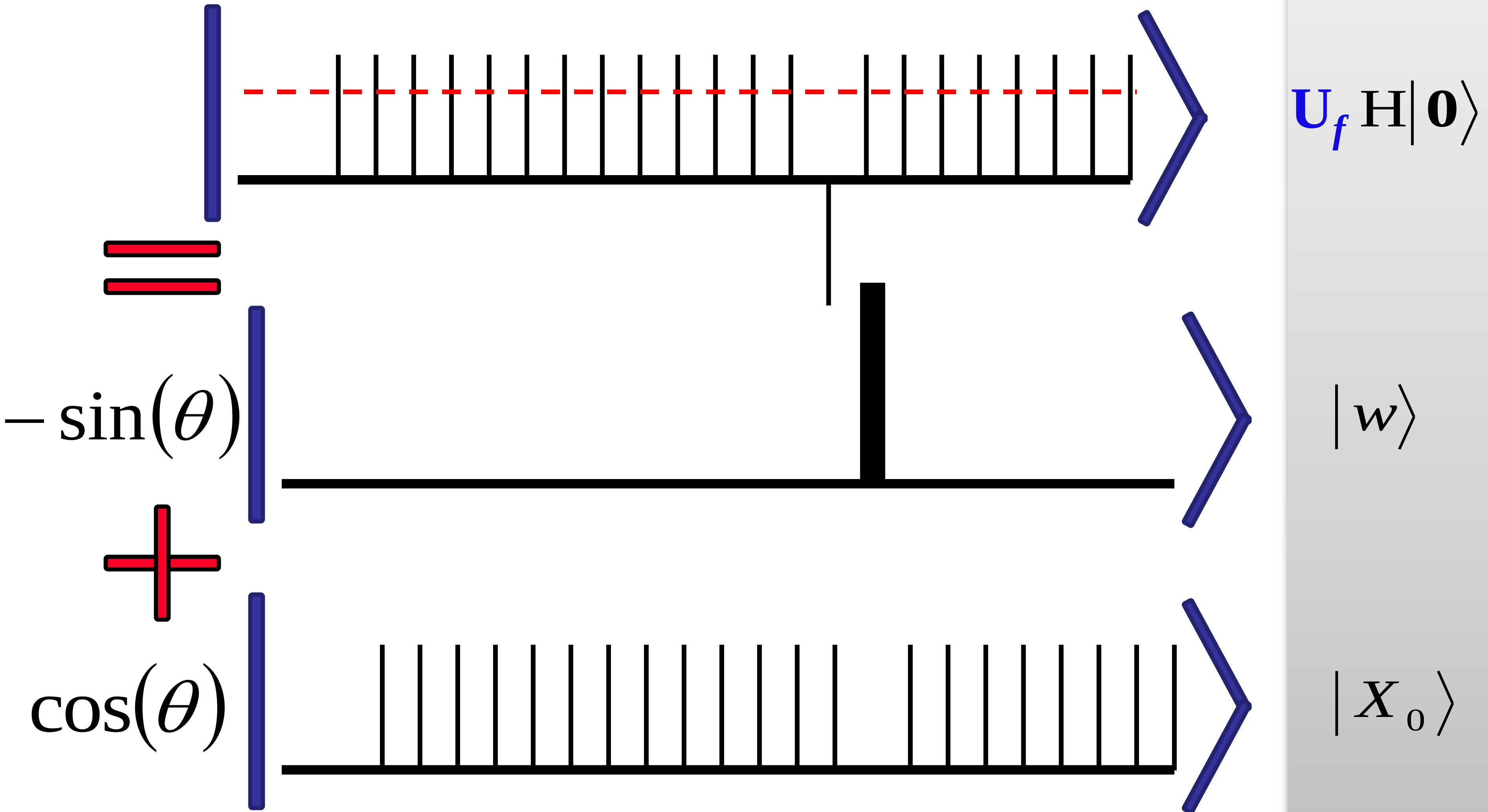
$$+$$

$$\cos(\theta)$$

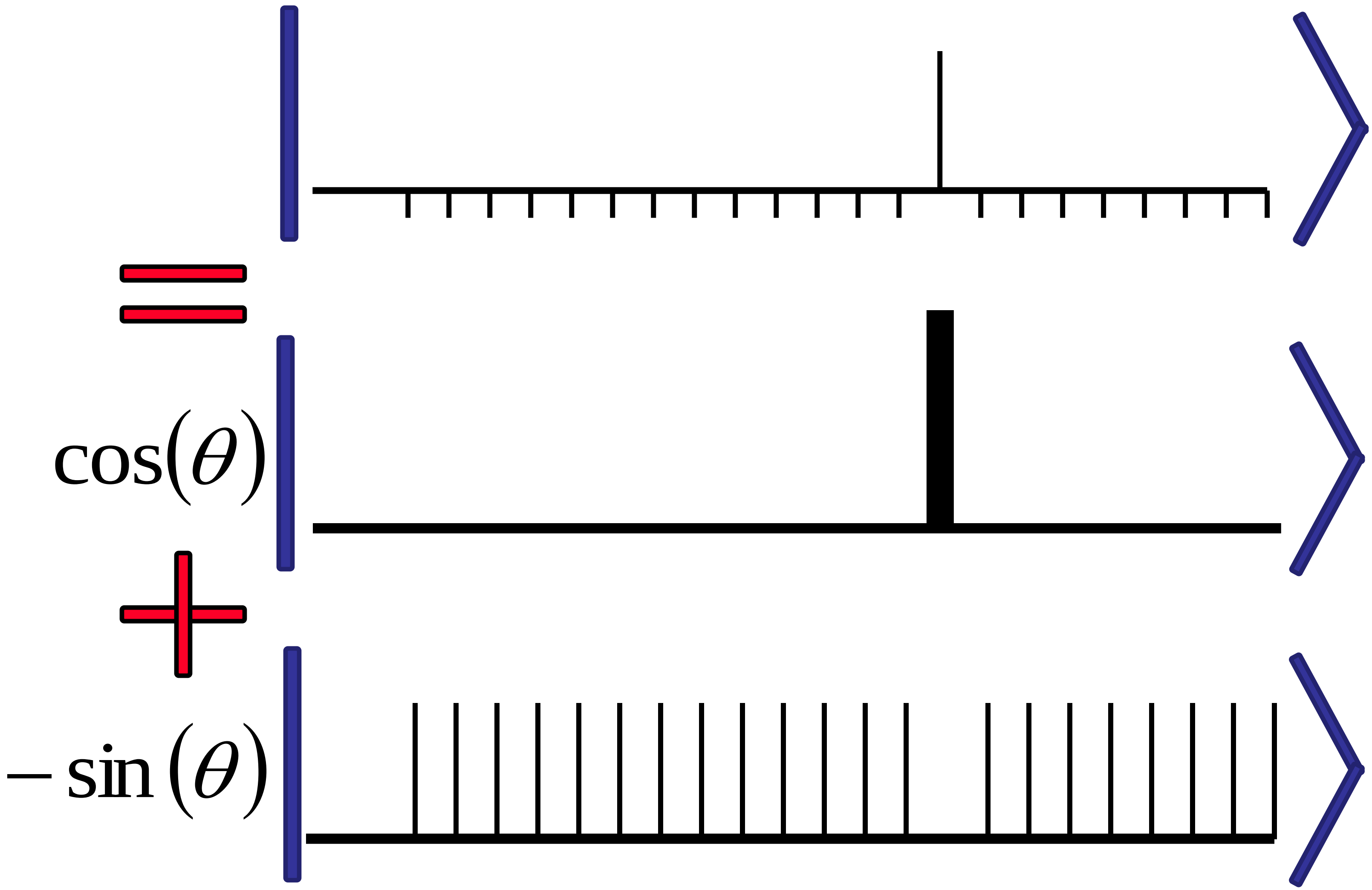


$$|X_0\rangle$$

A nice way to analyze this



Definition

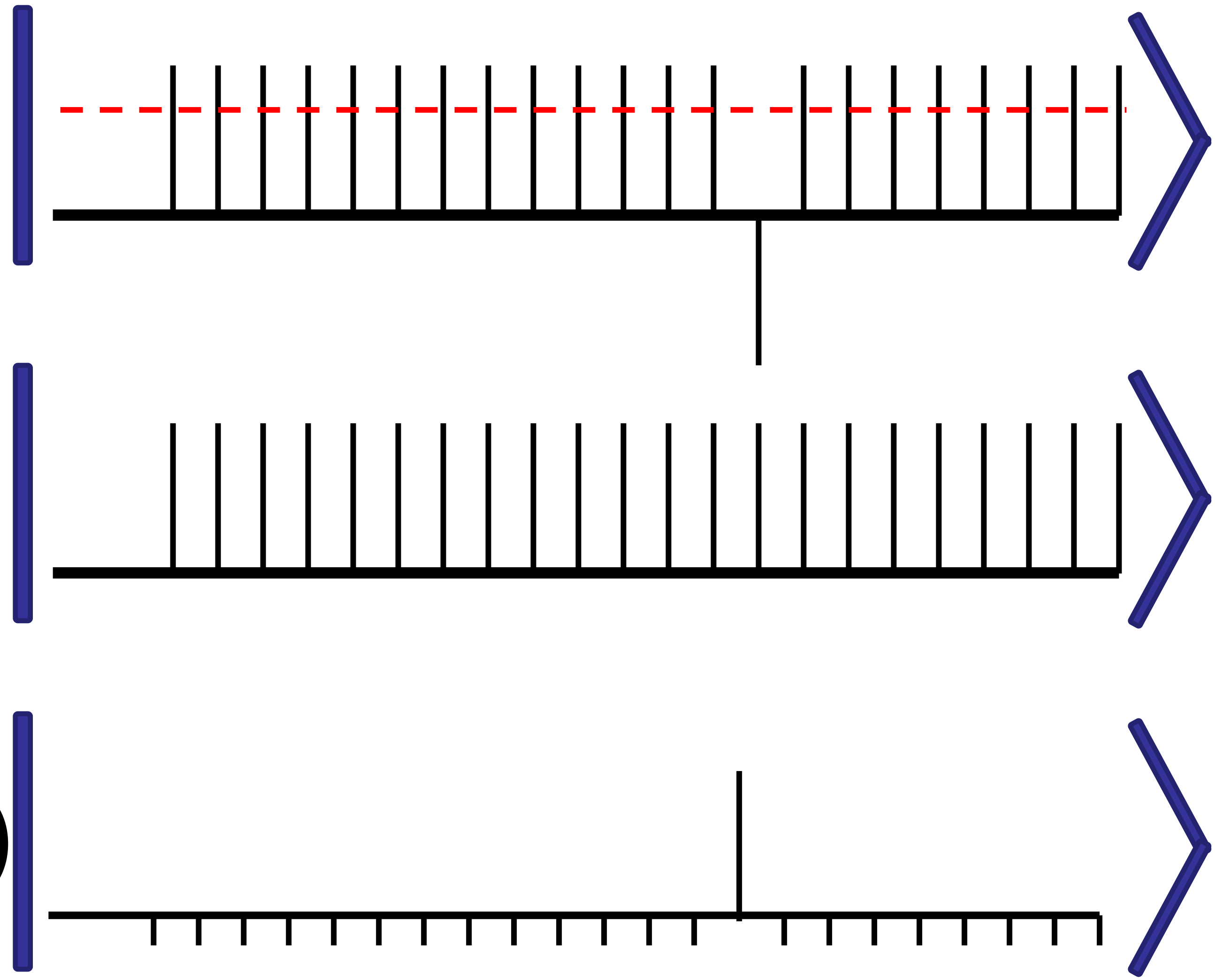


$\overline{H|\mathbf{0}\rangle}$

$|w\rangle$

$|X_0\rangle$

Note that …



$$U_f \, \mathrm{H}|\mathbf{0}\rangle = \cos(2\theta)\, \mathrm{H}|\mathbf{0}\rangle + \left(-\sin(2\theta)\right) \overline{H|\mathbf{0}\rangle}$$

Verify that

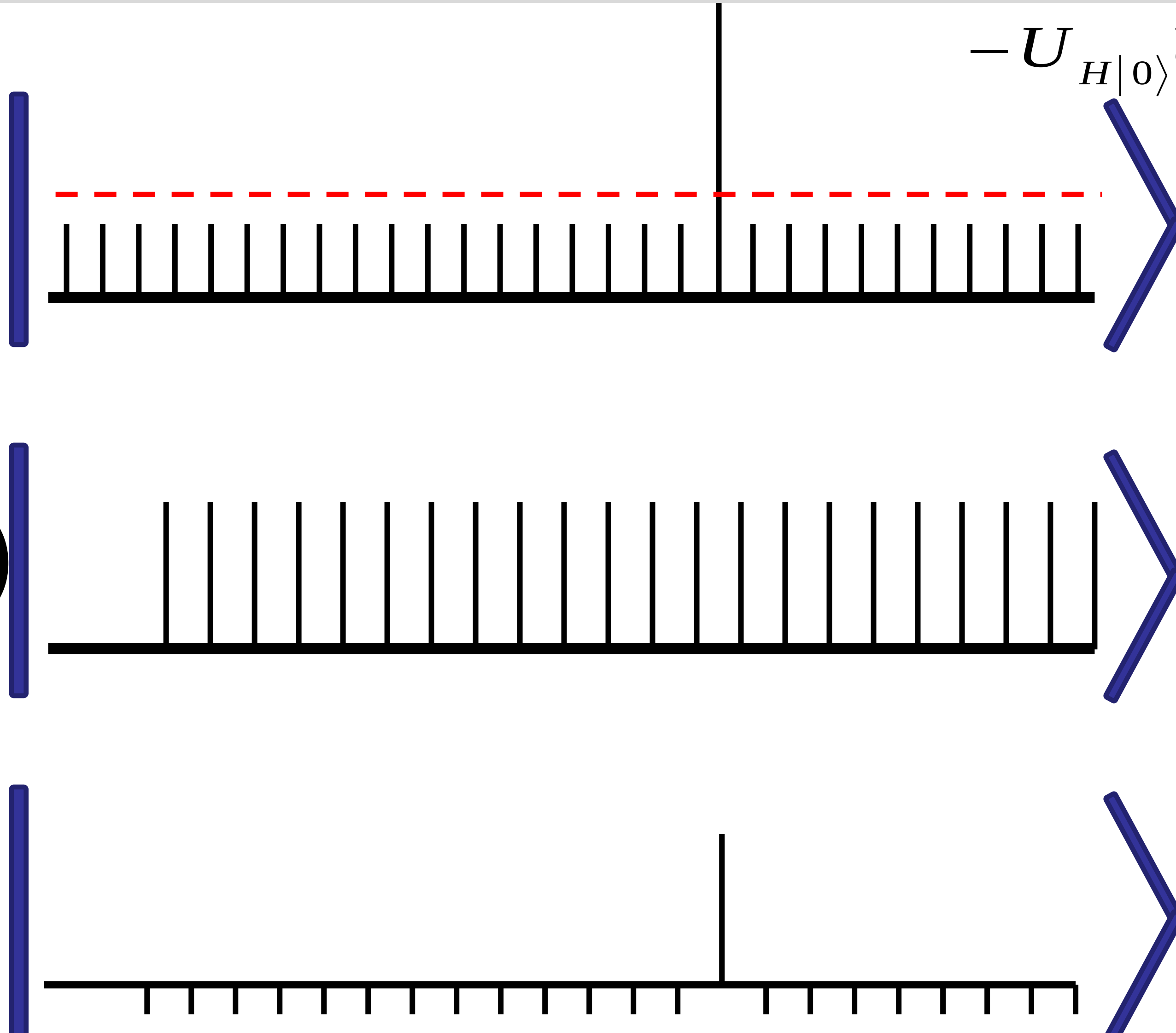
$$-\sin(\theta)|w\rangle + \cos(\theta)|X_0\rangle$$

$$=$$

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

After “inversion”

$$-U_{H|0\rangle}U_f H|\mathbf{0}\rangle$$



$=$

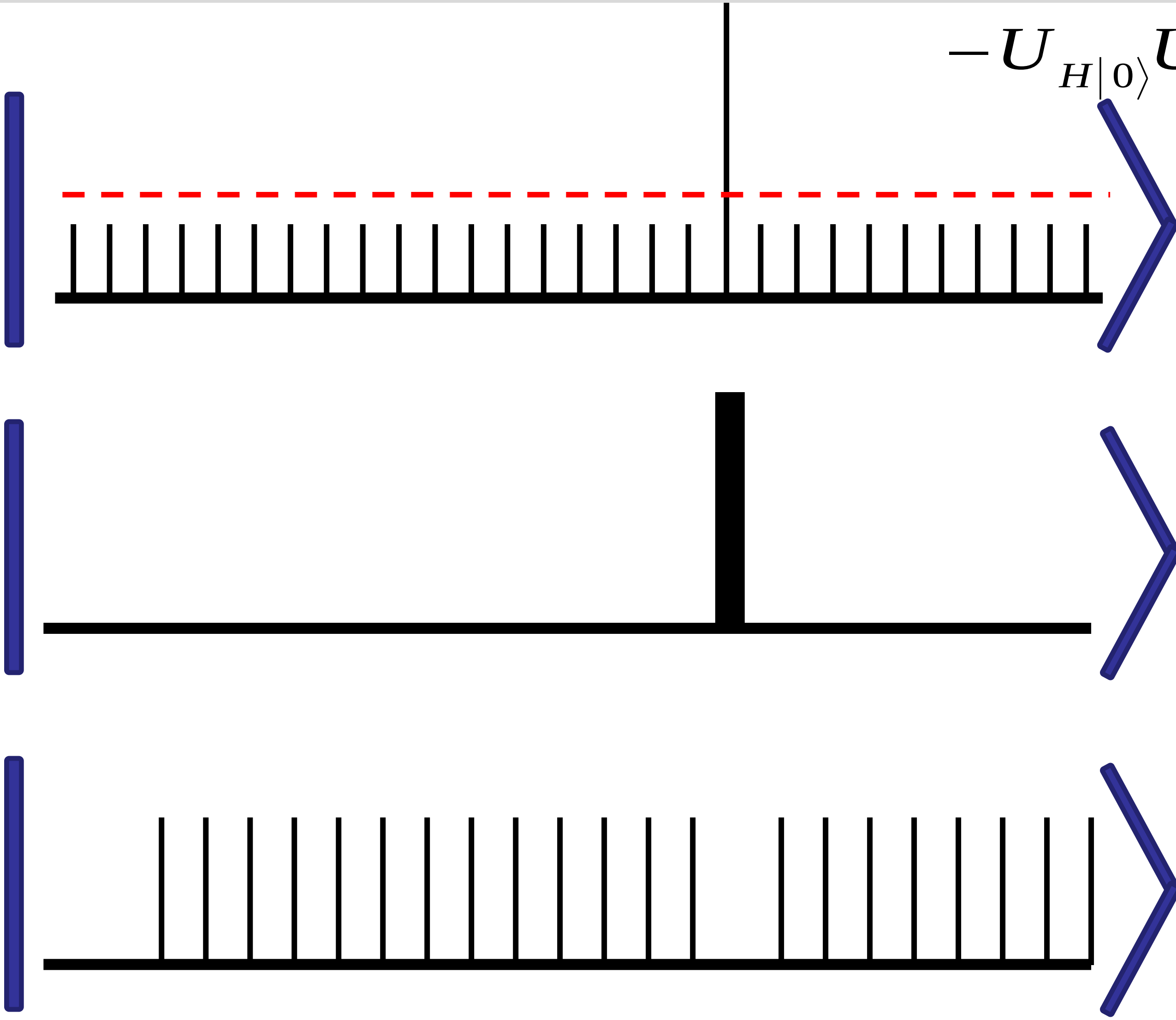
$\cos(2\theta)$ $\mathrm{H}|\mathbf{0}\rangle$

$+$

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

Alternatively

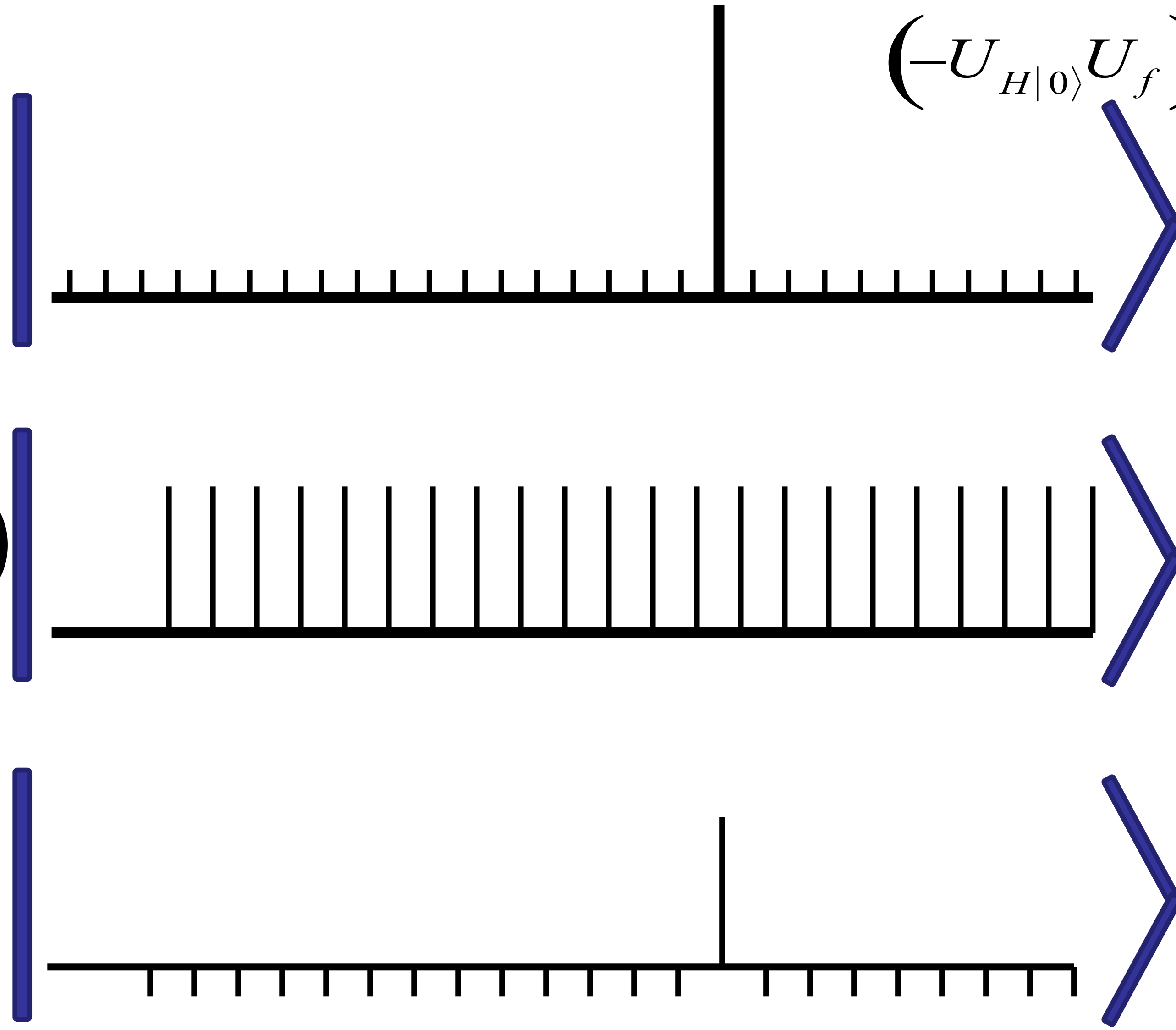
$$-U_{H|0\rangle} U_f H|\mathbf{0}\rangle$$



$$= \sin(3\theta)\,|w\rangle + \cos(3\theta)\,|X_0\rangle$$

After *k* iterations

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



$=$

$\cos(2k\theta)$

$\mathrm{H}|\mathbf{0}\rangle$

$+$

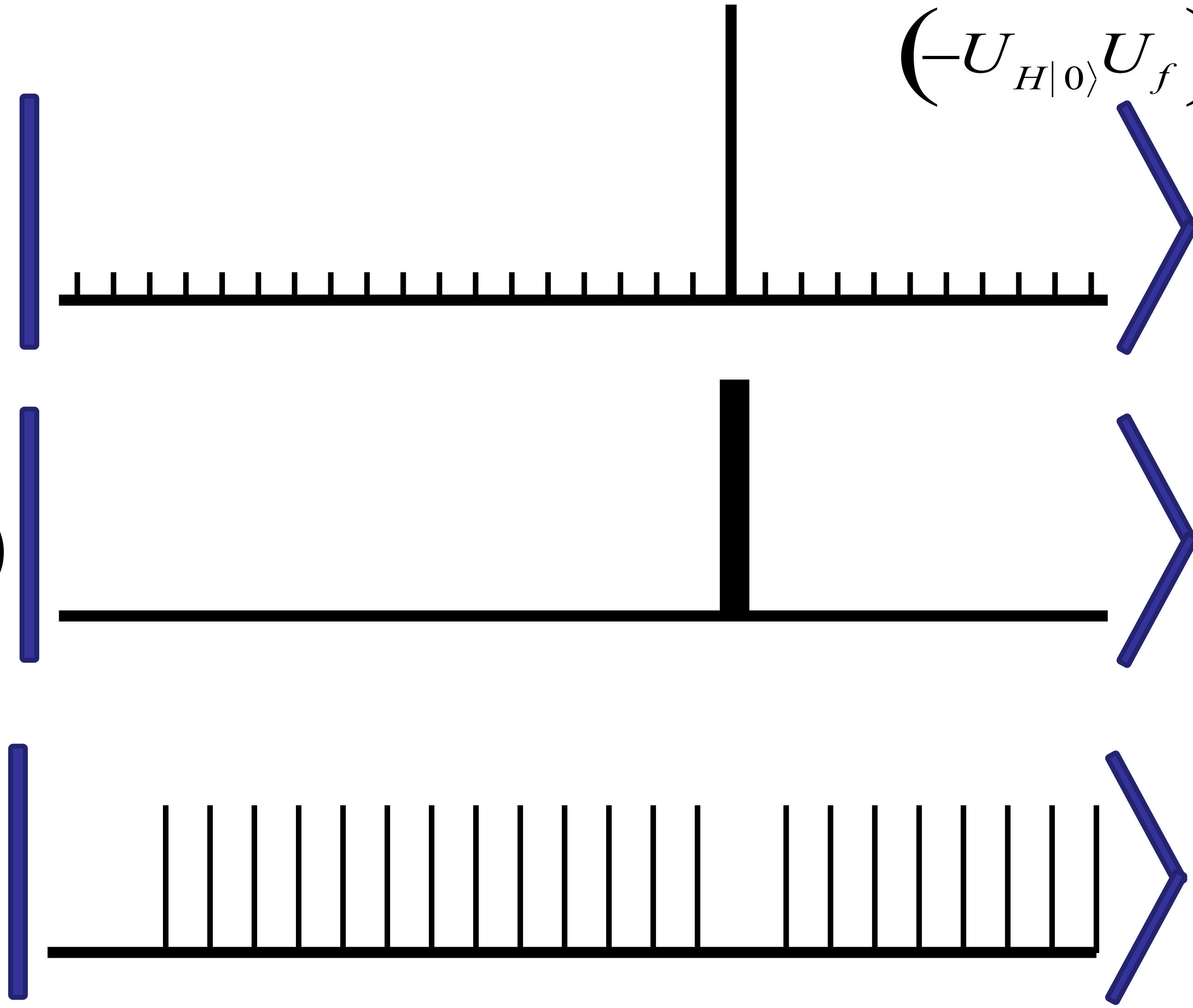
$\sin(2k\theta)$

$\overline{H|\mathbf{0}\rangle}$

Alternatively

*formula found by BBHT

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



$$= \sin\left((2k+1)\theta\right)|w\rangle + \cos\left((2k+1)\theta\right)|X_0\rangle$$

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!

We can prove this is optimal (see section 9.3 of the book)

What if we don't know the number of solutions? (…later)

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 $p = \sin^2(\theta)$

$$A|0\rangle = |\Psi\rangle$$

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

$$|\Psi_1\rangle = \sum_{x \in X_1} \alpha_x |x\rangle$$

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

$$|\Psi_0\rangle = \sum_{y \in X_0} \alpha_y |y\rangle$$

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

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

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

$$Q = -AU_0A^{-1}U_f$$

$$Q^k A|0\rangle = \sin((2k+1)\theta)|\psi_1\rangle + \cos((2k+1)\theta)|\psi_0\rangle$$

We need

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx O\left(\frac{1}{\sqrt{p}}\right)$$

Square root speed-up!

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

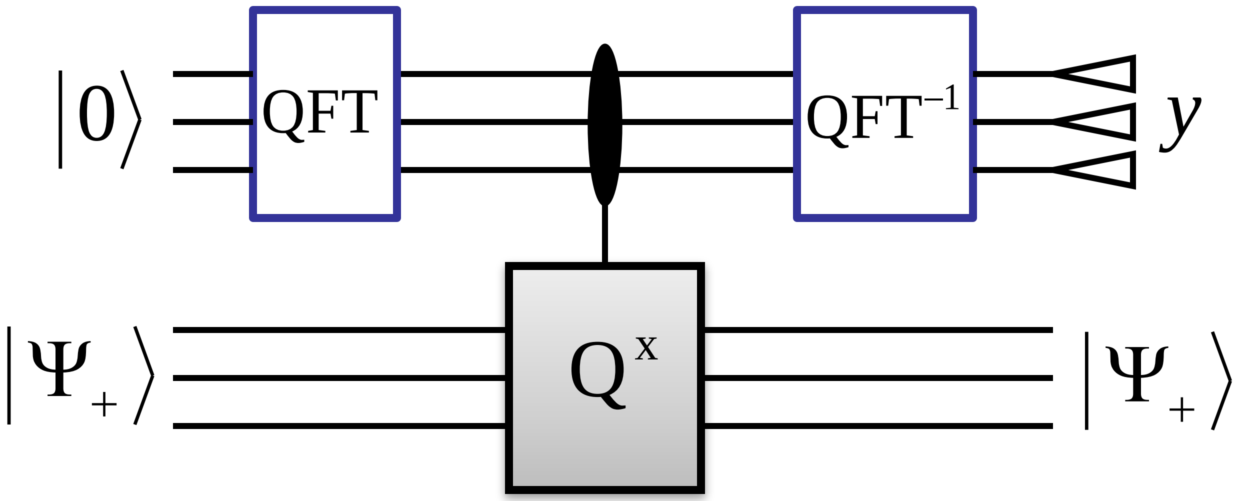
$$\left|\Psi_{+}\right\rangle = \frac{1}{\sqrt{2}}\left|\Psi_{0}\right\rangle + \frac{i}{\sqrt{2}}\left|\Psi_{1}\right\rangle$$

$$\left|\Psi_{-}\right\rangle = \frac{1}{\sqrt{2}}\left|\Psi_{0}\right\rangle - \frac{i}{\sqrt{2}}\left|\Psi_{1}\right\rangle$$

$$Q\left|\Psi_{+}\right\rangle = e^{i2\theta}\left|\Psi_{+}\right\rangle$$

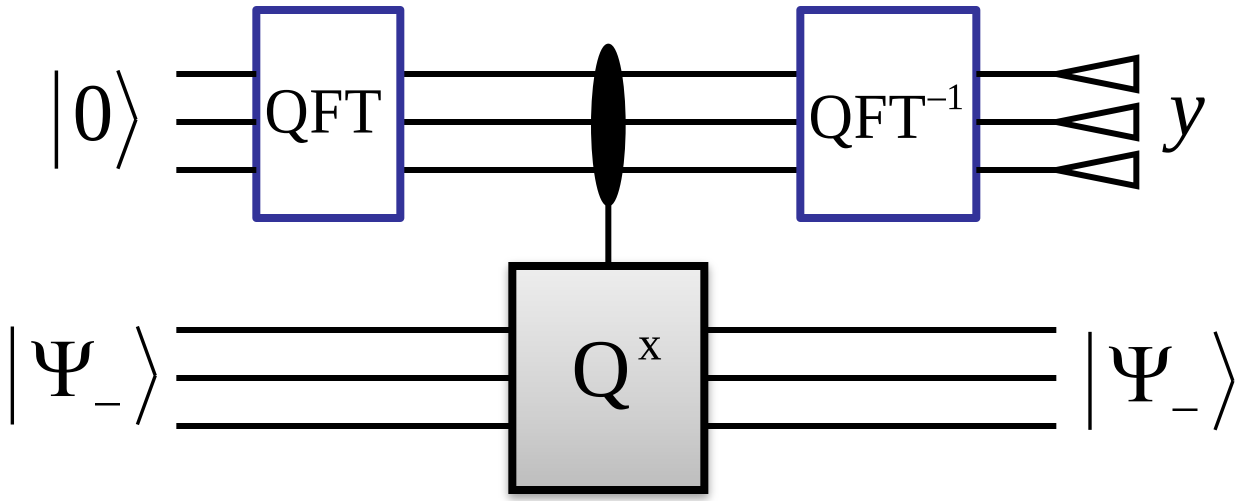
$$Q\left|\Psi_{-}\right\rangle = e^{-i2\theta}\left|\Psi_{-}\right\rangle$$

Amplitude estimation ≈ Eigenvalue estimation



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

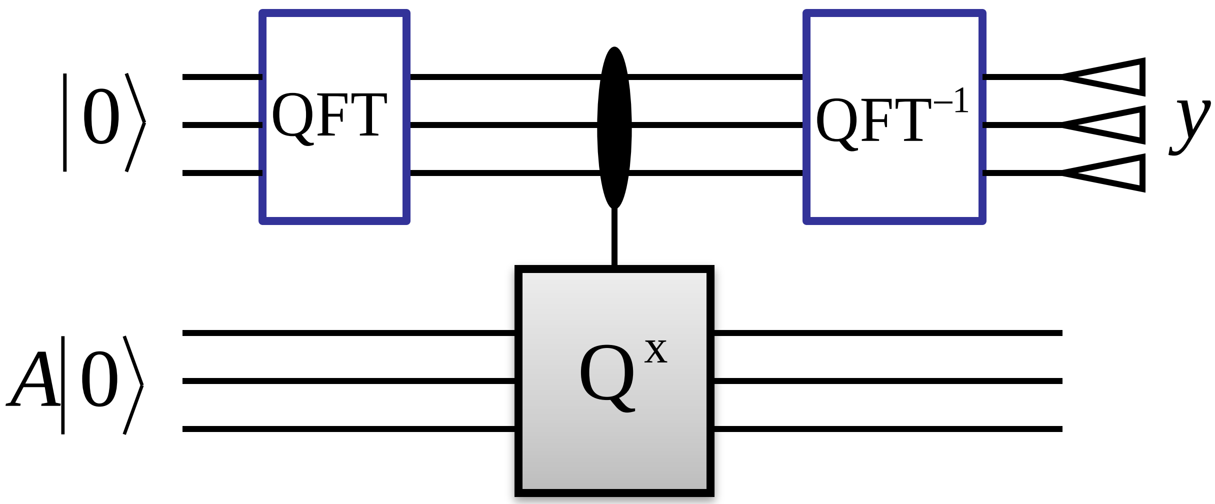
Amplitude estimation
≈ Eigenvalue estimation



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

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

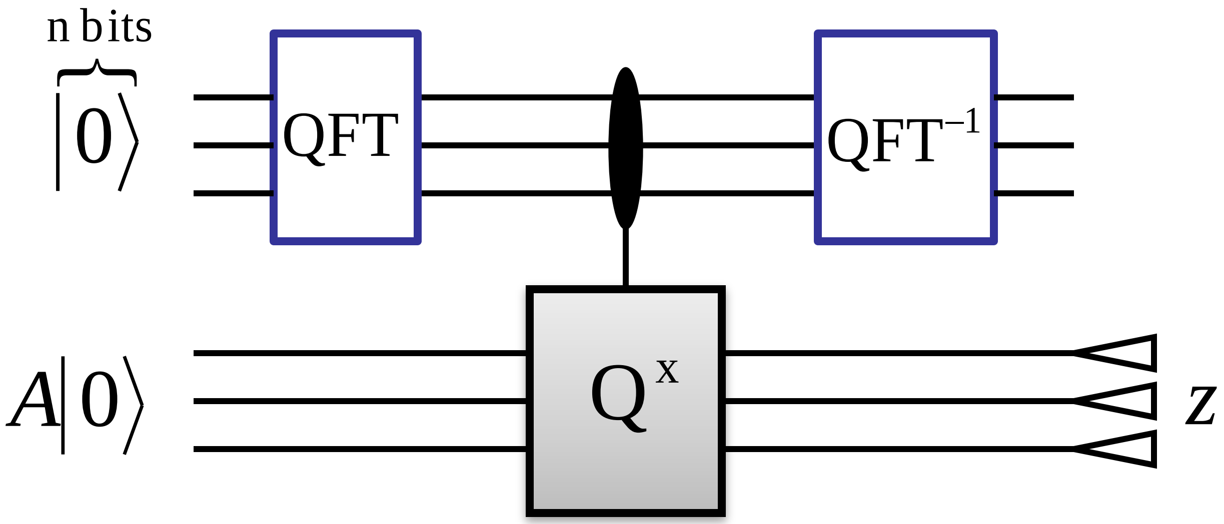
Note that the amplitude estimation network produces states

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

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



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

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

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

This means the expected running time is in $\mathrm{O}\left(\frac{1}{\theta}\right)$

In more detail…

This means that once $2^n \geq 2^{n_0} \geq c\dfrac{1}{\theta} \geq 2^{n_0-1}$ (for some constant c) we will find a satisfying x with probability in $\dfrac{3}{4} - \mathrm{O}\left(\dfrac{1}{2^n\theta}\right)$ which we can make at least $2/3$ for some appropriately chosen c.

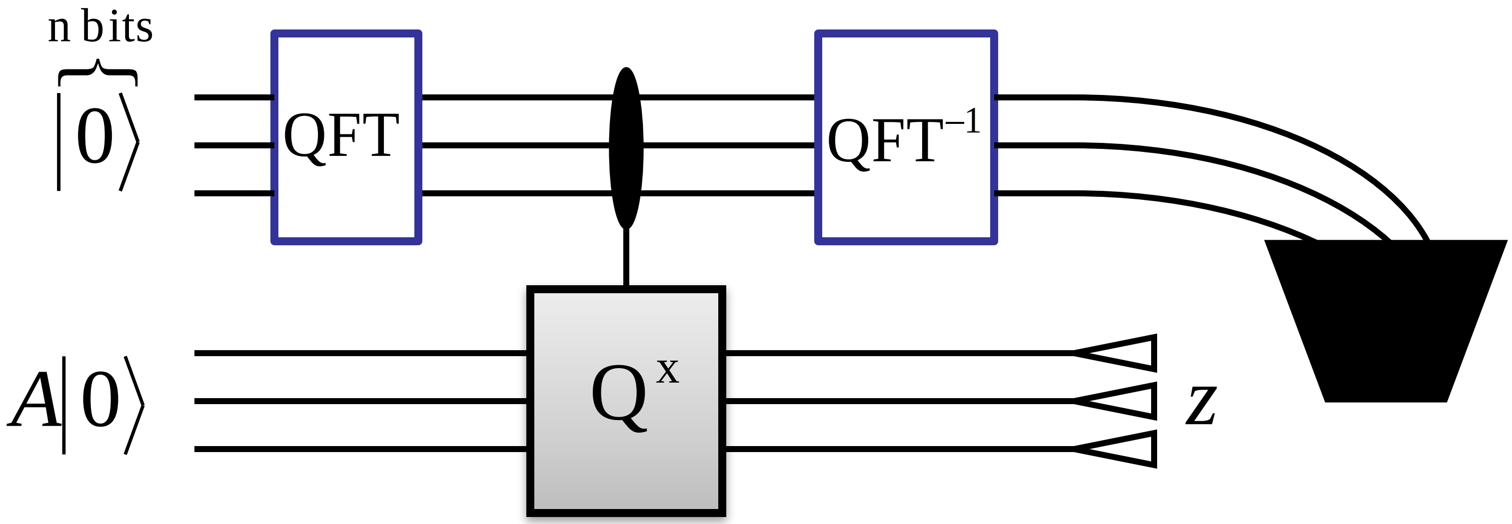
Thus the expected running time is at most

$$\leq 1+1+2+2+\cdots+2^{n_0-1}+2^{n_0-1}+\frac{2}{3}2^{n_0+1}+\frac{1}{3}\left(\frac{2}{3}2^{n_0+2}+\frac{1}{3}\left(\frac{2}{3}2^{n_0+3}+\cdots\right)\right)$$

$$= 2^{n_0+1}-2+\frac{2}{3}2^{n_0+1}\left(1+\frac{2}{3}+\left(\frac{2}{3}\right)^2+\left(\frac{2}{3}\right)^3+\cdots\right)=2^{n_0+1}-2+2\cdot 2^{n_0+1}\in \mathrm{O}\left(\frac{1}{\theta}\right)$$

Another way of doing it

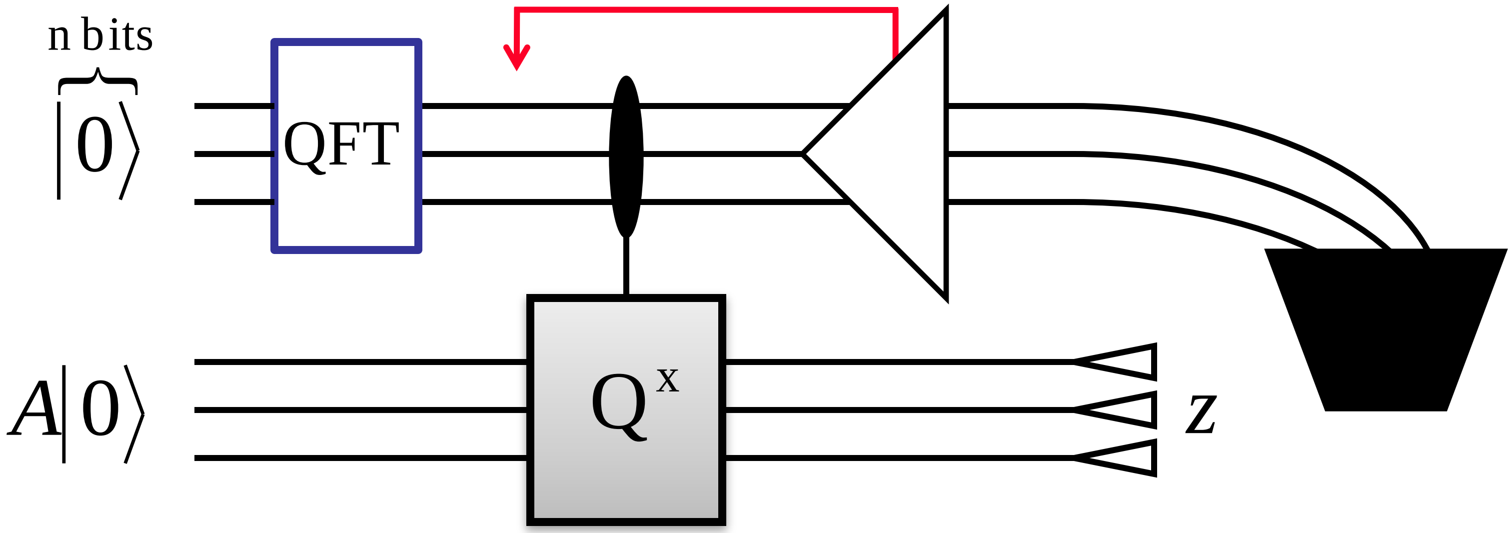
Notice



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

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

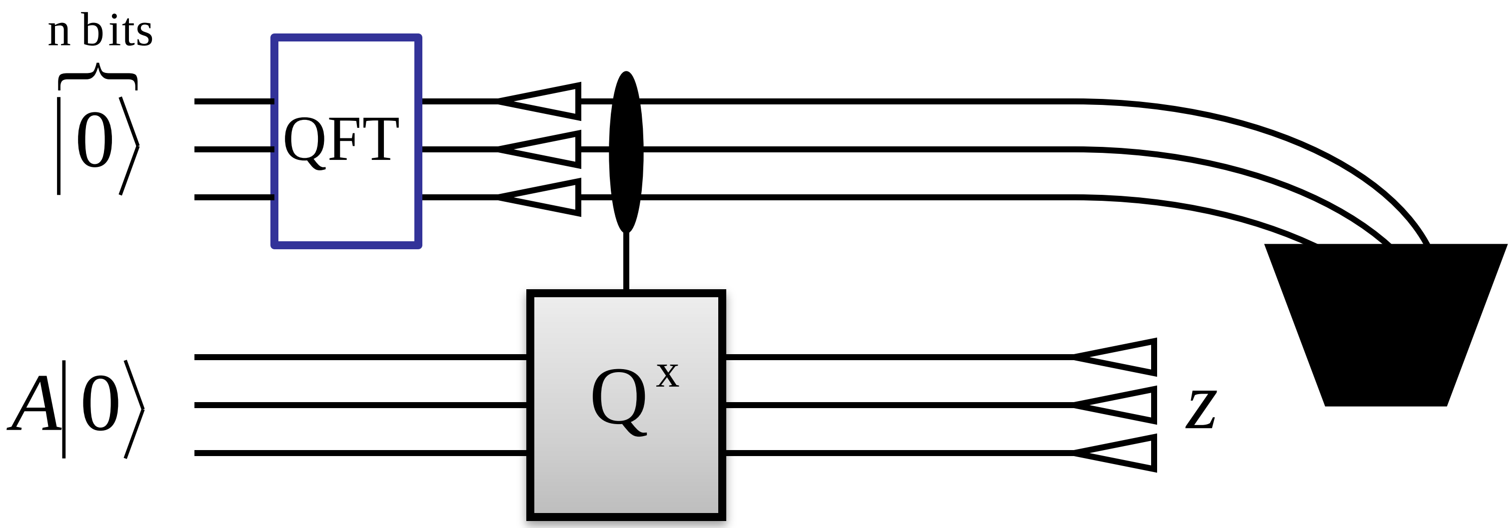
Notice



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

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

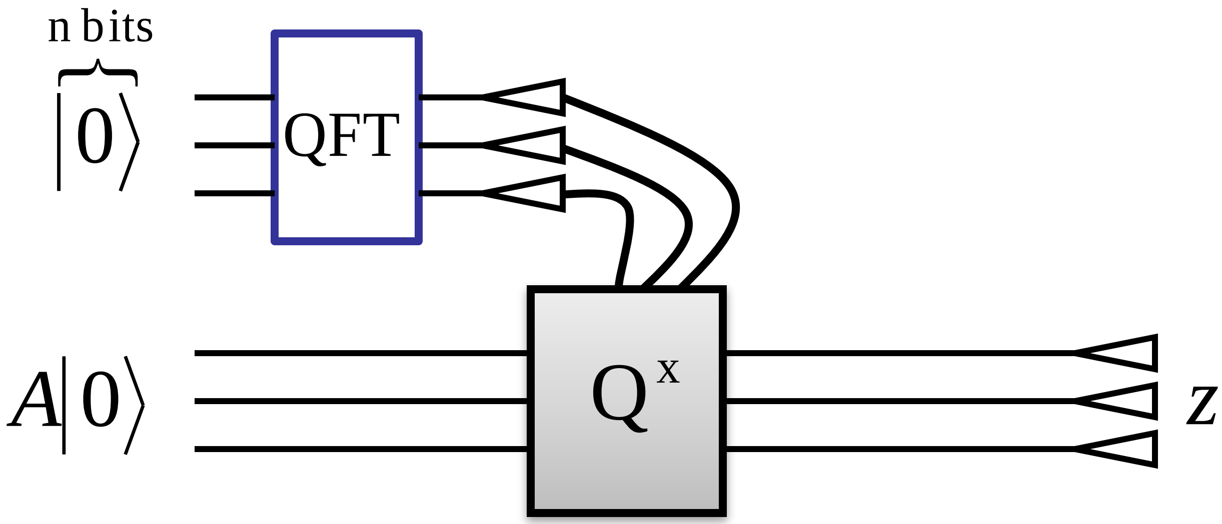
Notice



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

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

Notice

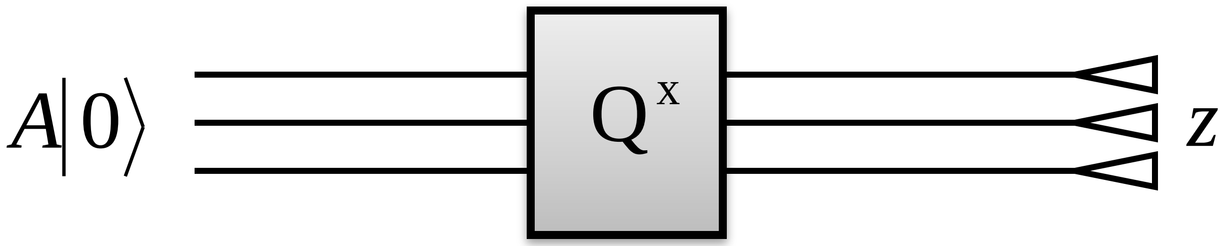


$$\mathrm{Prob}(f(z)=1) \in \frac{1}{2} - \mathrm{O}\left(\frac{1}{2^n \theta}\right)$$

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

The way BBHT do it

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



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

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