$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\underbrace{H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\text{2 gates}}$$

$|\psi\rangle = a|0\rangle + b|1\rangle$ $\quad \|a\|^2 + \|b\|^2 = 1$

$\langle 0|\psi\rangle = a$ $\quad \langle 1|\psi\rangle = b$

$P(0) = \|a\|^2$ $\quad P(1) = \|b\|^2$

Implications:

* Operations need to preserve the norm to 1

$|\det(U)| = 1 \Leftarrow$ * $\Rightarrow$ Unitary matrix

$\Rightarrow U^{\dagger} = U^{-1}$

Single qubit $\rightarrow$ unitary gates are rotations on Bloch sphere

properties

Eigenvalues & Eigenvectors

$\|E\| = 1$ (phase)

$U|x\rangle = \lambda_x |x\rangle$

matrix $\quad$ eigenvalues $\quad$ eigenvectors

$e^{i\theta}$

if 2 Eigenvalues $\lambda_x \neq \lambda_y$ $\quad |x\rangle, |y\rangle$ orthogonal

$\langle x|y\rangle = 0$

- Deutsch-Jozsa algorithm
- constant / balanced function in 1 shot

Grover's algorithm → unstructured search: $O(\sqrt{N})$ time

[1 4 9 5 8]

Problem: given a function that is periodic, find its period!

$f(x) = f(y) \quad x \neq y \quad \text{iff } |x-y| = p$

Classically: $O(\exp(c\, n^{1/3}(\log n)^{2/3})) \Rightarrow O(e^{c\, n^{1/3}(\log n)^{2/3}})$

n # of bits to describe the period

Quantum: $O(n^2 \log n \log\log n) \approx$ little faster than n^3

(1) Quantum Fourier Transform
(2) Modular Exponentiation

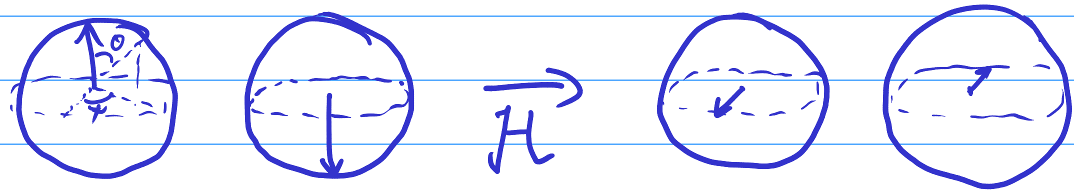
Quantum Fourier Transform
Quantum Phase Estimation
(Shor's algorithm is really just QPE in disguise)

WTF is QFT? Change of basis to fourier basis from computation basis

1-Qubit: $|0\rangle \; |1\rangle$

$\downarrow$

$|+\rangle \; |-\rangle$



$\cos\theta + i\sin\theta$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \cos\frac{\theta}{2}|0\rangle + \underbrace{e^{i\varphi}}_{\varphi = 0} \sin\frac{\theta}{2}|1\rangle$$

$\theta = \frac{\pi}{2}$

Build QFT:

Show circuit: