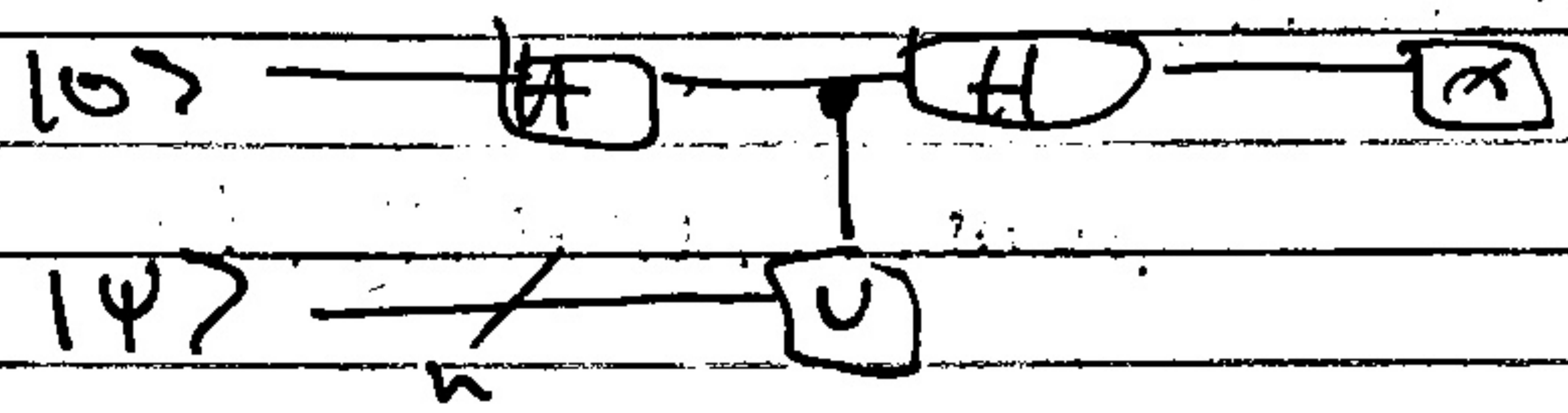
1/22

Hadamard test circuit



$\mathbb{P}(0)$

$$|0\rangle|\psi\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\psi\rangle \xrightarrow{cU} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle)$$

$$\xrightarrow{H\otimes I} \cancel{\frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle+|1\rangle|\psi\rangle)} + \frac{1}{2}(|0\rangle-|1\rangle)U|\psi\rangle$$

$$= \frac{1}{2}|0\rangle(I+U)|\psi\rangle + \underbrace{\frac{1}{2}|1\rangle(I-U)|\psi\rangle}_{|I\rangle}$$

want to write probability of 0; length of component:

$$\mathbb{P}(0) = \left\|\frac{1}{2}(I+U)|\psi\rangle\right\|^2 = \frac{1}{4}\langle\psi|(I+U)^\dagger(I+U)|\psi\rangle$$

$$= \frac{1}{4}(1+1+\langle\psi|U^\dagger|\psi\rangle + \langle\psi|U|\psi\rangle)$$

$$= \frac{1}{2}(1+\mathrm{Re}\langle\psi|U|\psi\rangle$$

Consider $U|\psi\rangle = e^{i\theta}|\psi\rangle$

find eigenvalues... "Phase Estimation"

$$\mathbb{P}(0) = \frac{1}{2}+\frac{1}{2}\cos\theta \rightarrow \theta = \arccos(2\mathbb{P}(0)-1)$$

"statistical estimation"

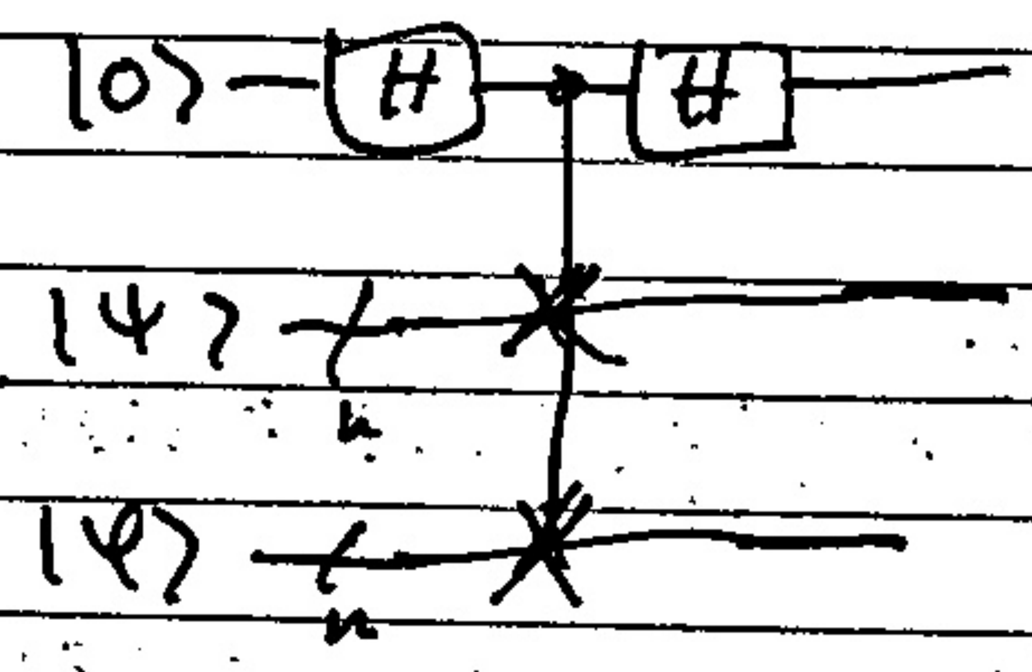
precision ε $\rightarrow$ # repetition $1/\varepsilon^2$; "this is like resource cost", "Standard quantum limit" (crazy name, not standard quantum limit)

"shot noise limit"

More powerful with cost $1/\varepsilon$, info-theoretic lower bound, "Heisenberg limit"

THINK: How to compute $\mathrm{Im}\langle\psi|U|\psi\rangle$?

Ex SWAP test $\quad U = \mathrm{SWAP} \qquad \mathrm{SWAP}|\psi\rangle|\varphi\rangle = |\varphi\rangle|\psi\rangle$



$$\mathbb{P}(0) = \frac{1}{2}\left(1 + \mathrm{Re}\langle\psi,\varphi|\varphi,\psi\rangle\right) = \frac{1}{2}\left(1 + |\langle\varphi|\psi\rangle|\right)^2$$

$$\longrightarrow |\langle\varphi|\psi\rangle|^2 = 2\mathbb{P}(0) - 1$$

way to compute fidelity, "most experimental friendly"

"trace norm related but not equivalent"

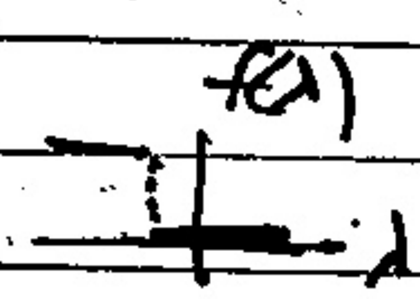
Block Encoding

"like a language", How to represent nonunitary matrices on a quantum computer?

Motivation: Linear systems $Ax = b \longrightarrow x = A^{-1}b$ (actual task: $|b\rangle$ is normalized. $|x\rangle \propto A^{-1}|b\rangle$)

Eigenvalue problem $Ax = \lambda x$

Spectral filtering $f(H)|\psi\rangle$



Linear Diff Eqs $\begin{cases} \partial_t u(t) = A(t)\, u(t) \\ u(0) = u_0 \end{cases}$

...

· Language, but not solution is Block Encoding

Any nonunitary matrix (after rescaling) can be expressed as a subblock of a unitary matrix

$A \in \mathbb{C}^{N\times N}$

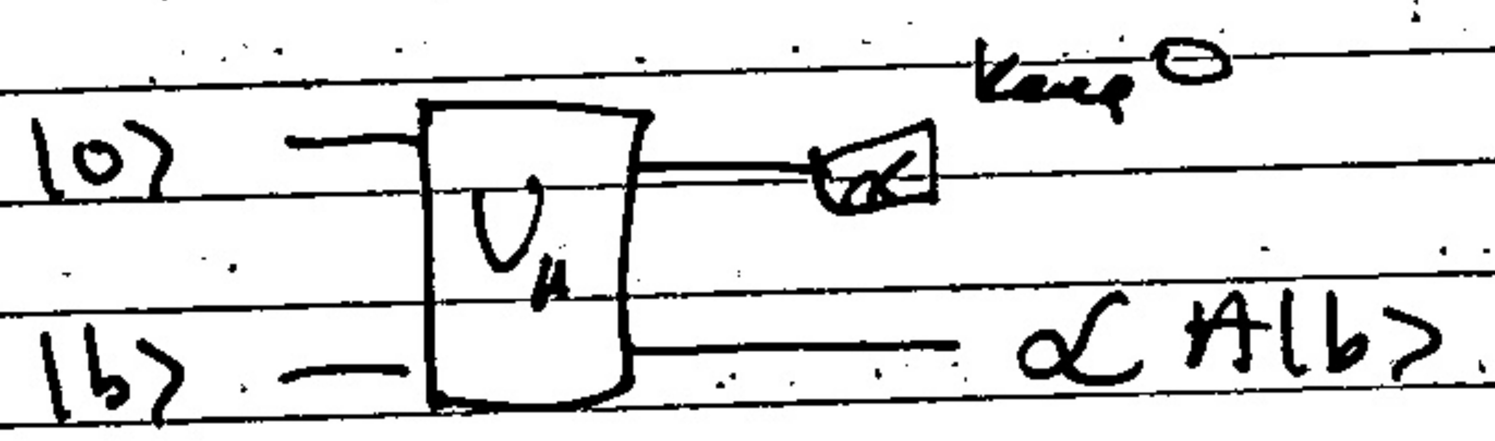
$$U_A = \begin{array}{c c} & \begin{array}{cc} N & N \end{array} \\ \begin{array}{c} N \\ N \end{array} & \begin{pmatrix} A & * \\ * & * \end{pmatrix} \end{array}$$

"Can we do matrix vector multiplication?"

goal: $A|b\rangle$ $\quad |0\rangle|b\rangle = \begin{pmatrix}|b\rangle \\ 0\end{pmatrix}$

$$U_A|0\rangle|b\rangle = \begin{pmatrix} A|b\rangle \\ * \end{pmatrix} = |0\rangle A|b\rangle + |\perp\rangle$$

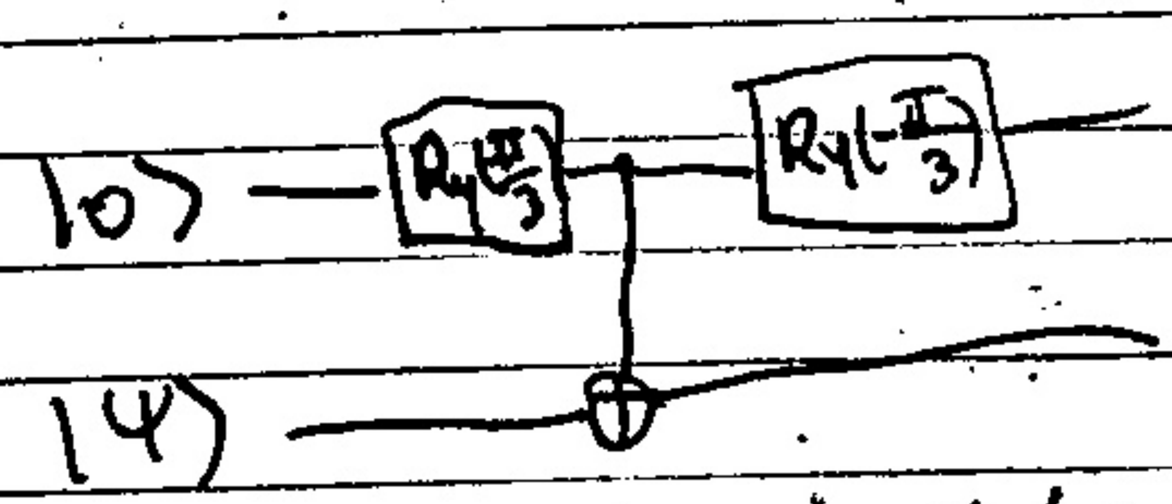
measure, first qubit, obtain 0 $\longrightarrow \dfrac{A|b\rangle}{\|A|b\rangle\|}$



what is success probability? similar to Hadamard test

$\mathbb{P}(0) = \|A|b\rangle\|^2$

Ex. $A = \frac{3}{4}I + \frac{1}{4}X = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}$ this is not unitary



$$R_y(\phi) = e^{-i\frac{\phi}{2}\sigma_y} = \begin{bmatrix} \cos(\frac{\phi}{2}) & -\sin(\frac{\phi}{2}) \\ \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix}$$

$$U_A = \begin{bmatrix} A & \cdot \\ - & - \end{bmatrix}$$

check calculations

"linear combination of unitary"

Ex. $\|A\| \le 1$ need at most 1-qubit for block encoding

$A = W\Sigma V^\dagger$ $\quad \Sigma = \begin{bmatrix} \sigma_0 & & \\ & \ddots & \\ & & \sigma_{N-1} \end{bmatrix}$ $\sigma_i \in [0,1]$

$$U_A = \begin{pmatrix} W & 0 \\ 0 & I_N \end{pmatrix} \begin{pmatrix} \Sigma & \sqrt{I-\Sigma^2} \\ \sqrt{I-\Sigma^2} & -\Sigma \end{pmatrix} \begin{pmatrix} V^\dagger & 0 \\ 0 & I_N \end{pmatrix}$$

$$= \begin{pmatrix} A & W\sqrt{I-\Sigma^2} \\ \sqrt{I-\Sigma^2}\,V^\dagger & -\Sigma \end{pmatrix}$$

THINK: A is not square?

- requires explicit knowledge of singular values and etc., in principle decompose any unitary, but large cost to compute

- for quantum advantage, amount of classical info must be poly(n) even though quantum computers can handle large matrices

- the key to block encoding is not to find a U_A, its to find ones that can be decomposed into 1 or 2-qubits, efficient encodings

- dilute to larger matrix, still easily constructible, but allow for error

$$U_A = MN\left\{ \begin{bmatrix} \overset{N}{A} & * & * \\ & \vdots & \vdots \\ * & \cdots & * \end{bmatrix} \right. \qquad |0^a\rangle = \left.\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right\} 2^a$$

$M = 2^a$ $\qquad \langle 0^a | U_A | 0^a \rangle = A$ ("partial inner product")

Ex. $|v\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|w\rangle = |0\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$\langle v|w\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$

$\langle v|$: maps a 3-qubit state $\longrightarrow$ 2-qubit state

More generally,

$|v\rangle \in \mathcal{H}_A$ $\langle v| : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_B$

$|w\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ From Def 2.22–2.25

$(\langle 0^a| \otimes I) U_A (|0^a\rangle \otimes I) = A \leftarrow \langle 0^a | U_A | 0^a\rangle = A$

"ignore these clarifying", for previous example

$\alpha \geq \|A\|$ $U_A =$

success $\frac{\|A|b\rangle\|^2}{\alpha^2}$ $\frac{A|b\rangle}{\|A|b\rangle\|}$ BQP $\subset$ post-BQP "post selection"

Def (Block Encoding) n-qubit A. find α, $\varepsilon > 0$, and $(m+n)$-qubit unitary

U_A s.t.

$\|A - \alpha\langle 0^m | U_A | 0^m\rangle\| \leq \varepsilon$

then U_A is called an (α, m, ε)-block-encoding of A

Set of all block encodings is $BE_{\alpha,m}(A, \varepsilon)$ when $\varepsilon = 0$ then $BE_{\alpha,m}(A)$

Pseudo Random Gen; classically create the matrix, or (better) create a pseudo random U, Haar Random

$\left[\frac{A}{\alpha} \;\; \right] |0\rangle|b\rangle$

How to do block encoding of matrix additions and multiplications?

matrix additions: linear combination of unitaries

Construct block encoding of $\sum_{i=0}^{m-1} \alpha_i U_i$ $\quad U_i = \begin{bmatrix} A_i & * \\ * & * \end{bmatrix}$

$\sum_i \alpha_i A_i$

"prepare/select circuit"

Select oracle: $U_{select} = \sum_{i=0}^{m-1} |i\rangle\langle i| \otimes U_i = \begin{bmatrix} U_1 & & \\ & \ddots & \\ & & U_{m-1} \end{bmatrix}$

prepare oracle: assume $\alpha_i \geq 0$, $V_{prep}|0^a\rangle = \frac{1}{\sqrt{\sum_i |\alpha_i|}} \sum_{i\in[m]} \sqrt{\alpha_i}\,|i\rangle$

$$V_{prep} = \frac{1}{\sqrt{\|\alpha\|_1}} \begin{pmatrix} \sqrt{\alpha_0} & \\ \sqrt{\alpha_1} & \\ \vdots & * \\ \sqrt{\alpha_{m-1}} & \end{pmatrix}$$