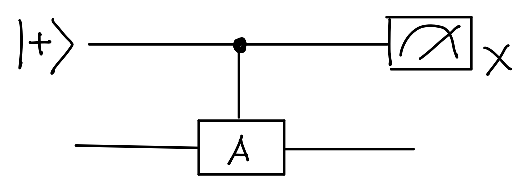
§1.5 Quantum Algorithms

Indirect Measurement and the Hadamard Test

An indirect measurement of an observable (hermitian) A with eigenvalues ± 1 can be performed by using $\Lambda(A)$:



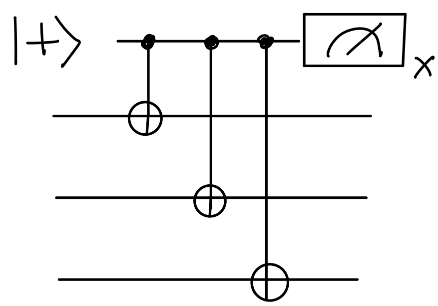
By denoting the input state $|\psi\rangle$, the post-measurement state is given by

$$\frac{I + (-1)^s A}{2} |\psi\rangle \Big/ \sqrt{\mathrm{Tr}\left[(I + (-1)^s A)/2 \, |\psi\rangle\langle\psi| \right]}$$

$$\begin{aligned}
&\Lambda_{1,2}(A) |+\rangle_1 |\psi\rangle_2 \\
&= \left(|0\rangle\langle 0|_1 I_2 + |1\rangle\langle 1|_1 A_2 \right) |+\rangle_1 |\psi\rangle_2 \\
&= \langle 0|+\rangle |0\rangle_1 |\psi\rangle_2 + \langle 1|+\rangle |1\rangle_1 A |\psi\rangle_2 \\
&= \frac{1}{\sqrt{2}} |0\rangle_1 |\psi\rangle_2 + \frac{1}{\sqrt{2}} |1\rangle_1 A |\psi\rangle_2 \\
&= \frac{1}{2} \left(|+\rangle_1 + |-\rangle_1 \right) |\psi\rangle_2 + \frac{1}{2} \left(|+\rangle_1 - |-\rangle_1 \right) A |\psi\rangle_2
\end{aligned}$$

$$\xrightarrow{\text{measurement}} \frac{I + (-1)^s A}{2} |\psi\rangle \Big/ \text{norm factor}$$

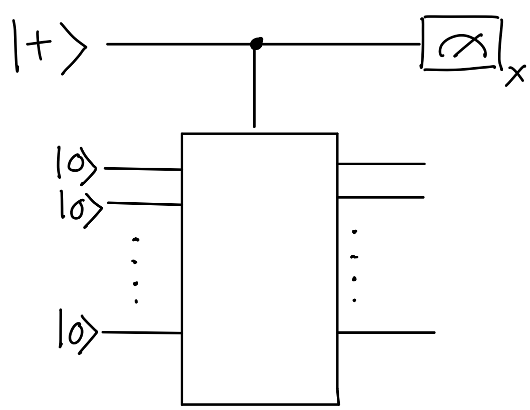
For example, a circuit measuring the eigenvalue of the operator $X_1 X_2 X_3$ is given by



According to the measurement outcome $s = 0, 1$, the post-measurement state is projected by

$$\frac{I + (-1)^s X_1 X_2 X_3}{2}$$

The Hadamard test of an arbitrary unitary operator U is defined by the following circuit:



The probabilities of the measurement outcomes $0, 1$ of the X-basis measurement are

$$p_0 = \frac{1}{2}\left(1 + \mathrm{Re}\langle 0|^{\otimes n} U |0\rangle^{\otimes n}\right)$$

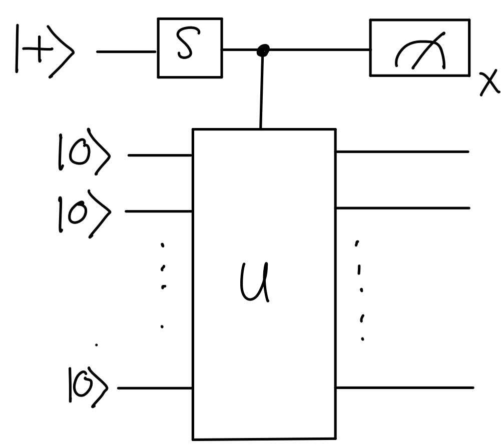
$$p_1 = \frac{1}{2}\left(1 - \mathrm{Re}\langle 0|^{\otimes} U |0\rangle^{\otimes n}\right)$$

$$\frac{1}{4} \sum_{\psi} \left(\langle 0|\psi\rangle + \langle 0|A|\psi\rangle\right)\left(\langle \psi|0\rangle + \langle \psi|A^{\dagger}|0\rangle\right)$$

$$= \frac{1}{4}\left(\langle 0|0\rangle + \langle 0|A|0\rangle + \overline{\langle 0|A|0\rangle} + \underbrace{\langle 0|AA^{\dagger}|0\rangle}_{=1}\right)$$

$$= \frac{1}{2}\left(1 + \mathrm{Re}\langle 0|A|0\rangle\right)$$

Similarly, the Hadamard test for the imaginary part is defined:

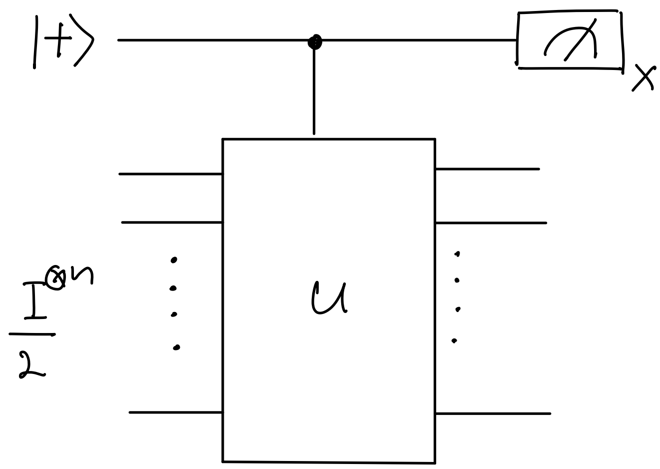


Suppose we perform the Hadamard test N times and obtain the measurement outcome 0, N_0 times. $\rightarrow$ probability of error

$$\mathrm{Prop}\left(\left|\frac{N_0}{N} - p_0\right| > \varepsilon\right) < 2e^{-2\varepsilon^2 N}$$ "Chernoff Höffding"

→ can estimate the matrix element $\langle 0|^{\otimes n} U|0\rangle^{\otimes}$ with an error ε by repeating Hadamard test $N = \text{poly}(1/\varepsilon)$ times

Choose input state to be completely mixed n-qubit state :

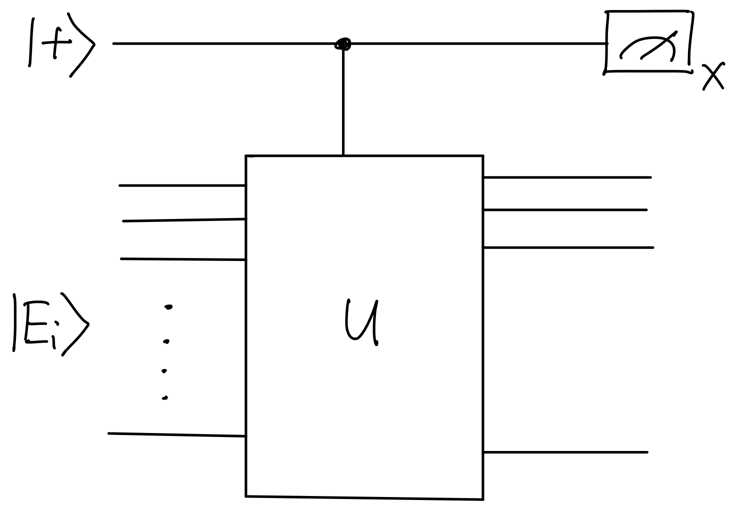


→ Hadamard test provides trace $\mathrm{Tr}[U]/2^n$

→ deterministic quantum computation with one clean qubit (DQC1)
(can compute Jones and Homefly polynomials)

Phase Estimation, Quantum Fourier Trf., and Factorization

Given an eigenstate $|E_i\rangle$ of unitary op. U, can estimate eigenvalues λ_i of U using Hadamard test:

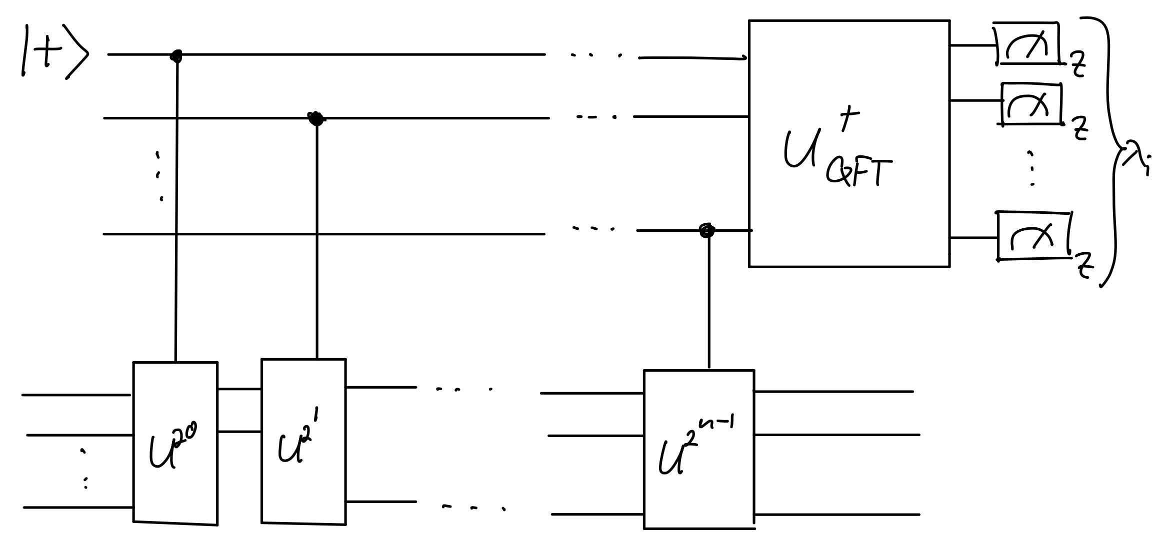


Moreover, if a controlled-U^{2^k} gate $\Lambda(U^{2^k})$ can be described by polynomial # of gates, we can efficiently estimate the eigenvalue with exponential accuracy.

Suppose $\lambda_i = e^{i\phi} = e^{2\pi i\, 0.j_1 j_2 \cdots j_n}$, where

$$0.j_1 j_2 \cdots j_n = \sum_{k=1}^{n} j_k \left(\frac{1}{2}\right)^k$$

→ Kitaev's phase estimation algorithm:



where U_{QFT} is the "quantum Fourier trf" operator. Let us first recall the discrete Fourier transform:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot e^{2\pi\sqrt{-1}\, jk/N} \qquad (*)$$

the quantum version is

$$|j\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi\sqrt{-1}\, jk/N} |k\rangle \quad \text{Unitary}$$

the action on an arbitrary state may be written as:

$$\sum_{j=0}^{N-1} x_j |j\rangle \longmapsto \sum_{k=0}^{N-1} y_k |k\rangle ,$$

where $y_k(x_j)$ is given by $(*)$

Take $N = 2^n \longrightarrow$ basis $|0\rangle, \ldots, |2^n-1\rangle$
"n qubit basis"

write state $|j\rangle$ using binary rep $j = j_1 j_2 \cdots j_n$

i.e $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$

Quantum Fourier trf. admits the following "product representation":

$$|j_1, \ldots, j_n\rangle \longrightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

<u>Proof:</u>

$$|j\rangle \longmapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi\sqrt{-1}\, jk/2^n} |k\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi\sqrt{-1}\, j\left(\sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right)} |k_1 \cdots k_n\rangle$$

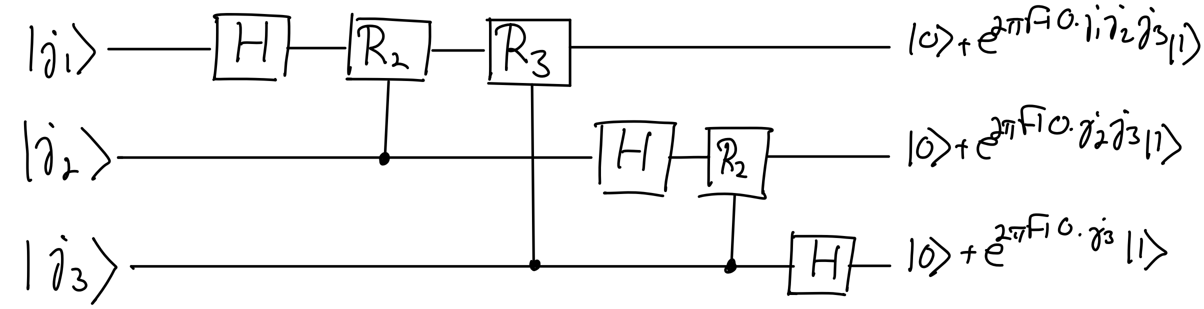
$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{\ell=1}^{n} e^{2\pi\sqrt{-1}\, j k_\ell 2^{-\ell}} |k_\ell\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left[\sum_{k_\ell=0}^{1} e^{2\pi\sqrt{-1}\, j k_\ell 2^{-\ell}} |k_\ell\rangle\right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left[|0\rangle + e^{2\pi\sqrt{-1}\, j 2^{-\ell}} |1\rangle\right]$$

$$= \frac{\left(|0\rangle + e^{2\pi\sqrt{-1}\, 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi\sqrt{-1}\, 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi\sqrt{-1}\, 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}} \qquad \square$$

Circuit representation (3-qubit example):



The gate R_k is the unitary trf.:

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi\sqrt{-1}/2^k} \end{bmatrix} \quad (R_2 = S,\ R_3 = T)$$

Suppose $|j_1 \cdots j_n\rangle$ is input state

$$\xrightarrow[\text{gate}]{\text{Hadamard}} \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_1}|1\rangle\right)|j_2 \cdots j_n\rangle$$

$$\xrightarrow{\text{controlled } R_2} \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_1 j_2}|1\rangle\right)|j_2 \cdots j_n\rangle$$

$\vdots$

$$\xrightarrow{C\text{-}R_n} \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_1 \cdots j_n}|1\rangle\right)|j_2 \cdots j_n\rangle$$

Continue similarly on second qubit etc.

$$\rightarrow \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi\sqrt{-1}\,0.j_1\cdots j_n}|1\rangle\right)$$

$\rightarrow$ $n(n+2)/2$ gates required in total