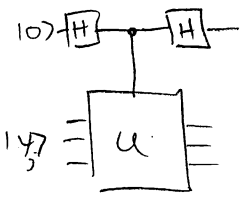
QIC 710 Lecture 8 : Phase estimation, QFT mod N for arbitrary N

Phase estimation [Kitaev]

Basic idea: Let U be unitary with o.n. eigenvectors $|\psi_1\rangle \cdots |\psi_N\rangle$, eigenvalues $\lambda_j = e^{\theta_j i}$



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi_j\rangle \xrightarrow{cU} \frac{(|0\rangle|\psi\rangle + |1\rangle\lambda_j|\psi_j\rangle)}{\sqrt{2}} = \frac{(|0\rangle + \lambda_j|1\rangle)}{\sqrt{2}}\otimes|\psi_j\rangle$$
$$\xrightarrow{H} \left(\frac{1+\lambda_j}{2}|0\rangle + \frac{1-\lambda_j}{2}|1\rangle\right)\otimes|\psi_j\rangle$$

$$\mathbb{P}[0] = \left|\frac{1+\lambda_j}{2}\right|^2 = \frac{1}{4}\left[(1+\cos\theta_j)^2 + \sin^2\theta_j\right] = \frac{1+\cos\theta_j}{2} = \cos^2\frac{\theta_j}{2}$$
$$\mathbb{P}[1] = \sin^2\frac{\theta_j}{2}$$

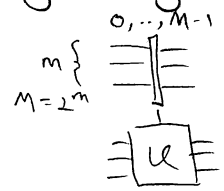
$\Rightarrow$ can estimate the phase θ_j (perfectly if the phase is 0 or π)

since $|\psi_j\rangle$ is unchanged, test can be repeated

use $O(\frac{1}{\epsilon^2})$ tests to estimate $\cos\theta_j$ to within ϵ

(exp. many measurements to get exp. precision)

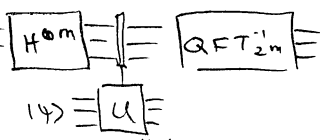
More generally:



$$|k\rangle\otimes|\psi\rangle \xrightarrow{c^m\text{-}U} |k\rangle\otimes U^k|\psi\rangle$$

Problem: Given an eigenvector $|\psi\rangle$ of U with eigenvalue $e^{2\pi i\theta}$, $\theta = \frac{j}{2^m}$,

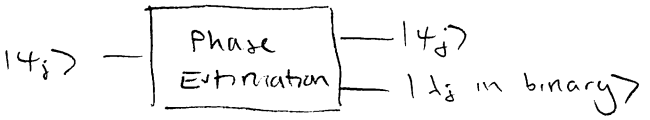
Determine j.



$$\frac{1}{\sqrt{M}}\sum_{k=0}^{M-1}|k\rangle\otimes|\psi\rangle \xrightarrow{c^m\text{-}U} \left(\frac{1}{\sqrt{M}}\sum_{k=0}^{M-1}\lambda^k|k\rangle\right)\otimes|\psi\rangle = \left(\frac{1}{\sqrt{M}}\sum_k \omega_{2^m}^{jk}|k\rangle\right)\otimes|\psi\rangle$$
$$\downarrow QFT^{-1}_{2^m}$$
$$|j\rangle$$

If θ is not exactly $j/2^m$, then with good probability get the closest integer...

Morally



Thus $|\psi\rangle = \sum_j \alpha_j |\psi_j\rangle \longmapsto \sum_j \alpha_j |\psi_j\rangle|\lambda_j\rangle$ + error term

Incredibly useful:

1. Let U be a unitary with eigenvalues all exactly $e^{2\pi i j/2^m}$, m constant.
   To compute U^p for $p \in \mathbb{R}$ (not necessarily >0, not necessarily an integer),
   $|\psi\rangle \xrightarrow{P.E.} \sum_k \alpha_k |\psi_k\rangle|\theta_k\rangle$
   $\longrightarrow \sum_k \alpha_k |\psi_k\rangle \cdot e^{i\theta_k p}|\theta_k\rangle$ (by single-qubit rotations $j_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i \cdot p/2^{m-k}} \end{pmatrix}$)
   $\xrightarrow{P.E.^{-1}} \sum_k \alpha_k e^{i\theta_k p}|\psi_k\rangle = U^p|\psi\rangle$

2. Isolate eigenvectors with eigenvalues in a specified range

3. QFT mod N for arbitrary N.
   Goal: $|a\rangle_{\bmod N} \longrightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \omega_N^{ab}|b\rangle \equiv |\chi_a\rangle$

   Two steps:

   ① $|a\rangle|0\rangle \longmapsto |a\rangle|\chi_a\rangle$ easy
   $\downarrow$ $\qquad\qquad$ $\|$
   $|a\rangle \sum_{b=0}^{N-1} |b\rangle \xrightarrow[c\text{-phase}]{} |a\rangle \sum_b \omega_N^{ab}|b\rangle$

   ② $|a\rangle|\chi_a\rangle \longrightarrow |0\rangle|\chi_a\rangle$
   Recall for $T|b\rangle = |b-1\rangle$, $T|\chi_a\rangle = \omega^a|\chi_a\rangle$
   thus $|\chi_a\rangle|0\rangle \longrightarrow |\chi_a\rangle|a\rangle$ is just phase estimation using $cm^{-}T$ (subtraction mod N) ✓

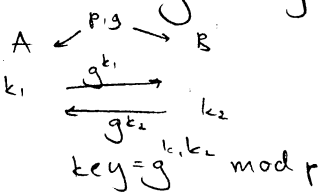
Discrete log problem

p prime $\Rightarrow \mathbb{Z}_p^* = (\{1, 2, \ldots, p-1\}, \cdot \bmod p)$ is cyclic

Given: p, a generator g for $\mathbb{Z}_p^*$, x

Find: y such that $g^y = x \bmod p$.

Diffie Hellman key exchange



Quantum algorithm:

$|0,0\rangle \xrightarrow{F_{p-1}^{\otimes 2}} \frac{1}{p-1} \sum_{a,b} |a,b\rangle$

$\longrightarrow \frac{1}{p-1} \sum_{a,b} |a,b,g^a x^{-b}\rangle$

measure

$g^a x^{-b} \equiv g^k \bmod p$

$a - by \equiv k \bmod p-1$

$\longrightarrow \frac{1}{\sqrt{p-1}} \sum_b |by+k, b\rangle$

↖ irrelevant shift since we will measure after F_{p-1}

$\xrightarrow{F_{p-1}^{\otimes 2}} \sum_{c,d} \alpha_{c,d} |c,d\rangle$

$\alpha_{c,d} = \frac{1}{(p-1)^{3/2}} \sum_b \omega_{p-1}^{(by+k)c} \omega_{p-1}^{bd}$

$= \frac{\omega^{kc}}{(p-1)^{3/2}} \sum_b \omega_{p-1}^{b\cdot(yc+d)}$

$= \begin{cases} 0 & \text{if } yc+d \neq 0 \bmod p-1 \\ \text{uniform, otherwise} \end{cases}$

$\xrightarrow{\text{measure}}$ get uniform c, d with $yc + d = 0 \bmod p-1$

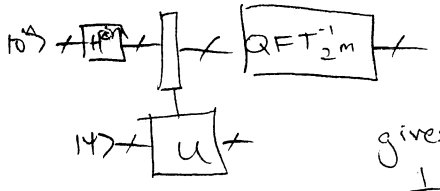
If $\gcd(c, p-1) = 1$, then output $y = -c^{-1} d \bmod p-1$.

Problem: How to implement F_{p-1} when $p-1$ is not a power of 2?

Phase estimation error analysis:

if eigenvalue is not exactly $e^{i2\pi \frac{j}{2^m}}$ for $j \in [M]$,

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



gives in the first register $\frac{1}{M}\sum_{a,b=0}^{M-1} e^{i\theta a}\cdot\omega^{-ab}|b\rangle$

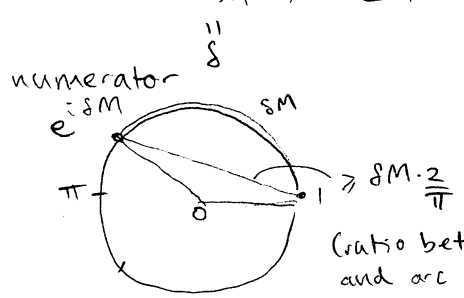
$$\mathbb{P}[\text{measuring } b] = \frac{1}{M^2}\left|\sum_{a=0}^{M-1} e^{i\theta a}\omega^{-ab}\right|^2$$

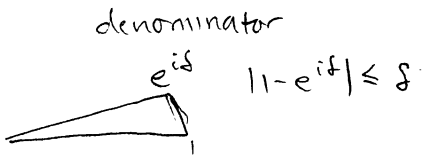
$$= \frac{1}{M^2}\left|\sum_{a=0}^{M-1} e^{ia(\theta - \frac{2\pi b}{M})}\right|^2$$

$$= \begin{cases} \frac{1}{M^2}\cdot\left|\frac{1-s^M}{1-s}\right| & \text{where } s = e^{i(\theta - \frac{2\pi b}{M})} \\ \text{or } 1 \text{ if } \theta = \frac{2\pi b}{M} \end{cases}$$

Let b^* be the closest approximation to θ,

so $\left|\theta - \frac{2\pi b^*}{M}\right| \le \frac{2\pi}{2M}$





$$\Rightarrow \frac{1}{M^2}\left|\frac{1-s^M}{1-s}\right| \geq \frac{1}{M^2}\cdot\left|\frac{\delta M \frac{2}{\pi}}{\delta}\right|^2 = \frac{4}{\pi^2} \approx 0.4$$

To get better precision, can either add more bits,
or repeat phase estimation, take majority, uncompute.

$O\left(\frac{1}{\delta_s \delta_c}\right)$ calls to cU

$O\left(\frac{1}{\delta_s}\log\frac{1}{\delta_c}\right)$ — [0904.1549]