Lecture 11

7 MAR 2014

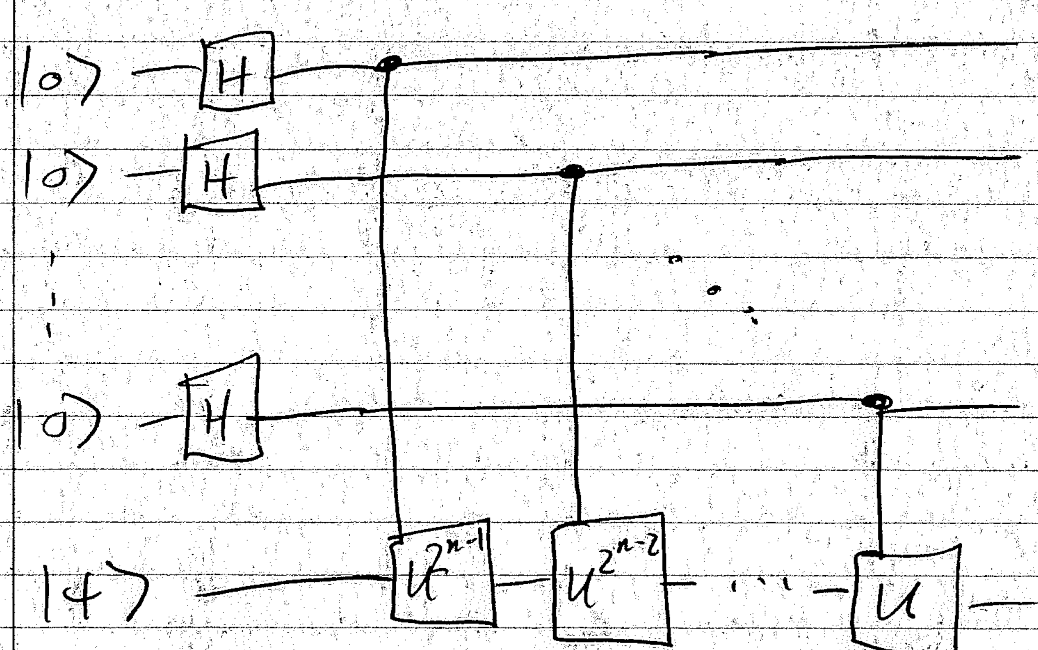
review of last time – QFT &
phase estimation

We considered the problem of
phase estimation:

~~Input~~ You are given a state $|\psi\rangle$
+ unitary U such that $U|\psi\rangle = e^{2\pi i \omega}|\psi\rangle$

+ black box access to $c\text{-}U^{2^j}$
for $j \in \{0, \ldots, n-1\}$

Algorithm B



output of the algorithm is the state

$$\left(\frac{|0\rangle + e^{2\pi i \omega 2^{n-1}}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i \omega 2^{n-2}}|1\rangle}{\sqrt{2}}\right) \otimes \cdots$$

$$\otimes \left(\frac{|0\rangle + e^{2\pi i \omega 2^{0}}|1\rangle}{\sqrt{2}}\right)$$

which we argued last time is equivalent to

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$$

The inverse QFT (on n qubits) implements the transformation:

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{+2\pi i \frac{kl}{2^n}} |k\rangle \rightarrow |l\rangle$$

i.e., matrix rep. is

$$QFT^{-1} = \frac{1}{\sqrt{2^n}} \sum_{k,l=0}^{2^n-1} e^{-\frac{2\pi i kl}{2^n}} |l\rangle\langle k|$$

so that

$$QFT^{-1} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i w y} |y\rangle$$

$$= \frac{1}{2^n} \sum_{y,l=0}^{2^n-1} e^{-\frac{2\pi i y l}{2^n}} e^{2\pi i w y} |l\rangle$$

$$= \frac{1}{2^n} \sum_{y,l=0}^{2^n-1} e^{2\pi i y\left(w - \frac{l}{2^n}\right)} |l\rangle$$

then what is the amplitude for a particular computational basis state $|k\rangle$?

$\alpha_k = \langle k|$ "

$$= \frac{1}{2^n} \sum_{y=0}^{2^n-1} e^{2\pi i y\left(w - \frac{k}{2^n}\right)}$$

But we can use the geometric series sum formula

$$\sum_{k=0}^{N-1} a^k = \frac{1-a^N}{1-a}$$

to see that

$$\alpha_k = \frac{1}{2^n}\left[\frac{1-e^{2\pi i(2^n\omega-k)}}{1-e^{2\pi i(\omega-\frac{k}{2^n})}}\right]$$

By the identity $|1-e^{2\pi i\theta}|$

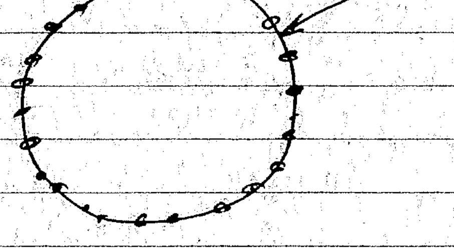
$$= |e^{-\pi i\theta}-e^{i\pi\theta}|$$

$$= 2|\sin(\pi\theta)|$$

we can write

$$\Pr\{k\} = |\alpha_k|^2 = \frac{1}{2^{2n}}\frac{\sin^2(\pi(2^n\omega-k))}{\sin^2(\pi(\omega-\frac{k}{2^n}))}$$

To think about the scenario, what we are doing is dividing up the unit circle into 2^n different arcs (uniformly spaced)



ω will be some phase on the unit circle

If $\omega = 0.x_1 \cdots x_n 00\cdots$
then phase estimation will work
w/ probability one. Otherwise,
we need to consider the distribution

$$\Pr\{k\} = |\alpha_k|^2$$

But it turns out to be highly
peaked around the 2 values containing
ω.
(show the distribution)

For an analysis, suppose that

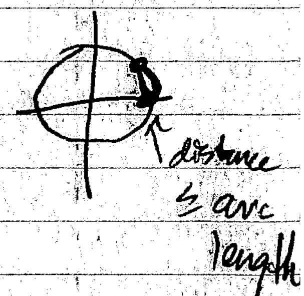
$\frac{k}{2^n}$ is the best n-bit approximation
of ω, so that

$$\omega = \frac{k}{2^n} + \delta \quad \text{where } |\delta| \leq \frac{1}{2^{n+1}}$$

This implies that

$2\pi \cdot \delta \cdot 2^n \leq \pi$ which in
turn means that $|1 - e^{2\pi i \delta 2^n}| \geq \frac{2\pi|\delta|2^n}{\pi/2}$
$= 4|\delta|2^n$

& $\left|1 - e^{2\pi i \delta}\right| \le 2\pi|\delta|$



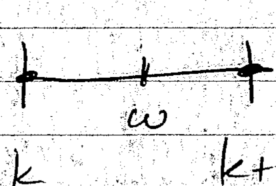
So this implies that

$$\Pr\{k\} = \frac{1}{2^{2n}} \frac{\left|1 - e^{2\pi i (2^n \omega - k)}\right|^2}{\left|1 - e^{2\pi i (\omega - k/2^n)}\right|^2}$$

$$\ge \frac{1}{2^{2n}} \left(\frac{4|\delta| 2^n}{2\pi|\delta|} \right)^2$$

$$= \frac{4}{\pi^2} \approx .40528$$

Worst-case is when ω is right between the two closest values



But from the above lemma, we can conclude that

$$\Pr\{k\} \ge \frac{4}{\pi^2} \quad \& \quad \Pr\{k+1\} \ge \frac{4}{\pi^2}$$

Thus we can conclude the following theorem:

- If $\frac{k}{2^n} \leq \omega \leq \frac{k+1}{2^n}$, then the phase estimation algorithm returns either k or $k+1$ w/ probability larger than $8/\pi^2 \approx 0.81$

This kind of probability is useful for Shor's algorithm.
But for some applications, we might need better success probability.

Idea is just to use more bits of precision to boost the success probability.

Let $\frac{k}{2^n}$ be the closest n-bit approximation of ω, so that

$$\omega = \frac{k}{2^n} + \delta \qquad \text{where } |\delta| \le \frac{1}{2^{n+1}}$$

WLOG suppose $\delta > 0$

For all t satisfying

$$-2^{n-1} \le t < 2^{n-1}$$

let α_t denote the amplitude for $|(\alpha - t) \bmod 2^m\rangle$. Then

$$\alpha_t = \frac{1}{2^n}\left(\frac{1 - \left[e^{2\pi i(\delta + \frac{t}{2^n})}\right]^{2^n}}{1 - e^{2\pi i(\delta + \frac{t}{2^n})}}\right)$$

Using our estimate from before, we have that

$$\left|1 - e^{2\pi i(\delta + \frac{t}{2^n})}\right| \ge \frac{2\pi(\delta + \frac{t}{2^n})}{\pi/2} = 4\left(\delta + \frac{t}{2^n}\right)$$

& that

$$|1 - e^{i\theta}| \le 2$$

we get that

$$|\alpha_t|^2 \le \left|\frac{1}{2^n}\left(\frac{2}{4(\delta + t/2^n)}\right)\right|^2$$

$$= \left[\frac{1}{2(\delta 2^n + t)}\right]^2 = \frac{1}{4(\delta 2^n + t)^2}$$

So the probability of getting an error greater than $\frac{\ell}{2^n}$ is

$$\sum_{\ell \le t < 2^{n-1}} |\alpha_t|^2 + \sum_{-2^{n-1} \le t < -\ell} |\alpha_t|^2$$

$$\le \sum_{t=\ell}^{2^{n-1}-1} \frac{1}{4(2^n\delta + t)^2} + \sum_{t=-2^{n-1}}^{-(\ell+1)} \frac{1}{4(2^n\delta + t)^2}$$

$$\le \sum_{t=\ell}^{2^{n-1}-1} \frac{1}{4t^2} + \sum_{t=\ell+1}^{2^{n-1}} \frac{1}{4(t-1/2)^2}$$

$$\le \sum_{t=2\ell}^{2^n-1} \frac{1}{4\left(\frac{t}{2}\right)^2}$$

$$\le \int_{2\ell-1}^{2^n-1} \frac{1}{t^2} \le \frac{1}{2\ell-1}$$

So, we can conclude from this that if we want an estimate that is within $\frac{1}{2^{n'+1}}$ of ω w/ prob. $\geq 1-\varepsilon$ then we use the phase estimation algorithm w/

$$n' = n + \lceil \log(\tfrac{1}{2\varepsilon} + 2) \rceil$$

bits.

To make use of phase estimation, we need an eigenstate of U, but if we don't have it, what happens then?

Write $|\psi\rangle = \sum_u c_u |u\rangle$

where $|u\rangle$ are eigenstates of U

Suppose that $U|u\rangle = e^{2\pi i \varphi_u}|u\rangle$

then phase estimation will output a state close to

$$\sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle \text{ where}$$

$|\tilde{\varphi}_u\rangle$ is an approximation to φ_u

so measuring the 1st register gives $\tilde{\varphi}_u$ w/ prob. $|c_u|^2$