CPEN 400Q Lecture 14
Quantum phase estimation and order finding

Monday 3 March 2025

Announcements

- Quiz 6 today
- Technical assignment 3 available later this week
- Project midterm checkpoint details available ~~later this week~~ now
- Tomorrow's tutorial: intro to RSA

Last time

We implemented the quantum Fourier transform using a *polynomial* number of gates:

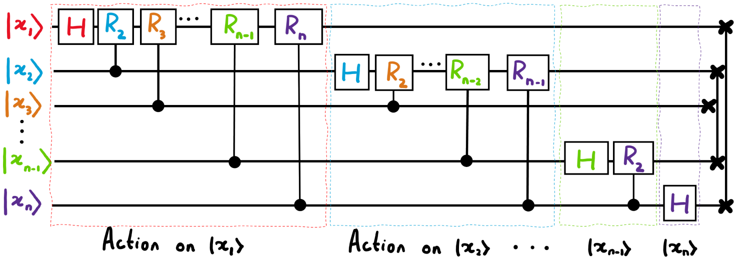
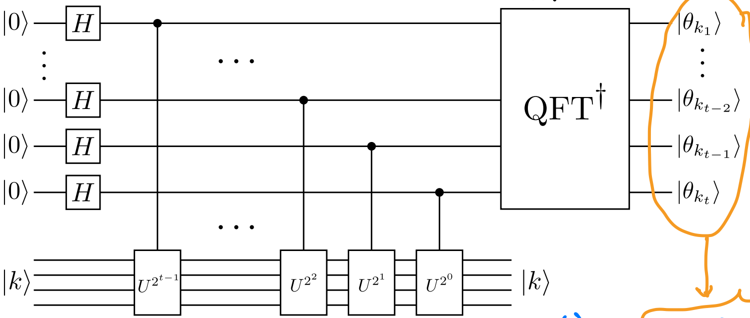


Image credit: Xanadu Quantum Codebook node F.3

We started learning about the quantum phase estimation subroutine which estimates the eigenvalues of unitary matrices.

$$U|k\rangle = \lambda_k |k\rangle = \underbrace{e^{2\pi i \theta_k}}_{|\lambda_k| = 1} |k\rangle$$



$0 \le \theta_k \le 1$ w/ t-bit representation

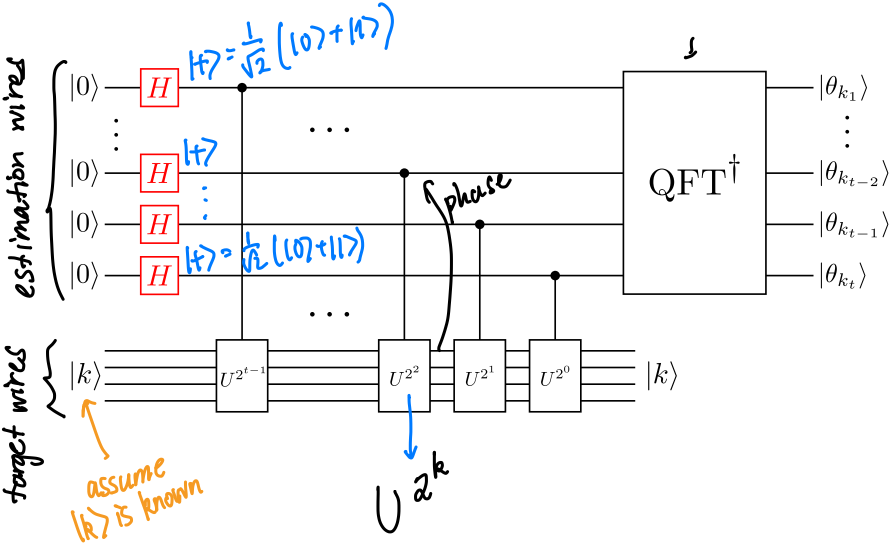
$$\theta_k = 0.\theta_{k_1}\theta_{k_2}\cdots\theta_{k_t} = \frac{\theta_{k_1}}{2} + \frac{\theta_{k_2}}{4} + \dots + \frac{\theta_{k_t}}{2^t}$$

Image credit: Xanadu Quantum Codebook node P.2

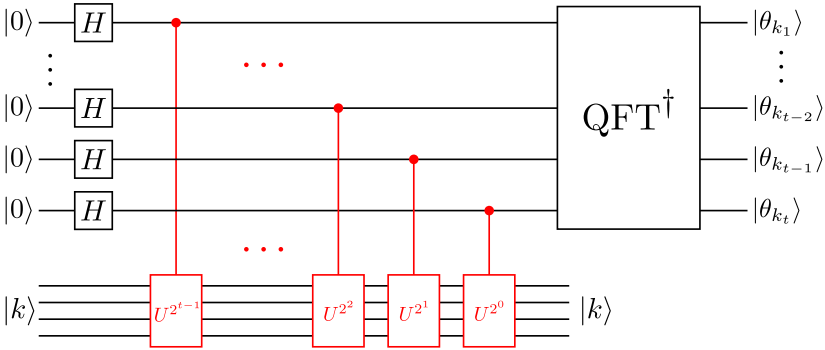
Learning outcomes

- Outline the steps of the quantum phase estimation (QPE) subroutine
- Use QPE to implement the order finding algorithm

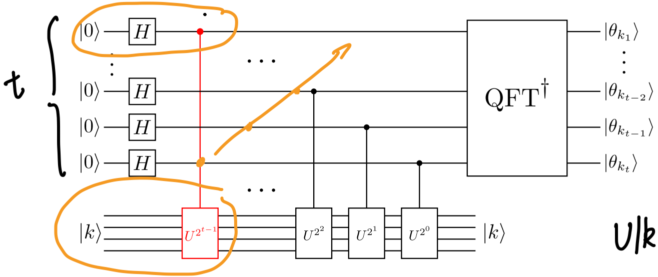
Quantum phase estimation: step 1



Quantum phase estimation: step 2



Quantum phase estimation: step 2



$$U|k\rangle = e^{2\pi i \theta_k}|k\rangle$$

$$|+\rangle|k\rangle = \frac{1}{\sqrt{2}}|0\rangle|k\rangle + \frac{1}{\sqrt{2}}|1\rangle|k\rangle$$

Apply C-U 2^{t-1} times $\rightarrow \frac{1}{\sqrt{2}}|0\rangle|k\rangle + \frac{1}{\sqrt{2}}|1\rangle\left(U^{2^{t-1}}|k\rangle\right)$

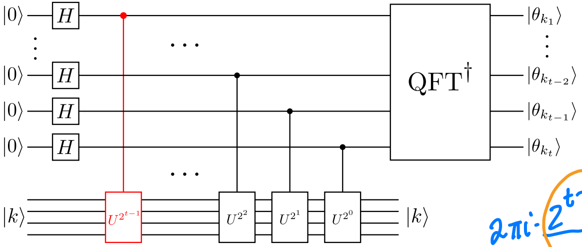
$$= \frac{1}{\sqrt{2}}|0\rangle|k\rangle + \frac{1}{\sqrt{2}}|1\rangle\left(e^{2\pi i\theta_k}\right)^{2^{t-1}}|k\rangle$$

kickback

$$= \frac{1}{\sqrt{2}}|0\rangle|k\rangle + \frac{1}{\sqrt{2}}\left(e^{2\pi i\theta_k}\right)^{2^{t-1}}|1\rangle|k\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + \left(e^{2\pi i\theta_k}\right)^{2^{t-1}}|1\rangle\right)|k\rangle$$

Quantum phase estimation: step 2



$(t \geq 1)$

$$e^{2\pi i\cdot\frac{2^{t-1}\theta_{k_1}}{2}} = e^{2\pi i\cdot m\cdot(0 \text{ or } 1)} = 1$$

Use phase kickback

$$\frac{1}{\sqrt{2}}\left(|0\rangle + \underbrace{\left(e^{2\pi i\theta_k}\right)^{2^{t-1}}}|1\rangle\right)|k\rangle$$

$$\left(e^{2\pi i\theta_k}\right)^{2^{t-1}} = \left(e^{2\pi i\left(\frac{\theta_{k_1}}{2}+\frac{\theta_{k_2}}{4}+\cdots+\frac{\theta_{k_t}}{2^t}\right)}\right)^{2^{t-1}}$$

$t-1$

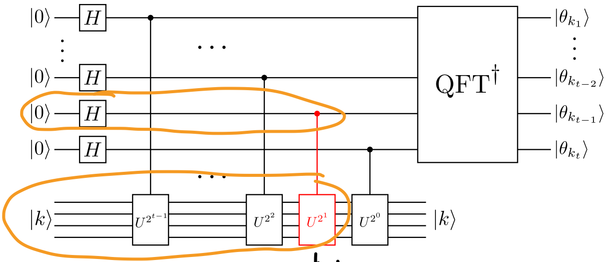
bits

$$\frac{2^{t-1}}{2^t}\cdot\theta_{k_t} = \frac{\theta_{k_t}}{2}$$

$$= e^{2\pi i\left(\frac{2^{t-1}\theta_{k_1}}{2}+\frac{2^{t-1}\theta_{k_2}}{4}+\cdots+\frac{2^{t-1}\theta_{k_t}}{2^t}\right)}$$

$$= e^{2\pi i\cdot 0.\theta_{k_t}}$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.\theta_{k_t}}|1\rangle\right)|k\rangle$$



$$U^{2^1} = U^2$$

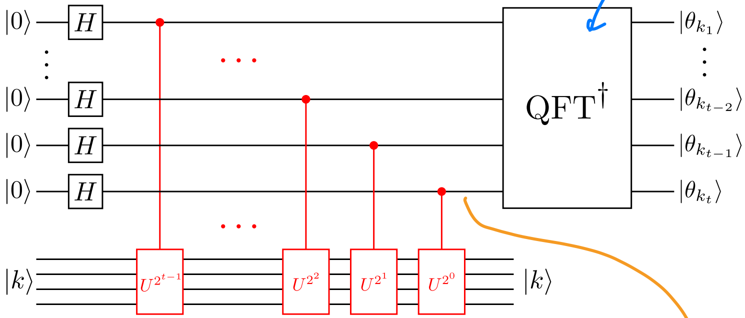
Check second-last qubit (ignore the others)

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|k\rangle \xrightarrow{C-U^2} \frac{1}{\sqrt{2}}|0\rangle|k\rangle + \frac{1}{\sqrt{2}}|1\rangle\left(e^{2\pi i\theta_k}\right)^2|k\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + \underbrace{\left(e^{2\pi i\theta_k}\right)^2}\,|1\rangle\right)|k\rangle$$

$$e^{2\pi i\cdot 2\theta_k} = e^{2\pi i\cdot 2\left(\frac{\theta_{k_1}}{2}+\frac{\theta_{k_2}}{4}+\dots+\frac{\theta_{k_t}}{2^{t}}\right)} = e^{2\pi i\left(\theta_{k_1}+\frac{\theta_{k_2}}{2}+\frac{\theta_{k_3}}{4}+\dots\right)} = e^{2\pi i\, 0.\theta_{k_2}\theta_{k_3}\cdots\theta_{k_t}}$$

Quantum phase estimation: step 2



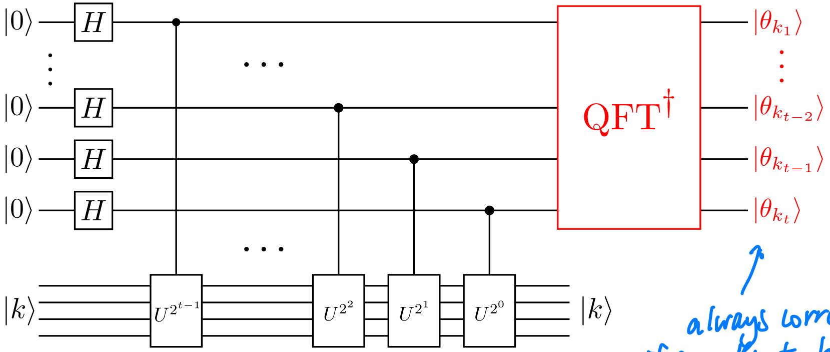
After step 2, we have the state

$$\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_t}}|1\rangle)\cdots\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_2}\cdots\theta_{k_t}}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_1}\cdots\theta_{k_t}}|1\rangle)|k\rangle$$

$$= \mathrm{QFT}\,|\theta_{k_1}\theta_{k_2}\cdots\theta_{k_t}\rangle$$

Quantum phase estimation: step 3

Measure to learn the bits of θ_k.



always correct if exactly t bits and $|k\rangle$ is exact eigenstate

Example: QPE for the T gate

Let's apply QPE to estimate the phase of an eigenstate of T: $|1\rangle$.

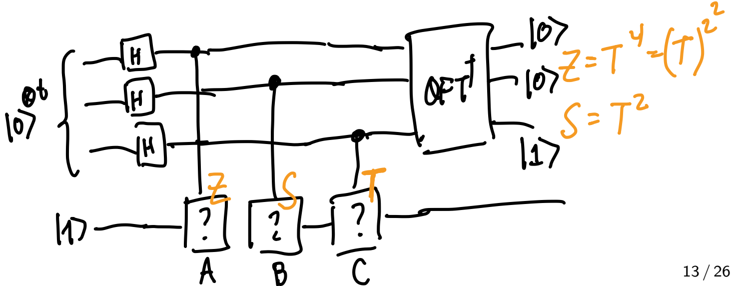
1. What answer do we expect?
2. How many estimation bits?
3. What does the circuit look like?

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

(1) $\theta = \frac{1}{8} \Rightarrow e^{\frac{i\pi}{4}} = e^{2\pi i \cdot \frac{1}{8}}$ $\quad \theta = 0.125$

(2) $t = 3$

(3)



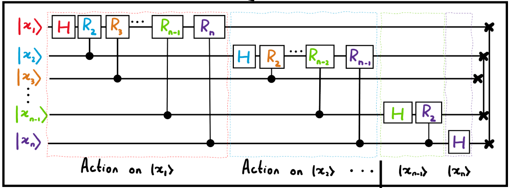
Example: QPE for the T gate

Let's apply QPE to estimate the phase of an eigenstate of T: $|1\rangle$.

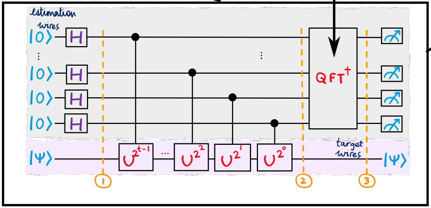
1. What answer do we expect?
2. How many estimation bits?
3. What does the circuit look like?

Reminder: where are we going?

1. QFT



2. QPE



3. Shor

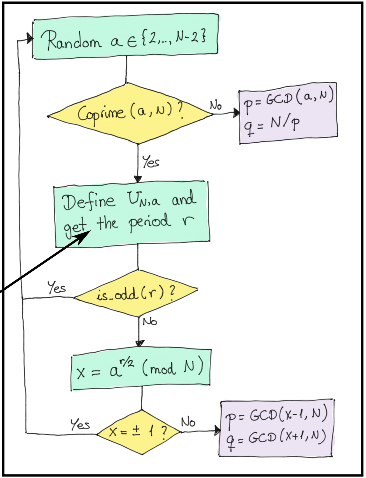


Image credit: Xanadu Quantum Codebook nodes F.3, P.3, S.4

Order finding on a quantum computer

$$7 \cdot \cancel{4} \ \% \ 12 = 4$$

Suppose we have a function

$$f(x)$$

over the integers modulo N. → in Shor, this is the thing we want to factor

If there exists $r \in \mathbb{Z}$ s.t.

$$f(x+r) = f(x) \quad \forall x$$

$f(x)$ is periodic with period r.

Suppose

$$f_{a,N}(x) = a^x \bmod N \qquad a \in \mathbb{Z}$$

non-zero

The *order* of *a* is the smallest *m* such that

$$f(m) = a^{m} \bmod N = 1 \bmod N$$

find this!

Note that this is also the period:

$$f(x+m) = a^{x+m} \underset{\bmod N}{=} a^x a^m \underset{\bmod N}{=} a^x \underset{\bmod N}{=} f(x)$$

Exercise: find the order of $a = 5$ for $N = 7$. $\Rightarrow 6$

1 5

2 $25 \% 7 = 4$

3 $125 \% 7 = \cdots$

4

$\vdots$

6 $5^6 = (5^2)(5^2)(5^2) = 4 \cdot 4 \cdot 4 = 64 \Rightarrow 64 \% 7 = 1$

More formally, define

$$f_{N,a}(x) = a^x \bmod N$$

$$\to f_{N,a}(m) = a^m \bmod N = 1$$

Define a unitary operation that performs

$$U_{N,a} |k\rangle = |ka \bmod N\rangle$$

If m is the order of a, and we apply $U_{N,a}$ m times,

$$(U_{N,a})^m |k\rangle = |k \cdot a^m \bmod N\rangle = |k\rangle$$

So m is also the order of $U_{N,a}$! We can find it efficiently using a quantum computer.

Next time

Content:

- Hands-on about RSA
- Shor's algorithm

Action items:

1. A3 when available
2. Work on project

Recommended reading:

- Codebook modules QFT, QPE, SH
- Nielsen & Chuang 5.3, Appendix A.5