CPEN 400Q Lecture 11
Quantum phase estimation; order finding

Monday 13 February 2023

Announcements

- Quiz 5 today
- (Technical) assignment 2 available soon
- Project group and paper selection due Friday (use Piazza to find teammates)

Last time

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

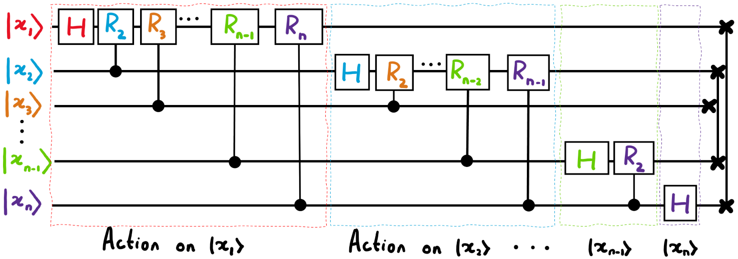


Image credit: Xanadu Quantum Codebook node F.3

Last time

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

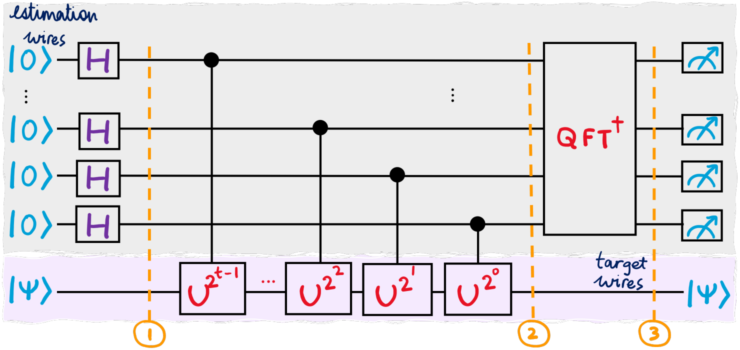


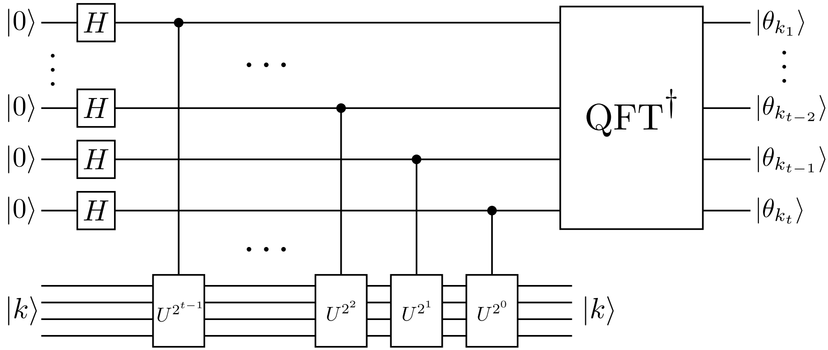
Image credit: Xanadu Quantum Codebook node P.2

Last time

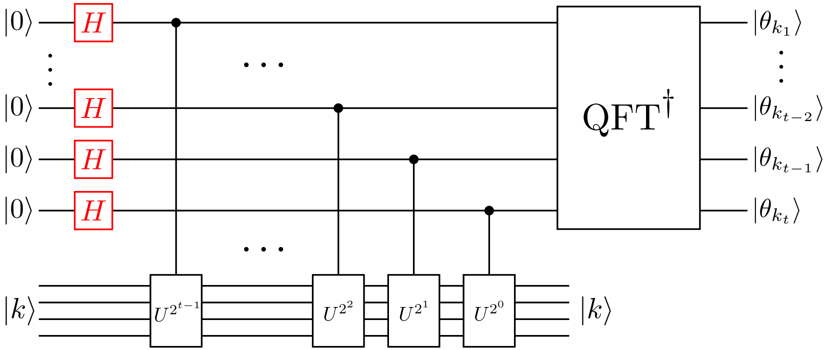
We saw the *phase kickback trick*.

Learning outcomes

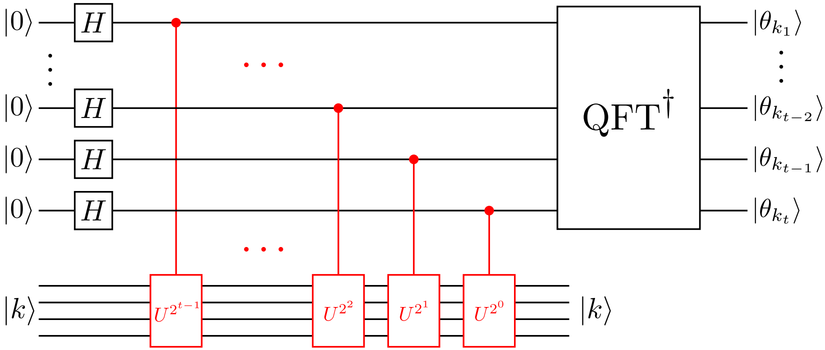
- Outline the steps of the quantum phase estimation (QPE) subroutine
- Use the QFT to implement QPE
- Use QPE to implement the order finding algorithm


$|0\rangle$
H
$|0\rangle$
H
$|0\rangle$
H
$|0\rangle$
H
$|k\rangle$
$U^{2^{t-1}}$
U^{2^2}
U^{2^1}
U^{2^0}
$|k\rangle$
$\mathrm{QFT}^\dagger$
$|\theta_{k_1}\rangle$
$|\theta_{k_{t-2}}\rangle$
$|\theta_{k_{t-1}}\rangle$
$|\theta_{k_t}\rangle$

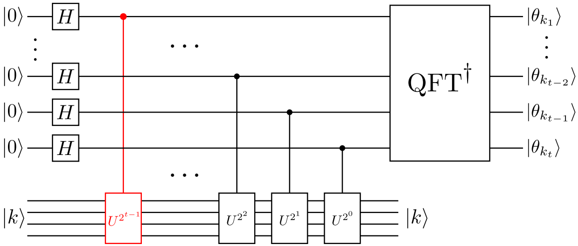
Quantum phase estimation: step 1



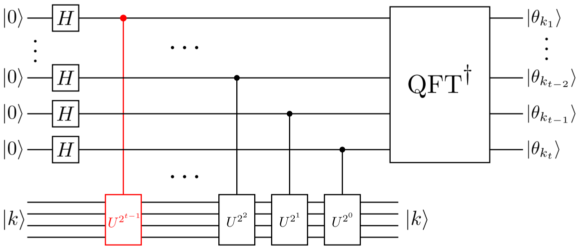
Quantum phase estimation: step 1



Quantum phase estimation: step 2

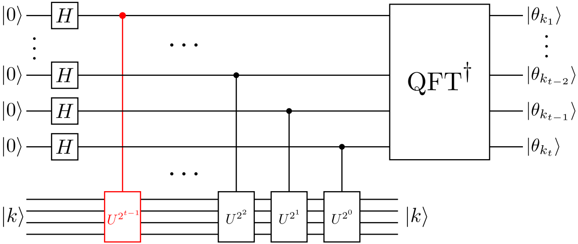


Quantum phase estimation: step 2



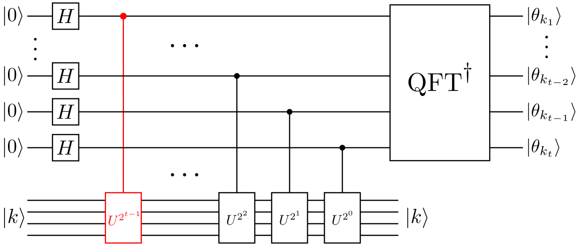
Use phase kickback

Quantum phase estimation: step 2

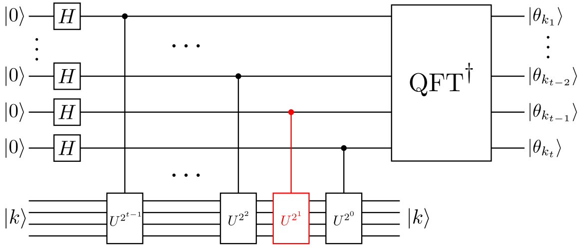


What is happening in the exponent?

Quantum phase estimation: step 2

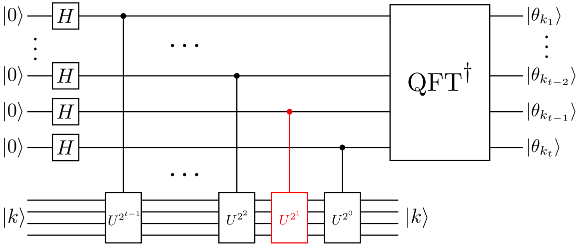


Quantum phase estimation: step 2



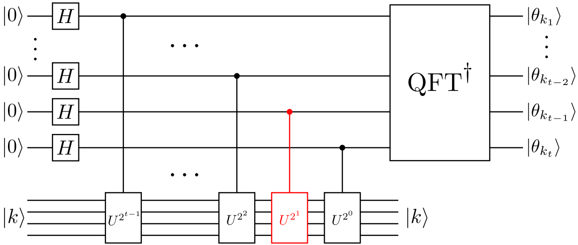
Check second-last qubit (ignore the others)

Quantum phase estimation: step 2

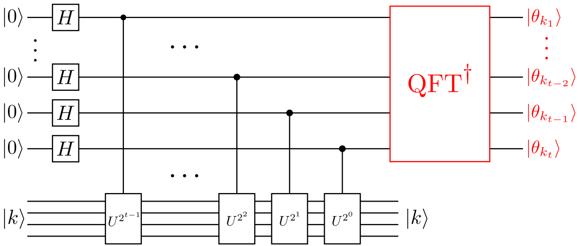


Again check the exponent...

Quantum phase estimation: step 2

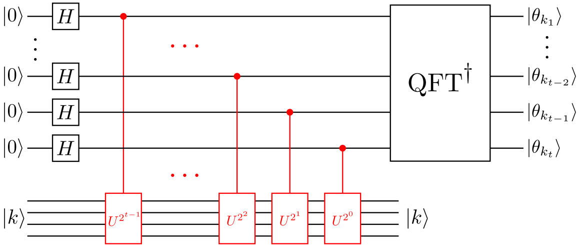


Quantum phase estimation: step 2



Can show in the same way for the last qubit (ignore others)

Quantum phase estimation: step 2



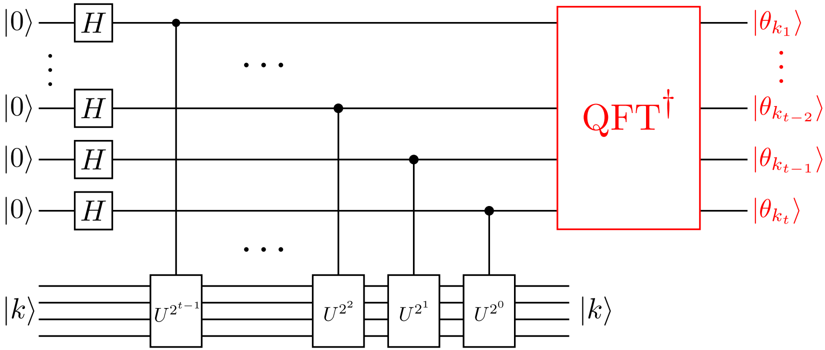
After step 2, we have the state

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

Should look familiar!

Quantum phase estimation: step 3

Measure to learn the bits of θ_k.



Let's implement it.

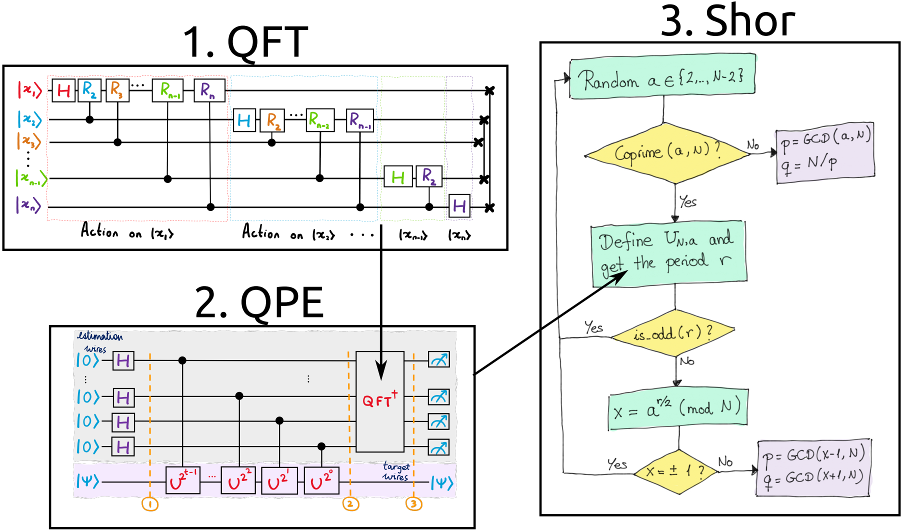


Image credit: Xanadu Quantum Codebook nodes F.3, P.3, S.4

Suppose we have a function

over the integers modulo N.

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

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

Order finding on a quantum computer

Suppose

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

Note that this is also the period:

Order finding on a quantum computer

More formally, define

Define a unitary operation that performs

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

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

Order finding on a quantum computer

Let U be an operator and $|\phi\rangle$ any state. How do we find the minimum r such that

QPE does the trick if we set things up in a clever way:

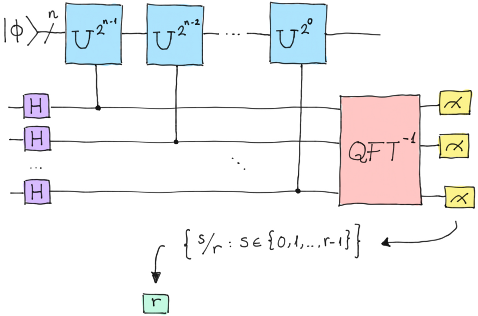


Image credit: Xanadu Quantum Codebook node S.3

Consider the state

If we apply U to this:

Now consider the state

If we apply U to this:

This generalizes to $|\Psi_s\rangle$

It has eigenvalue

Idea: if we can create *any* one of these $|\Psi_s\rangle$, we could run QPE and get an estimate for s/r, and then recover r.

Problem: to construct any $|\Psi_s\rangle$, we would need to know r in advance!

Solution: construct the uniform superposition of all of them.

But what does this equal?

The superposition of all $|\Psi_s\rangle$ is just our original state $|\phi\rangle$!

$$
|\Psi\rangle = \frac{1}{\sqrt{r}} \cdot \left(\begin{array}{l} |\Psi_0\rangle + \\ + |\Psi_1\rangle + \\ \quad \vdots \\ + |\Psi_{r-1}\rangle \end{array} \right) = \frac{1}{\sqrt{r}} \cdot \begin{array}{l}
1/\sqrt{r} \left(|\phi\rangle + 1 \cdot U|\phi\rangle + \cdots + 1 \cdot U^{r-1}|\phi\rangle \right) \\
+ 1/\sqrt{r} \left(|\phi\rangle + e^{\frac{-2\pi i}{r}} U|\phi\rangle + \cdots + e^{\frac{-2\pi i (r-1)}{r}} U^{r-1}|\phi\rangle \right) \\
\quad \vdots \\
+ 1/\sqrt{r} \left(|\phi\rangle + e^{\frac{-2\pi i (r-1)}{r}} U|\phi\rangle + \cdots + e^{\frac{-2\pi i (r-1)^2}{r}} U^{r-1}|\phi\rangle \right) \\
\quad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \\
\quad r \qquad\qquad\; 0 \quad \cdots \quad 0 \quad \cdots \quad 0
\end{array}
$$

$$
= 1/\sqrt{r} \cdot 1/\sqrt{r} \cdot r\,|\phi\rangle = \boxed{|\phi\rangle}
$$

If we run QPE, the output will be s/r for one of these states.

Image credit: Xanadu Quantum Codebook node S.3

Shor's algorithm

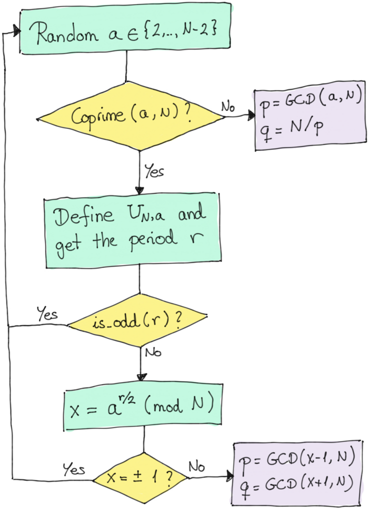


Image credit: Xanadu Quantum Codebook node S.4

Next time

Content:

- RSA
- Shor's algorithm

Action items:

1. Start working on prototype implementation for project

Recommended reading:

- Codebook modules F, P, and S
- Nielsen & Chuang 5.3, Appendix A.5