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:

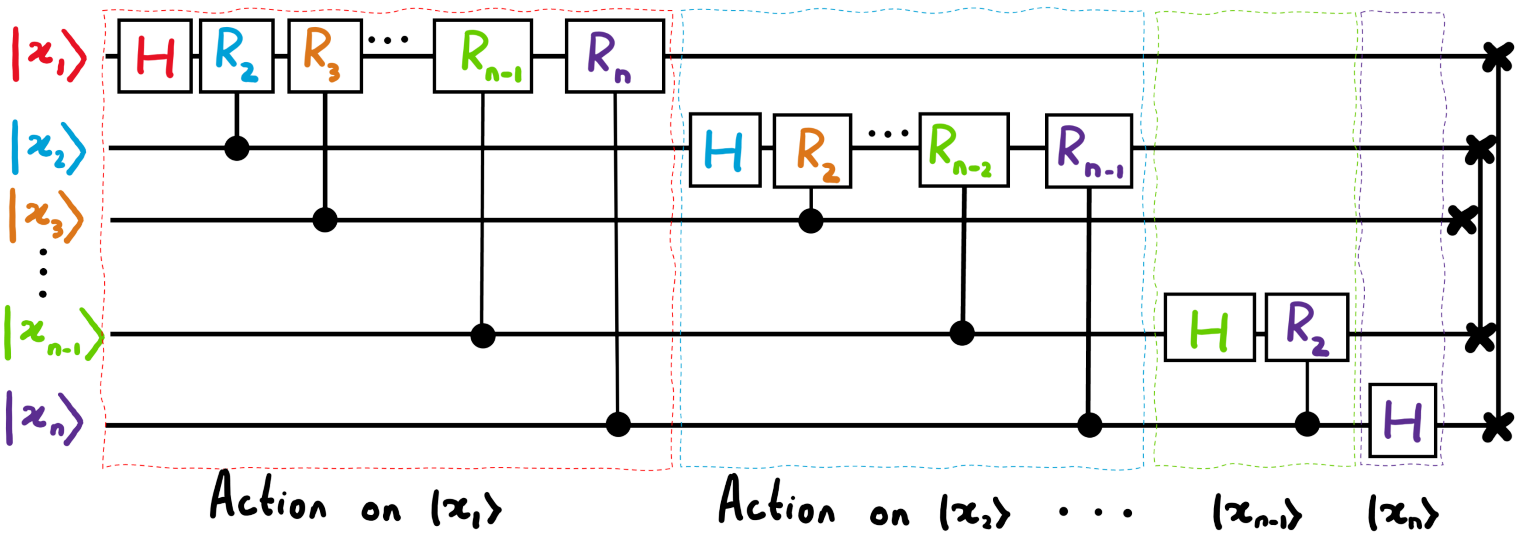


Image credit: Xanadu Quantum Codebook node F.3

Last time

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

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

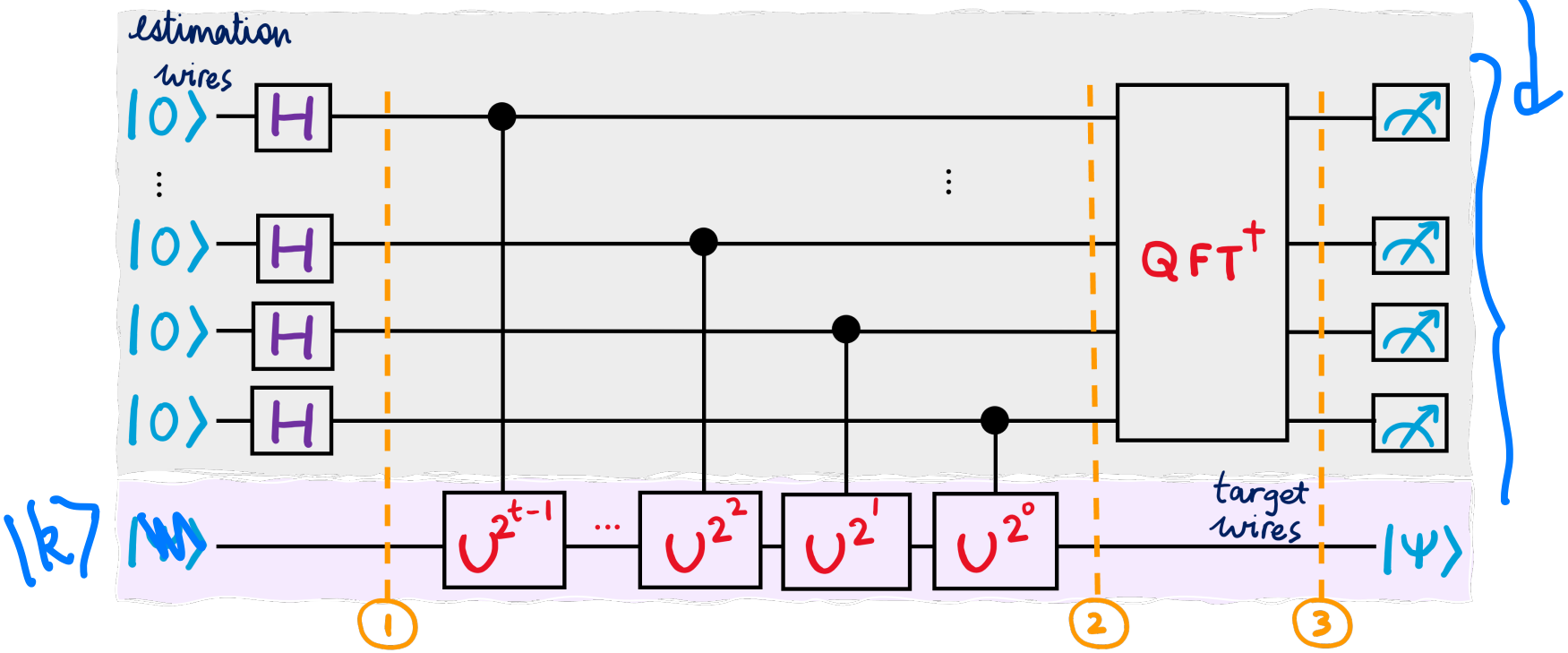
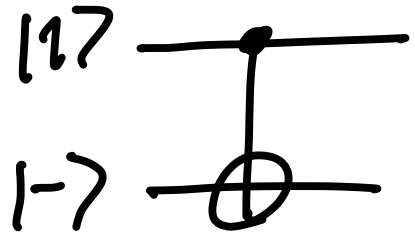


Image credit: Xanadu Quantum Codebook node P.2

Last time



We saw the *phase kickback trick*.

$$\text{CNOT}\,|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = |1\rangle\left(\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right)$$

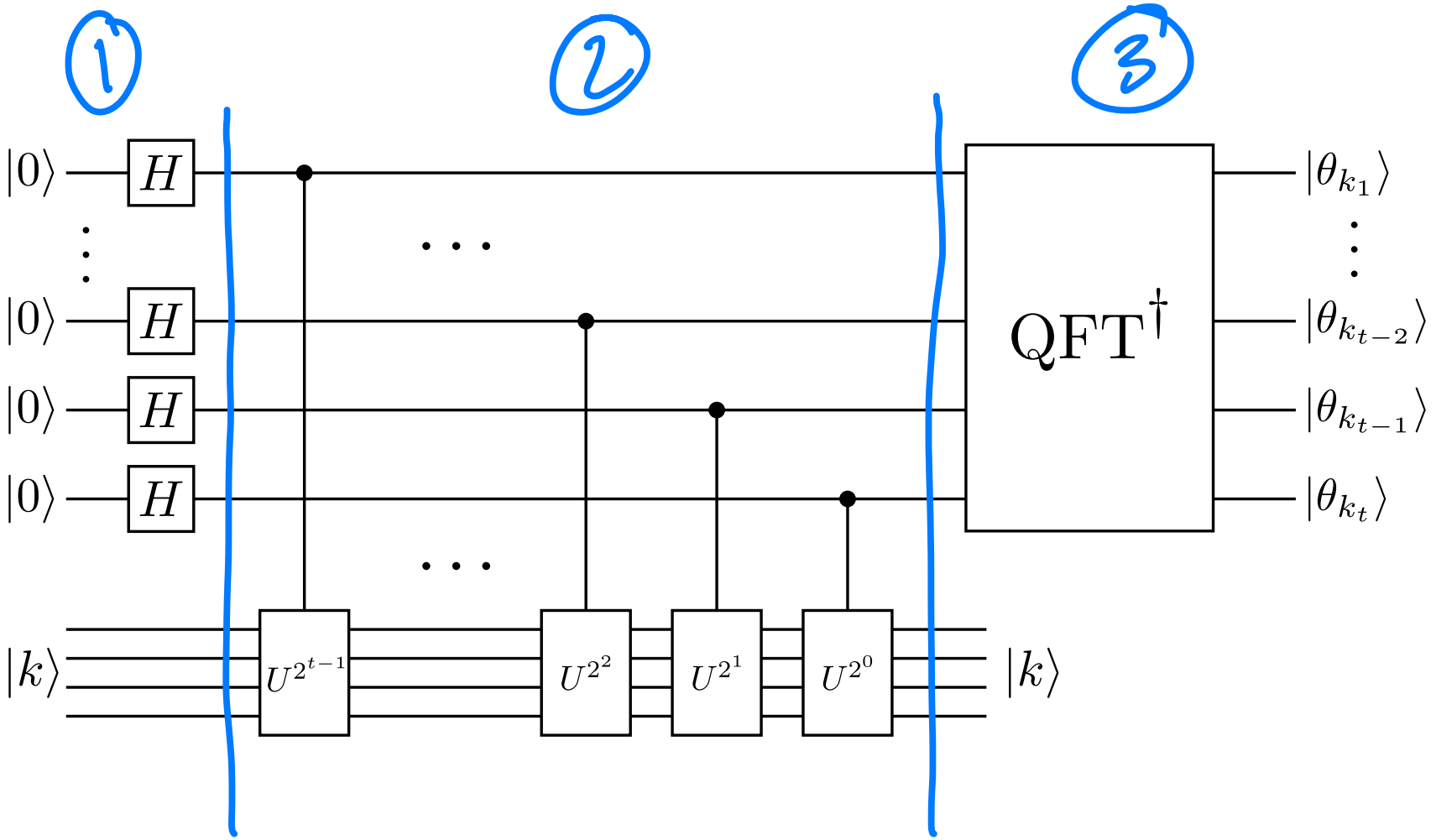
$$= |1\rangle(-|-\rangle)$$

$$= (-|1\rangle)\,|-\rangle$$

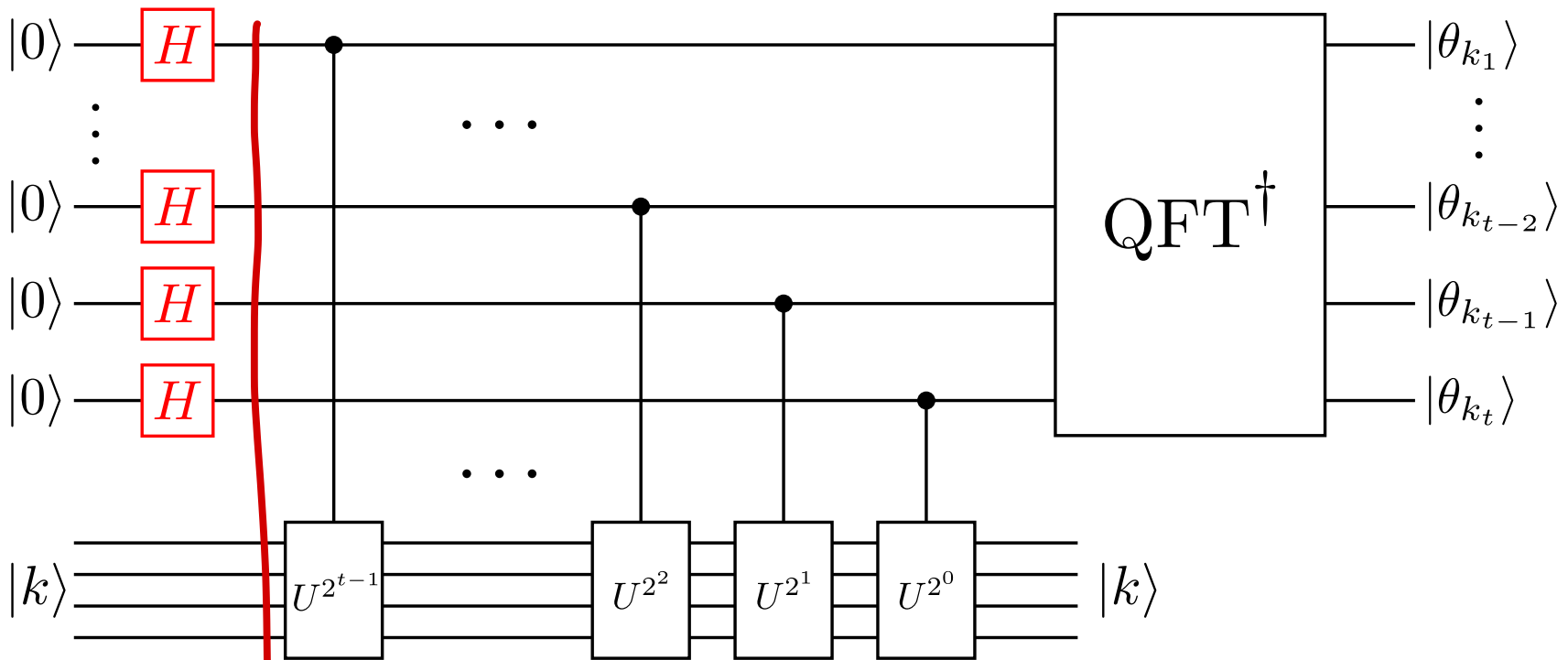
Learning outcomes

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

Quantum phase estimation



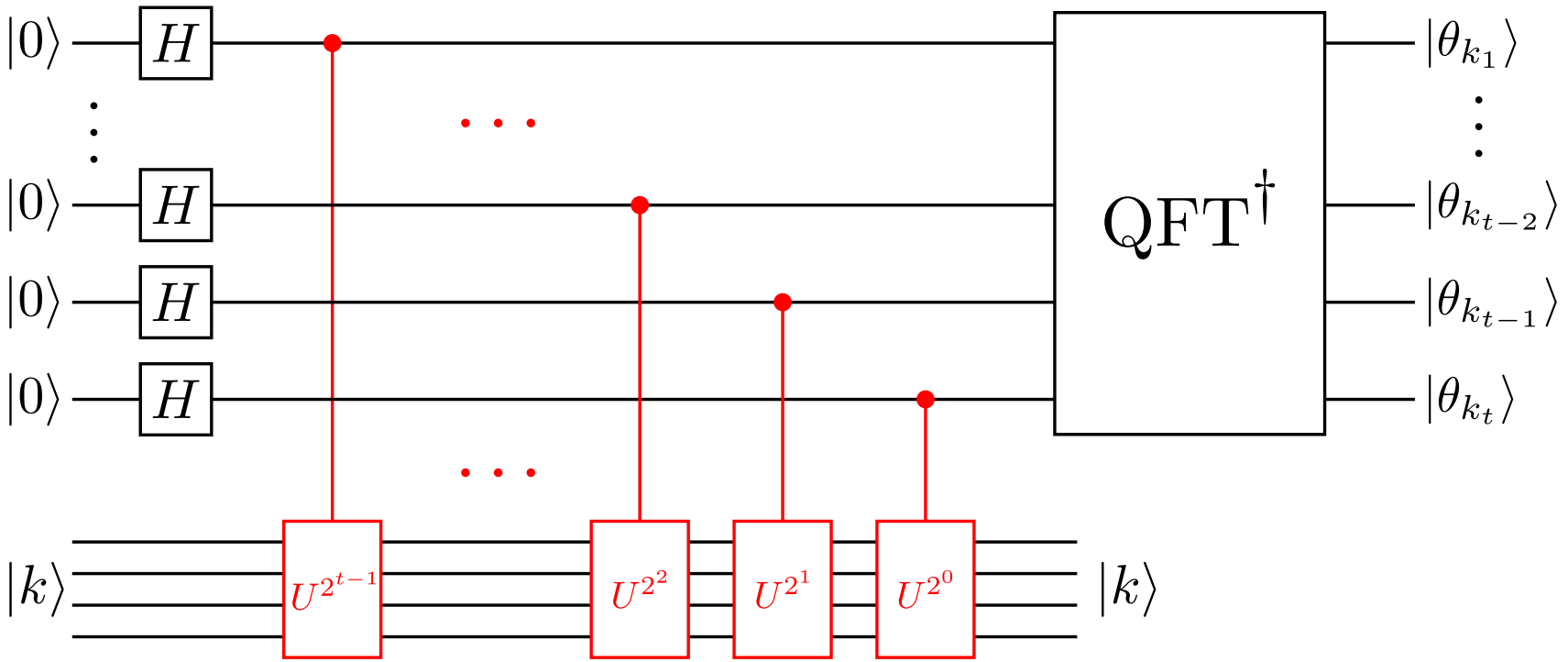
Quantum phase estimation: step 1



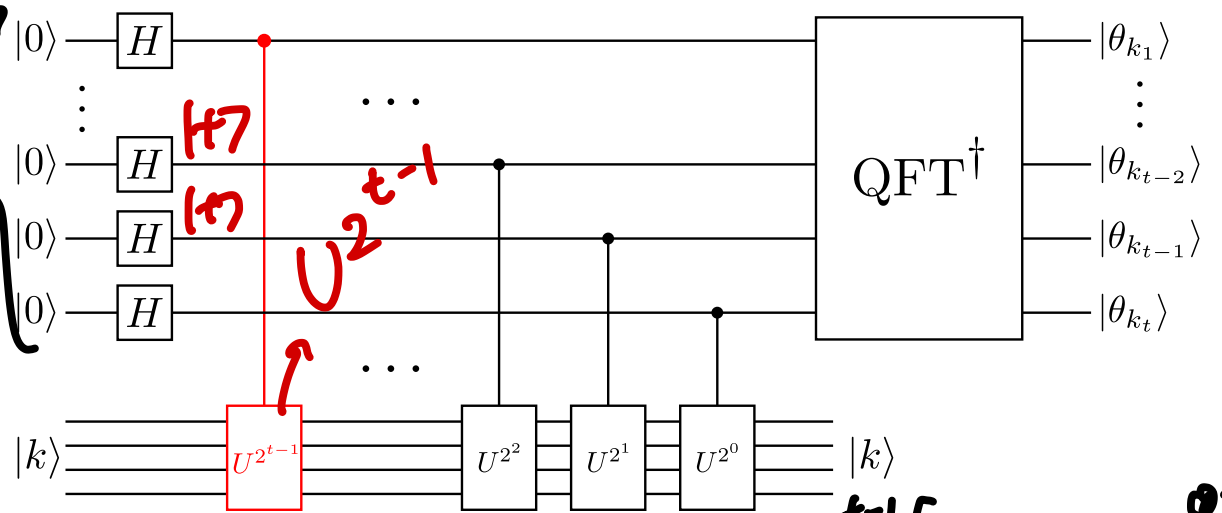
① uniform superposition

$\frac{(|0\rangle+|1\rangle)}{\sqrt{2}} \otimes \frac{(|0\rangle+|1\rangle)}{\sqrt{2}} \cdots$

Quantum phase estimation: step 1



Quantum phase estimation: step 2



$|+\rangle^{\otimes n}$ t

$|+\rangle\otimes|+\rangle\otimes\cdots\otimes|+\rangle$

xn

$|+\rangle$

$|+\rangle$

$U^{2^{t-1}}$

$(CU)^{2^{t-1}}\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|+\rangle^{\otimes t-1}|k\rangle\right] = (CU)^{2^{t-1}}\left(\frac{1}{\sqrt{2}}|0\rangle|+\rangle^{\otimes t-1}|k\rangle\right)$

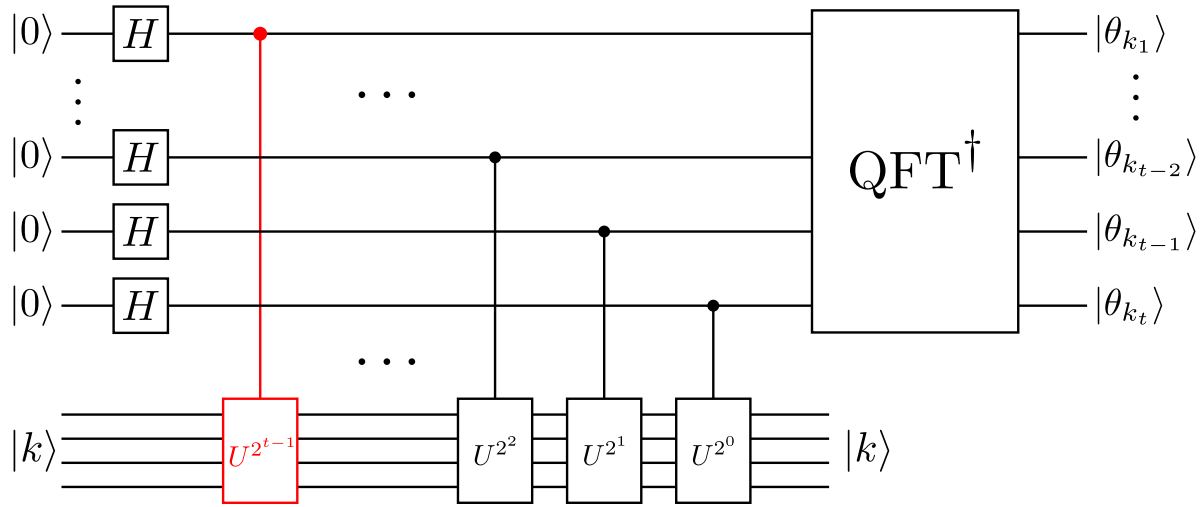
$+(CU)^{2^{t-1}}\left(\frac{1}{\sqrt{2}}|1\rangle|+\rangle^{\otimes t-1}|k\rangle\right)$

$= \frac{1}{\sqrt{2}}|0\rangle|+\rangle^{\otimes t-1}|k\rangle$

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

ctrl'd U

Quantum phase estimation: step 2



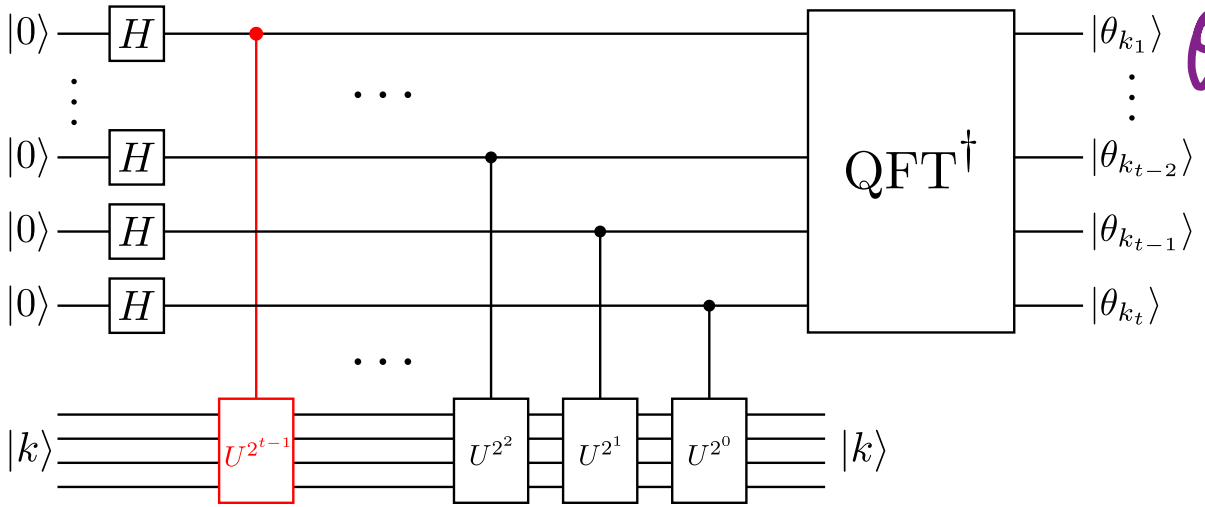
Use phase kickback

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

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

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

Quantum phase estimation: step 2



$e^{2\pi i \theta_k}$

$0 < \theta_k \leq 1$

$\theta_k = 0.\theta_{k_1}\theta_{k_2}\cdots\theta_{k_t}$

What is happening in the exponent?

$$(e^{2\pi i\theta_k})^{2^{t-1}} = e^{2\pi i\theta_k 2^{t-1}}$$

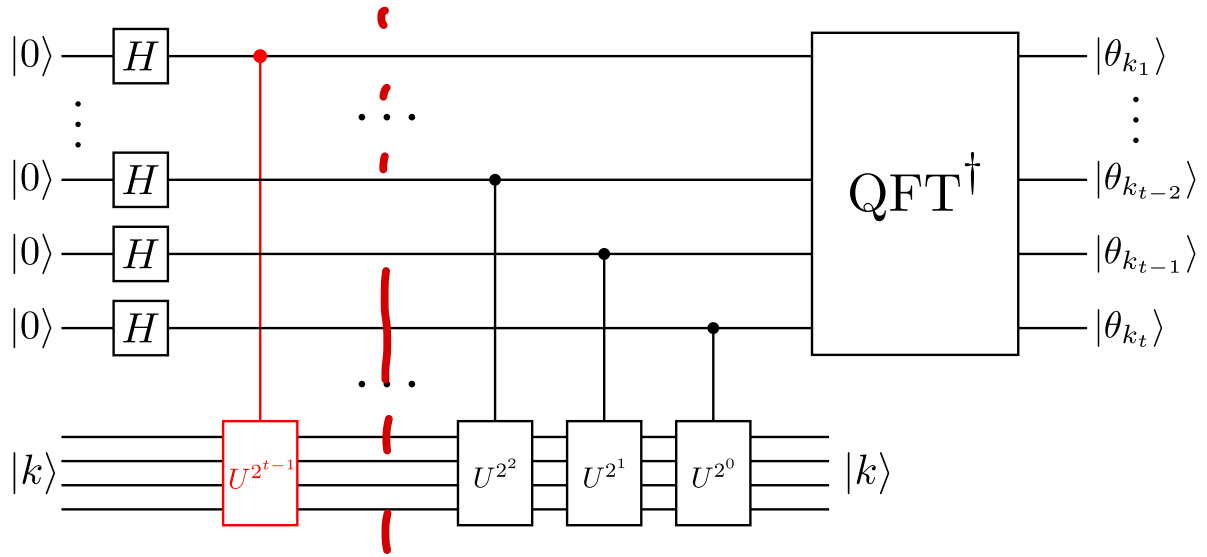
$$= e^{2\pi i\left(\frac{\theta_{k_1}}{2} + \frac{\theta_{k_2}}{2^2} + \cdots \frac{\theta_{k_t}}{2^t}\right)\cdot 2^{t-1}}$$

$$= e^{2\pi i\left(2^{t-2}\theta_{k_1} + 2^{t-3}\theta_{k_2} + \cdots + \theta_{k_{t-1}} + \frac{1}{2}\theta_{k_t}\right)}$$

$$= e^{2\pi i \cdot \frac{1}{2}\theta_{k_t}}$$

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

Quantum phase estimation: step 2

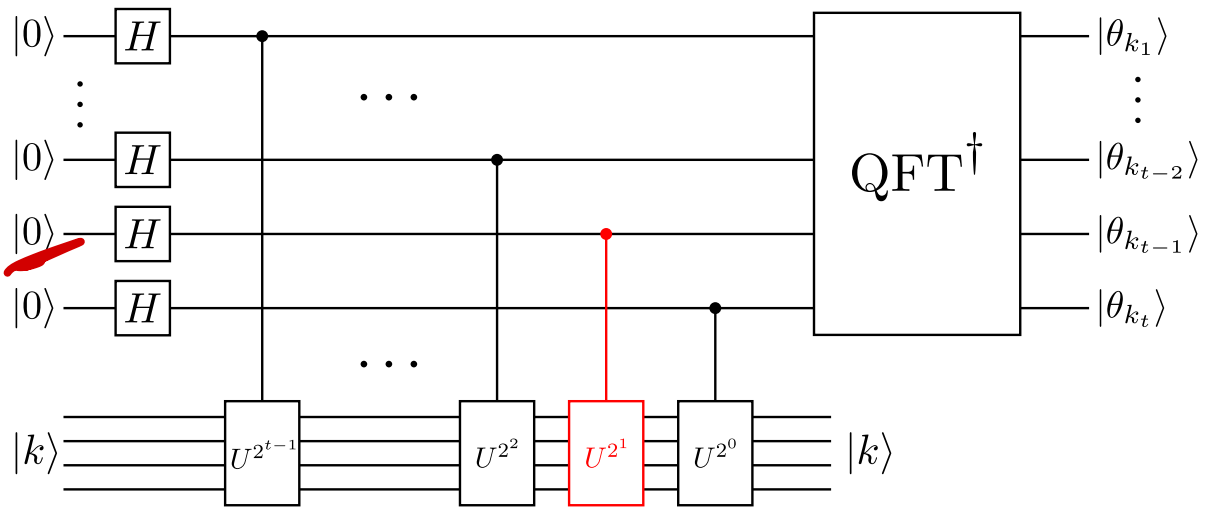


$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.\theta_{k_t}}|1\rangle\right)|+\rangle^{\otimes t-1}|k\rangle$$

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

$$= \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.\theta_{k_t}}|1\rangle)|+\rangle^{\otimes t-1}|k\rangle$$

Quantum phase estimation: step 2

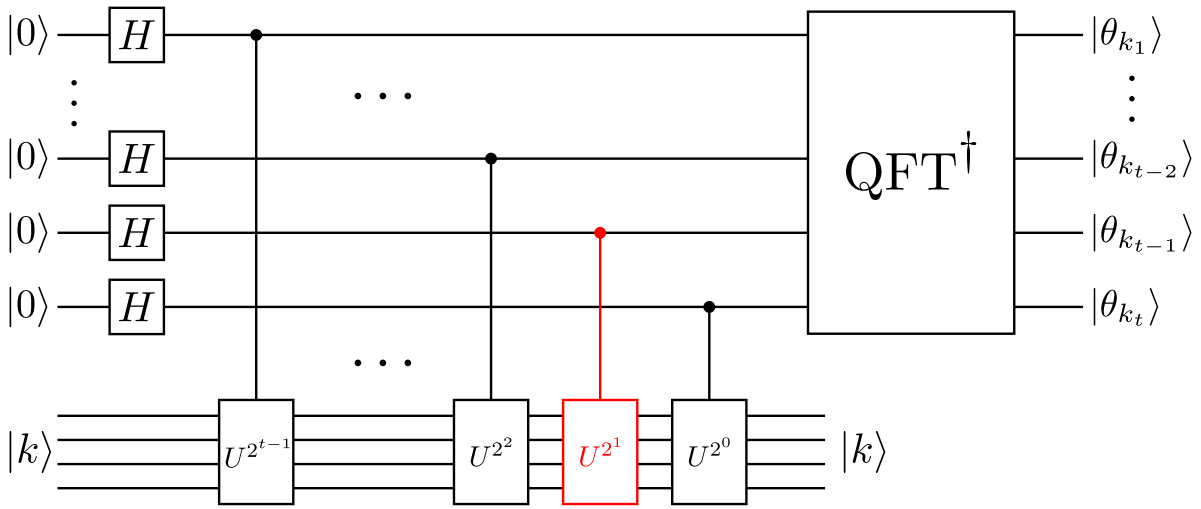


Check second-last qubit (ignore the others)

$$(CU)^2\left[|+\rangle^{\otimes t-2}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|+\rangle|k\rangle\right]$$

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

Quantum phase estimation: step 2



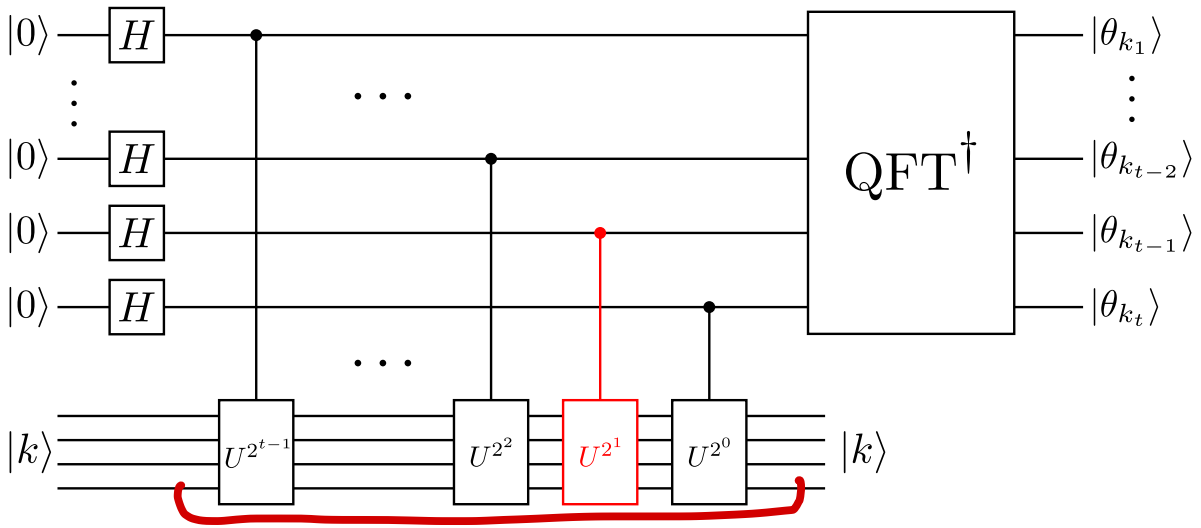
Again check the exponent...

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

$$= e^{2\pi i\ 0.\theta_{k_2}\cdots\theta_{k_t}}$$

$$|+\rangle^{\otimes t-2}\ \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\ 0.k_2\cdots k_t}|1\rangle\right)|+\rangle\,|k\rangle$$

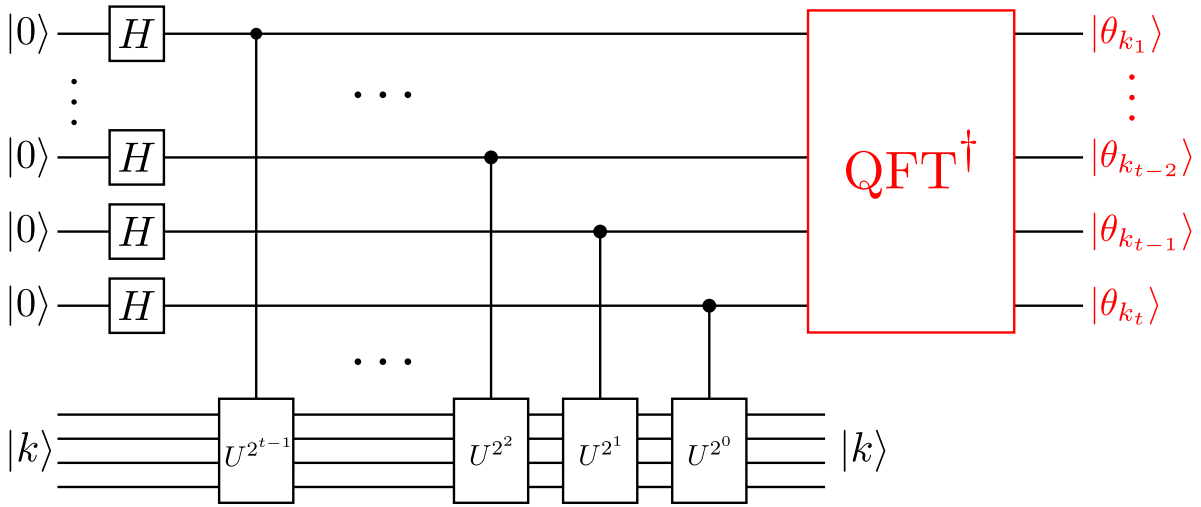
Quantum phase estimation: step 2



$$\frac{(|0\rangle + e^{2\pi i\, 0.\theta_{k_t}}|1\rangle)}{\sqrt{2}} \otimes \frac{(|0\rangle + e^{2\pi i\, 0.\theta_{k_{t-1}}\theta_t}|1\rangle)}{\sqrt{2}} \otimes \cdots \otimes \frac{(|0\rangle + e^{2\pi i\, 0.\theta_{k_1}\cdots\theta_{k_t}}|1\rangle)}{\sqrt{2}} \otimes |k\rangle$$

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

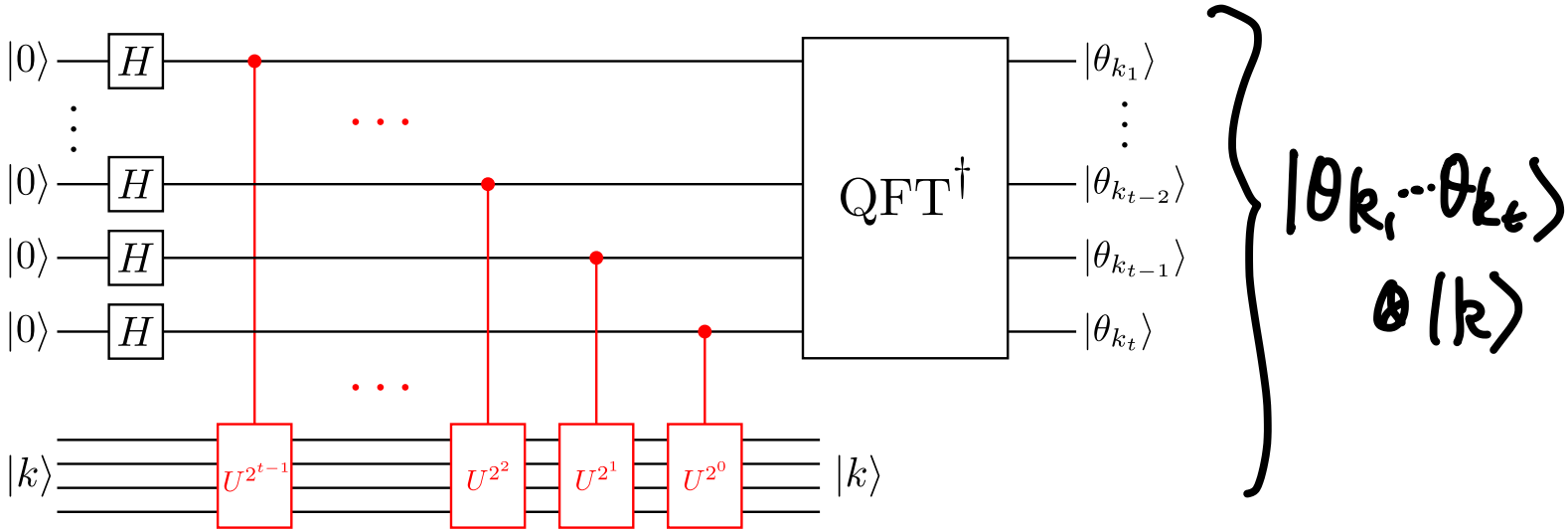
Quantum phase estimation: step 2



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

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

Quantum phase estimation: step 2



After step 2, we have the state

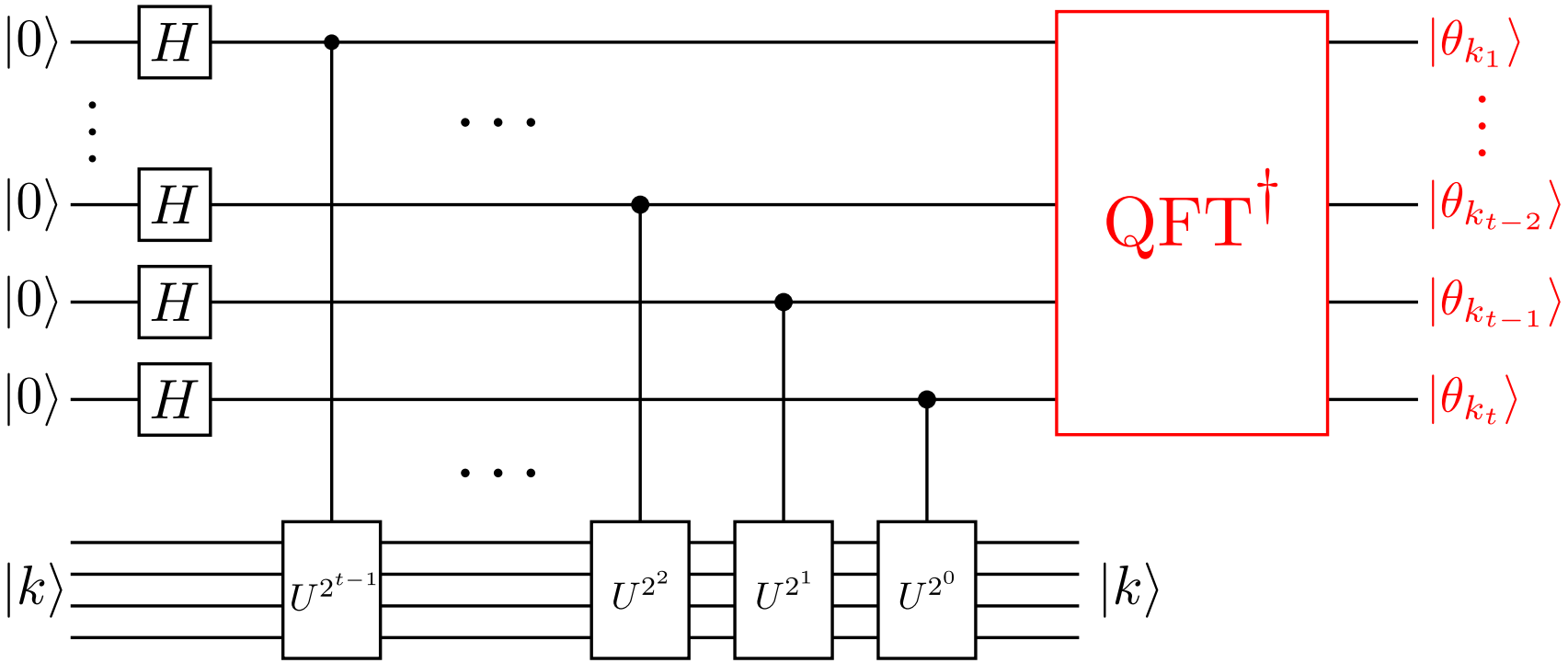
$$\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_t}}|1\rangle)\cdots\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_2}\cdots\theta_{k_t}}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i 0.\theta_{k_1}\cdots\theta_{k_t}}|1\rangle)|k\rangle$$

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

Should look familiar!

Quantum phase estimation: step 3

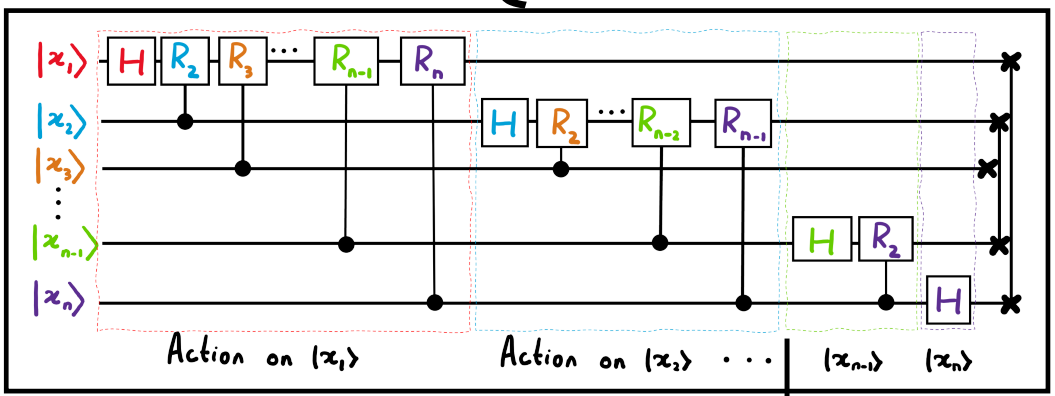
Measure to learn the bits of θ_k.



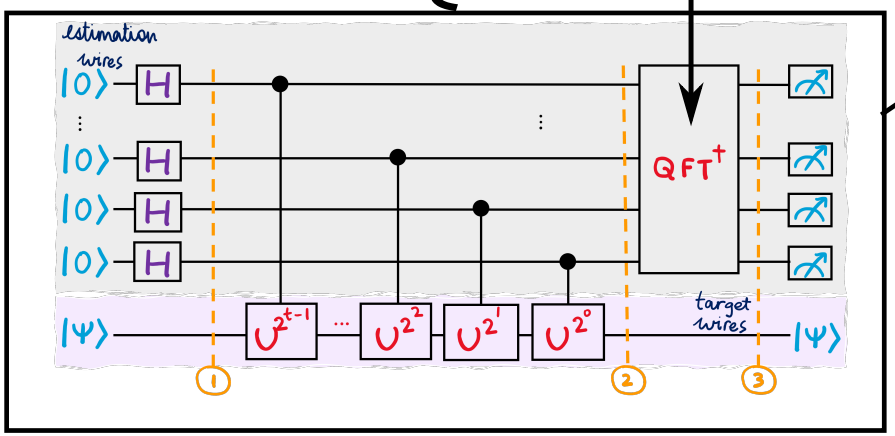
Let's implement it.

Reminder: where are we going?

1. QFT ✓



2. QPE ✓



3. Shor

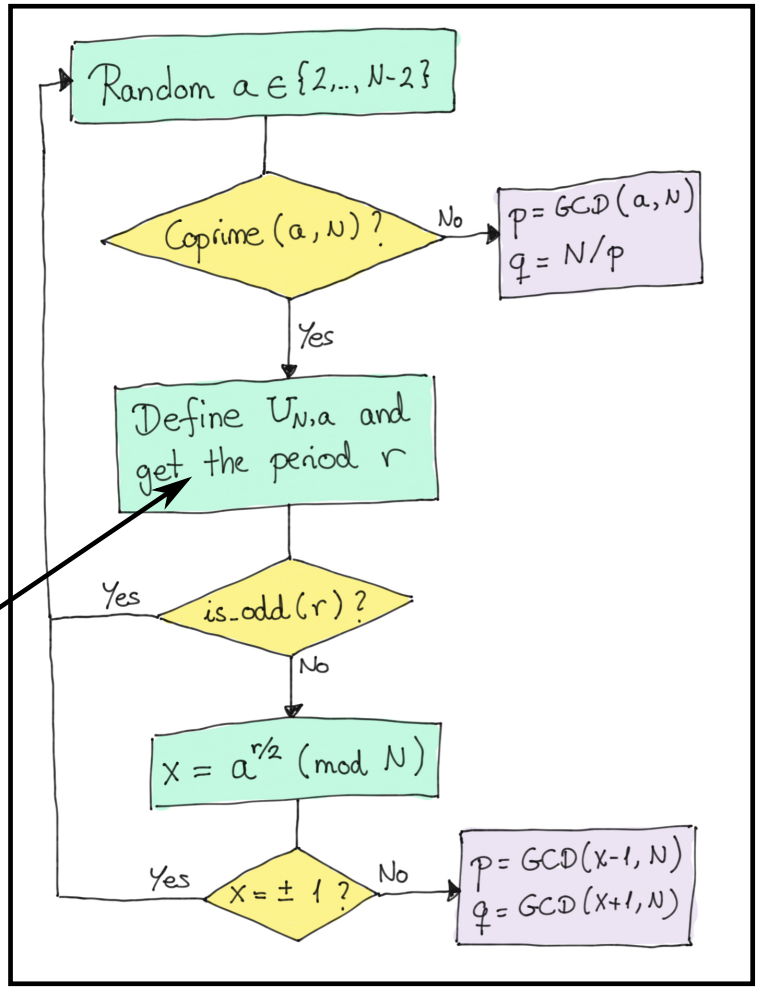


Image credit: Xanadu Quantum Codebook nodes F.3, P.3, S.4

Order finding on a quantum computer

S.1

Suppose we have a function

$$f(x)$$

over the integers modulo N.

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

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

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

Order finding on a quantum computer

Suppose

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

$$f(x) = a^x \bmod N$$

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

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

Note that this is also the period:

$$f(x+m) = a^{x+m} = a^x \underbrace{a^m}_{=1} = a^x = f(x)$$

Order finding on a quantum computer

More formally, define

$$f_{N,a}(m) = a^m \overset{?}{\equiv} 1 \bmod N$$

Define a unitary operation that performs

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

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

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

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

We will start here on Friday.

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

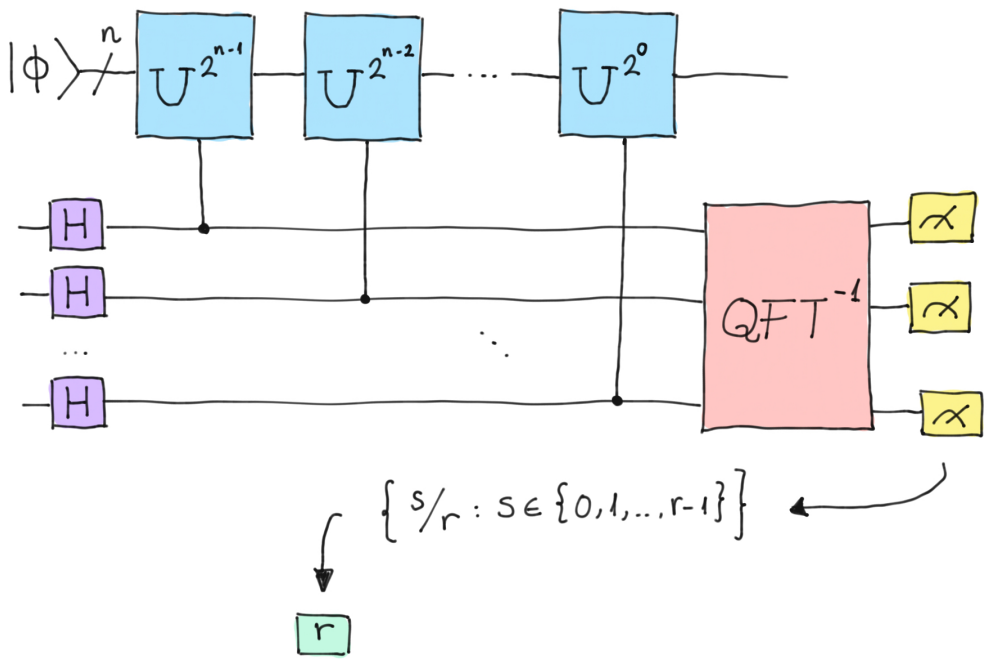


Image credit: Xanadu Quantum Codebook node S.3

Order finding on a quantum computer

Consider the state

$$|\Psi_0\rangle = \frac{1}{\sqrt{r}}\left(|\phi\rangle + U|\phi\rangle + \cdots + U^{r-1}|\phi\rangle\right)$$

If we apply U to this:

$$\begin{aligned} U|\Psi_0\rangle &= \frac{1}{\sqrt{r}}\left(U|\phi\rangle + U^2|\phi\rangle + \cdots + U^r|\phi\rangle\right) \\ &= \frac{1}{\sqrt{r}}\left(U|\phi\rangle + U^2|\phi\rangle + \cdots + |\phi\rangle\right) \\ &= |\Psi_0\rangle \end{aligned}$$

Order finding on a quantum computer

Now consider the state

$$|\psi_1\rangle = \frac{1}{\sqrt{r}}\left(|\phi\rangle + e^{-\frac{2\pi i}{r}}U|\phi\rangle + e^{-2\cdot\frac{2\pi i}{r}}U^2|\phi\rangle + \cdots + e^{-(r-1)\cdot\frac{2\pi i}{r}}U^{r-1}|\phi\rangle\right)$$

If we apply U to this:

$$\begin{aligned}
U|\psi_1\rangle &= \frac{1}{\sqrt{r}}\left(U|\phi\rangle + e^{-\frac{2\pi i}{r}}U^2|\phi\rangle + \cdots + e^{-(r-1)\cdot\frac{2\pi i}{r}}U^r|\phi\rangle\right) \\
&= \frac{1}{\sqrt{r}}\left(U|\phi\rangle + e^{-\frac{2\pi i}{r}}U^2|\phi\rangle + \cdots + e^{\frac{2\pi i}{r}}|\phi\rangle\right) \\
&= e^{\frac{2\pi i}{r}}\frac{1}{\sqrt{r}}\left(e^{-\frac{2\pi i}{r}}U|\phi\rangle + e^{-2\frac{2\pi i}{r}}U^2|\phi\rangle + \cdots + |\phi\rangle\right) \\
&= e^{\frac{2\pi i}{r}}|\psi_1\rangle
\end{aligned}$$

Order finding on a quantum computer

This generalizes to $|\Psi_s\rangle$

$$|\Psi_s\rangle = \frac{1}{\sqrt{r}}(|\phi\rangle + e^{-s\frac{2\pi i}{r}} U|\phi\rangle + e^{-2s\cdot\frac{2\pi i}{r}} U^2|\phi\rangle$$
$$+ \cdots + e^{-(r-1)s\cdot\frac{2\pi i}{r}} U^{r-1}|\phi\rangle)$$

It has eigenvalue

$$U|\Psi_s\rangle = e^{\frac{2\pi i s}{r}}|\Psi_s\rangle$$

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.

Order finding on a quantum computer

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

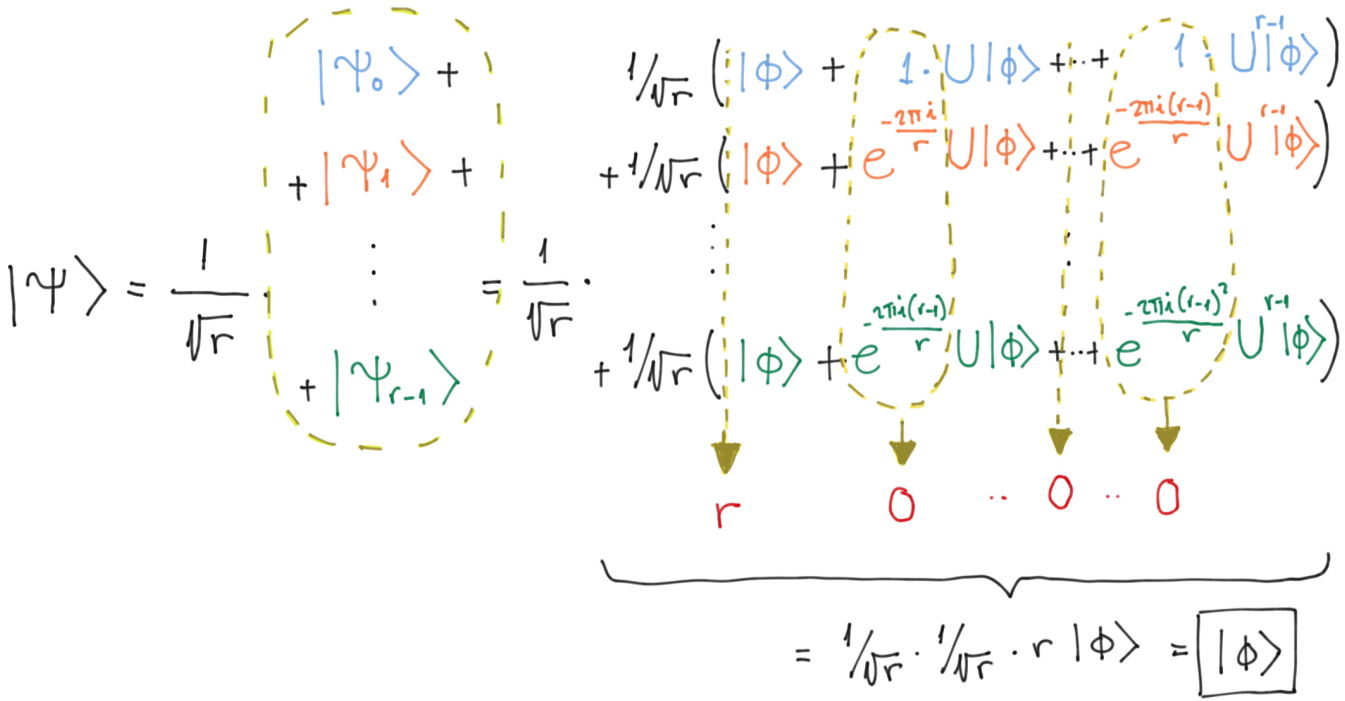
Solution: construct the uniform superposition of all of them.

$$|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\Psi_s\rangle$$

But what does this equal?

Order finding on a quantum computer

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



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

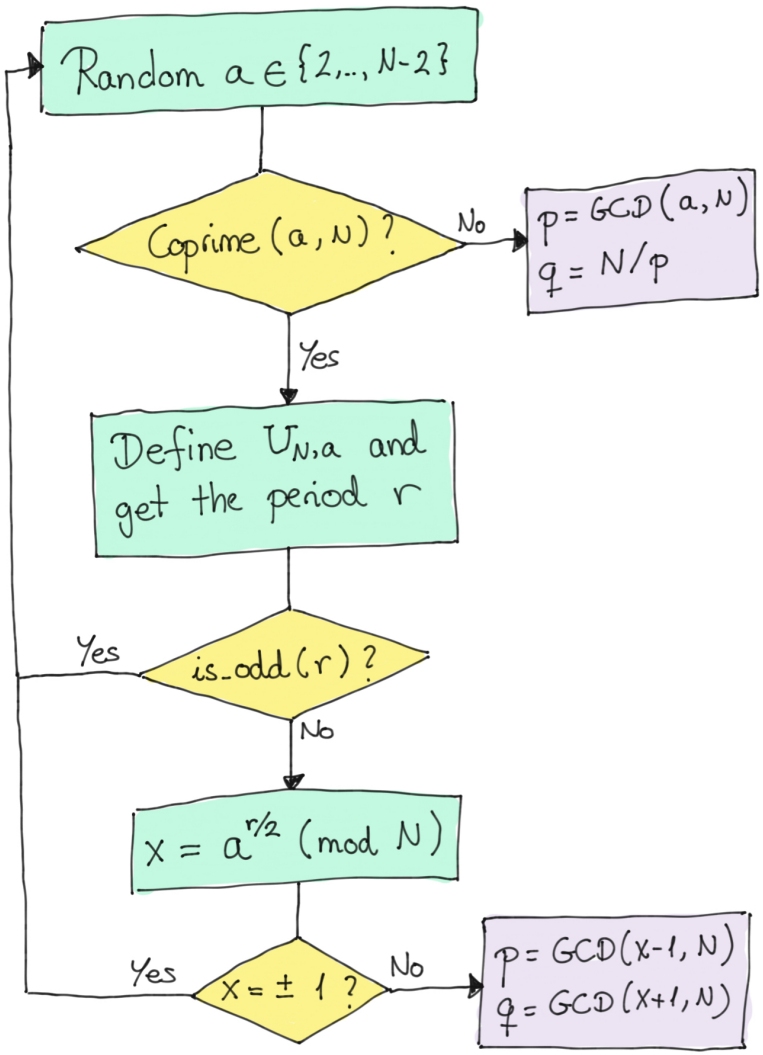


Image credit: Xanadu Quantum Codebook node S.4

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