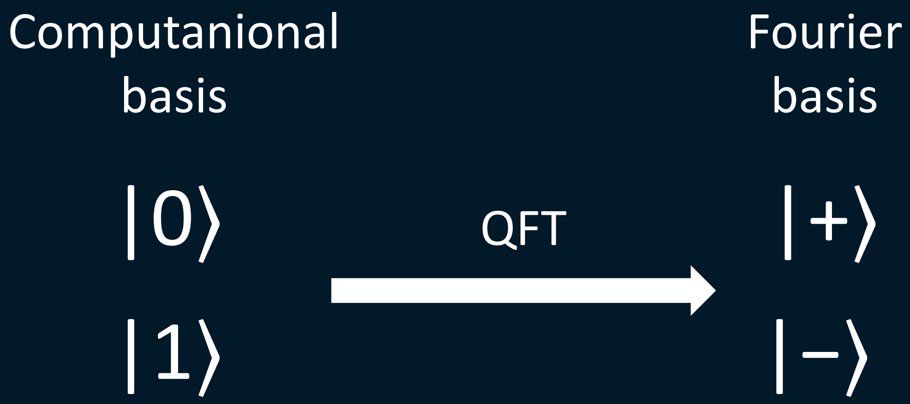
Quantum Fourier transform (QFT)

QFT is effectively a change of basis from the computanional basis to Fourier basis.



Computanional basis

$|0\rangle$

$|1\rangle$

QFT

Fourier basis

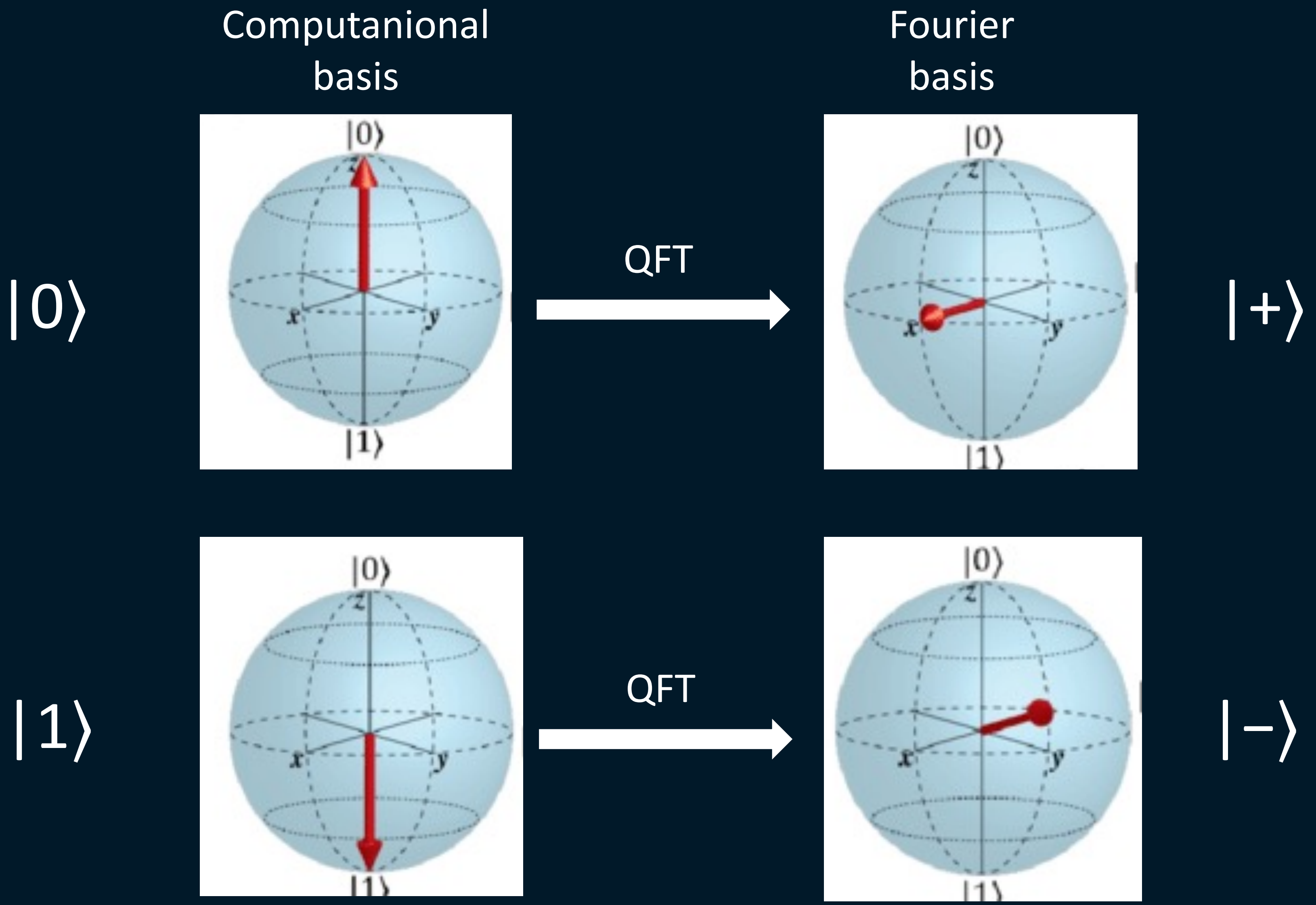
$|+\rangle$

$|-\rangle$

The gate that takes you from the state zero to the state plus and state one to the state minus, is the Hadamar gate!

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Quantum Fourier transform (QFT)



Computanional basis

Fourier basis

$|0\rangle$ QFT $|+\rangle$

$|1\rangle$ QFT $|-\rangle$

Quantum Fourier transform (QFT)

n qubits: 2^n basis state

N = 2^n

$$|\tilde{x}\rangle\text{=QFT}|x\rangle\text{=}\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}}|\text{y}\rangle$$

Quantum Fourier transform (QFT)

Example: 1-qubit case [N = 2^1=2]

$$|\tilde{x}\rangle=\text{QFT}|x\rangle=\frac{1}{\sqrt{2}}\sum_{y=0}^{2-1=1} e^{\frac{2\pi ixy}{N}}|\text{y}\rangle = \frac{1}{\sqrt{2}}\left[e^{\frac{2\pi ix0}{2}}|0\rangle+e^{\frac{2\pi ix1}{2}}|1\rangle\right] = \frac{1}{\sqrt{2}}\left[|0\rangle+e^{i\pi x}|1\rangle\right]$$

When x = 0

$$\text{QFT}|0\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle+e^{i\pi 0}|1\rangle\right] = \frac{1}{\sqrt{2}}[|0\rangle+|1\rangle] = |+\rangle$$

When x = 1

$$\text{QFT}|1\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle+e^{i\pi 1}|1\rangle\right] = \frac{1}{\sqrt{2}}[|0\rangle-|1\rangle] = |-\rangle$$

What’s happen when we have to work with multiple qubits?

Quantum Fourier transform (QFT)

What kind of notation do we should use for multiple qubits?
Decimal or binary?

$|\mathrm{y}\rangle = |4\rangle$ $\quad\quad$ $|\mathrm{y}\rangle = |100\rangle$

$|\mathrm{y}\rangle = |y_1 y_2 y_3\rangle$

$|\mathrm{y}\rangle = |100\rangle = |2^2.1 + 2^1.0 + 2^0.0\rangle = |4\rangle$

Quantum Fourier transform (QFT)

So, let’s we write the following:

$$y = \sum_{k=1}^{n} y_k \, 2^{n-k}$$

Then, we write a new expretion for QFT:

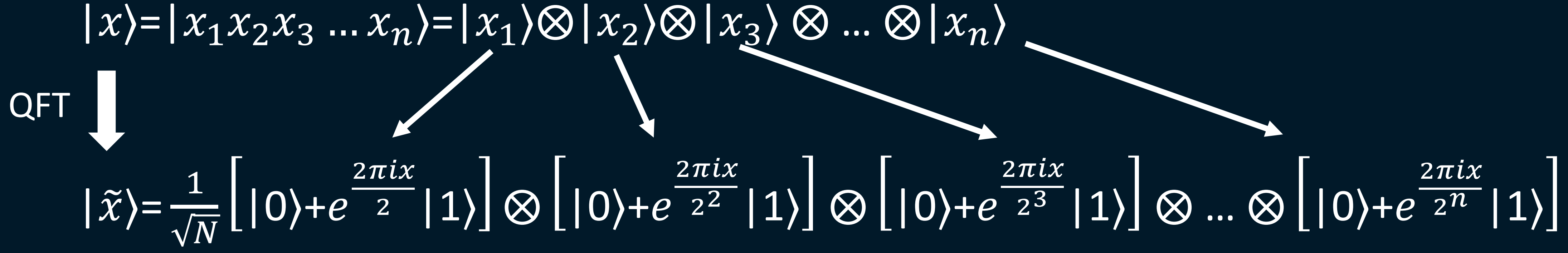
$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{k=1}^{n} y_k 2^{-k}} |y_1 y_2 y_3 \ldots y_n\rangle$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y_k}{2^k}} |y_1 y_2 y_3 \ldots y_n\rangle$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \left[|0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle\right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle\right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^3}} |1\rangle\right] \otimes \ldots \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle\right]$$

Quantum Fourier transform (QFT)

In summary, what we have done is take $|x\rangle$, apply to it a QFT and as result we have a new form.



$$|x\rangle=|x_1x_2x_3 \ldots x_n\rangle=|x_1\rangle\otimes|x_2\rangle\otimes|x_3\rangle \otimes \ldots \otimes|x_n\rangle$$

$$|\tilde{x}\rangle=\frac{1}{\sqrt{N}}\left[|0\rangle+e^{\frac{2\pi i x}{2}}|1\rangle\right]\otimes\left[|0\rangle+e^{\frac{2\pi i x}{2^2}}|1\rangle\right]\otimes\left[|0\rangle+e^{\frac{2\pi i x}{2^3}}|1\rangle\right]\otimes \ldots \otimes\left[|0\rangle+e^{\frac{2\pi i x}{2^n}}|1\rangle\right]$$

Notice that each qubit went from $|x_k\rangle$ to $\left[|0\rangle+e^{\frac{2\pi i x}{2^k}}|1\rangle\right]$

Now we can see something very clearly. The main difference between each term of the QFT is the phases.

Quantum Fourier transform (QFT)

If we have $|\tilde{x}\rangle$=$|\tilde{0}\rangle$ (which really is QFT of $|000\rangle$), we do not have any phases contribution.

Otherwise, if I have $|\tilde{x}\rangle$=$|\tilde{7}\rangle$ (which really is QFT of $|111\rangle$), we will.

Therefore, it give us two hints of form of QFT circuit:

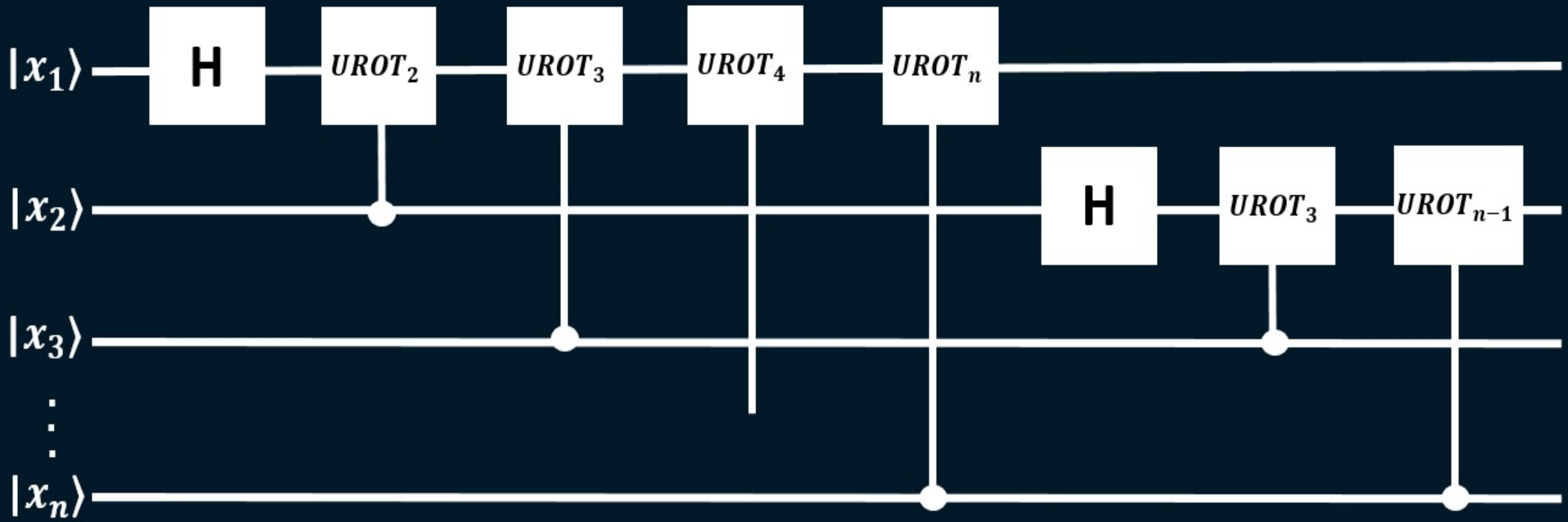
1. Phase is qubit-dependent
2. Need to add up more component with more “1”s

For achieve that we read before we will use the U Rotation gate!

$$UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \longrightarrow UROT_k|x_j\rangle = e^{\frac{2\pi i}{2^k}}|x_j\rangle$$

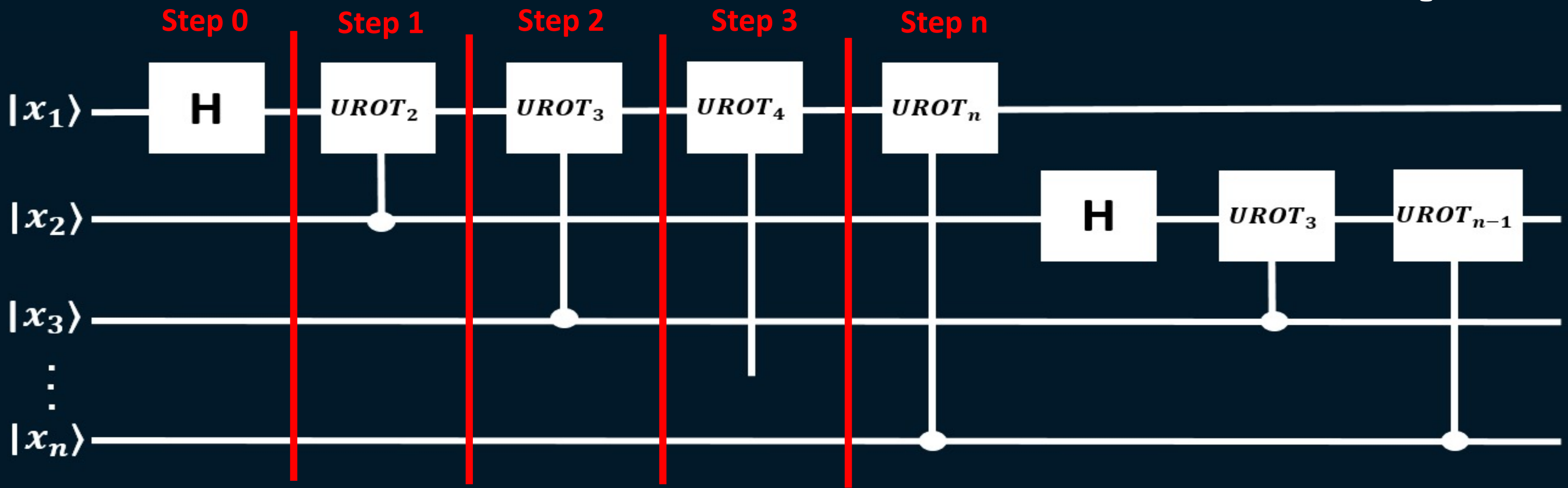
Quantum Fourier transform (QFT)

The quantum circuit that implements QFT looks like:



This circuit reverses order of qubits at output, so we need to put SWAP gates in the end!

Quantum Fourier transform (QFT)



Step 0: $|x_1 x_2 x_3 \ldots x_n\rangle$

Step 1: $\left[|0\rangle + e^{\frac{2\pi i x_1}{2}} |1\rangle\right] \otimes |x_1 x_2 x_3 \ldots x_n\rangle$

Step 2: $\left[|0\rangle + e^{\frac{2\pi i x_2}{2^2}} e^{\frac{2\pi i x_1}{2}} |1\rangle\right] \otimes |x_1 x_2 x_3 \ldots x_n\rangle$

Step 3: $\left[|0\rangle + e^{\frac{2\pi i x_3}{2^3}} e^{\frac{2\pi i x_2}{2^2}} e^{\frac{2\pi i x_1}{2}} |1\rangle\right] \otimes |x_1 x_2 x_3 \ldots x_n\rangle$

Step n: $\left[|0\rangle + e^{\frac{2\pi i x_n}{2^n}} e^{\frac{2\pi i x_{n-1}}{2^{n-1}}} \ldots e^{\frac{2\pi i x_1}{2}} |1\rangle\right] \otimes |x_1 x_2 x_3 \ldots x_n\rangle$

Quantum Phase Estimation (QPE)

Here, we will use QFT to do something useful.

Remember that a unitary matrix has eigenvalues of the form $e^{i\theta}$ and that if has eigenvectors that form an orthonormal basis

$$\mathrm{U}|\boldsymbol{\psi}\rangle = e^{i\theta_\psi}|\boldsymbol{\psi}\rangle$$

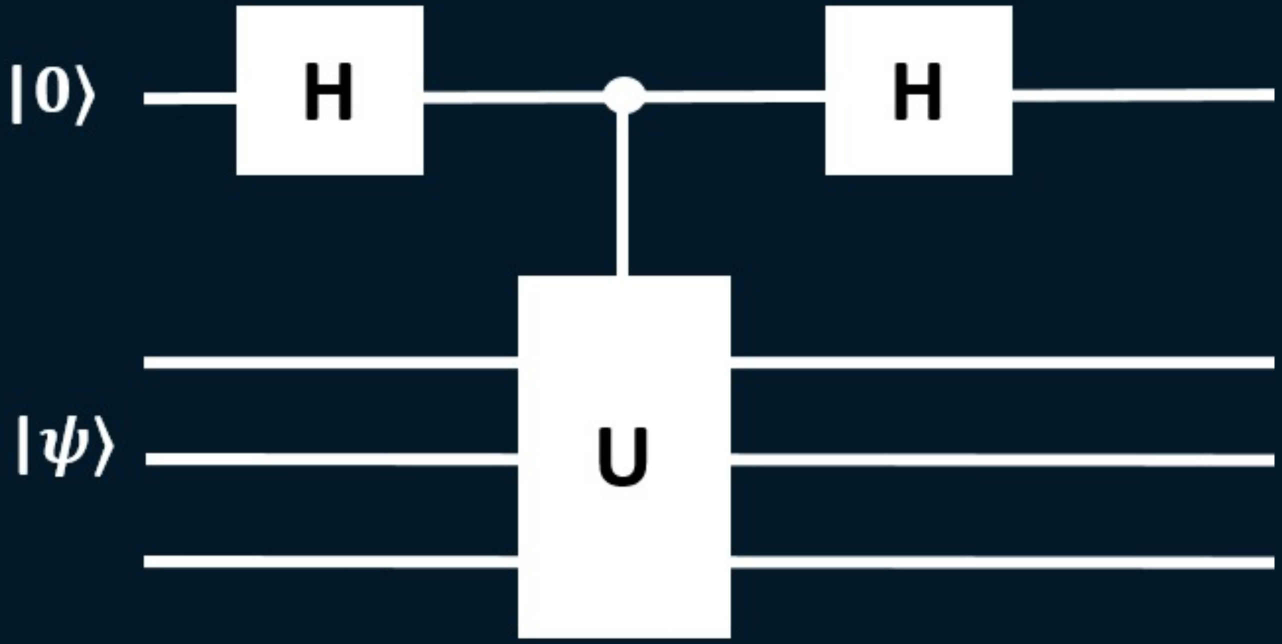
can we extract given θ_ψ the ability to prepare $|\boldsymbol{\psi}\rangle$ and the ability to apply U?

Answer: Yes, use QPE.

Why do we care? This has implications for quantum simulation.

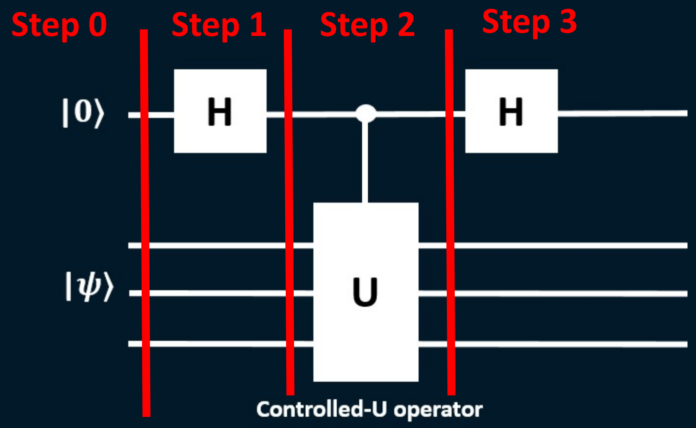
Quantum Phase Estimation (QPE)

The circuit that we show now it help us to see how QPE works.



Controlled-U operator

Quantum Phase Estimation (QPE)



Step 0: $|0\rangle|\psi\rangle$

Step 1: $\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle|\psi\rangle+|1\rangle|\psi\rangle]$

Step 2: $\frac{1}{\sqrt{2}}[|0\rangle|\psi\rangle+|1\rangle e^{i\theta_\psi}|\psi\rangle]$

Step 3: $\frac{1}{\sqrt{2}}\left[\frac{[|0\rangle+|1\rangle]}{\sqrt{2}}|\psi\rangle + e^{i\theta_\psi}\frac{[|0\rangle-|1\rangle]}{\sqrt{2}}|\psi\rangle\right] = \frac{1}{2}[|0\rangle(1+e^{i\theta_\psi}) + |1\rangle(1-e^{i\theta_\psi})]|\psi\rangle$

What is the probability of measuring zero and one?

Prob. measuring $|0\rangle = \left|\frac{1}{2}(1+e^{i\theta_\psi})\right|^2$

Prob. measuring $|1\rangle = \left|\frac{1}{2}(1-e^{i\theta_\psi})\right|^2$

Quantum Phase Estimation (QPE)

$\theta_\psi = 1°$ prob(0) , prob(1) = { 0,9999 , 7.6x10^{-5}}

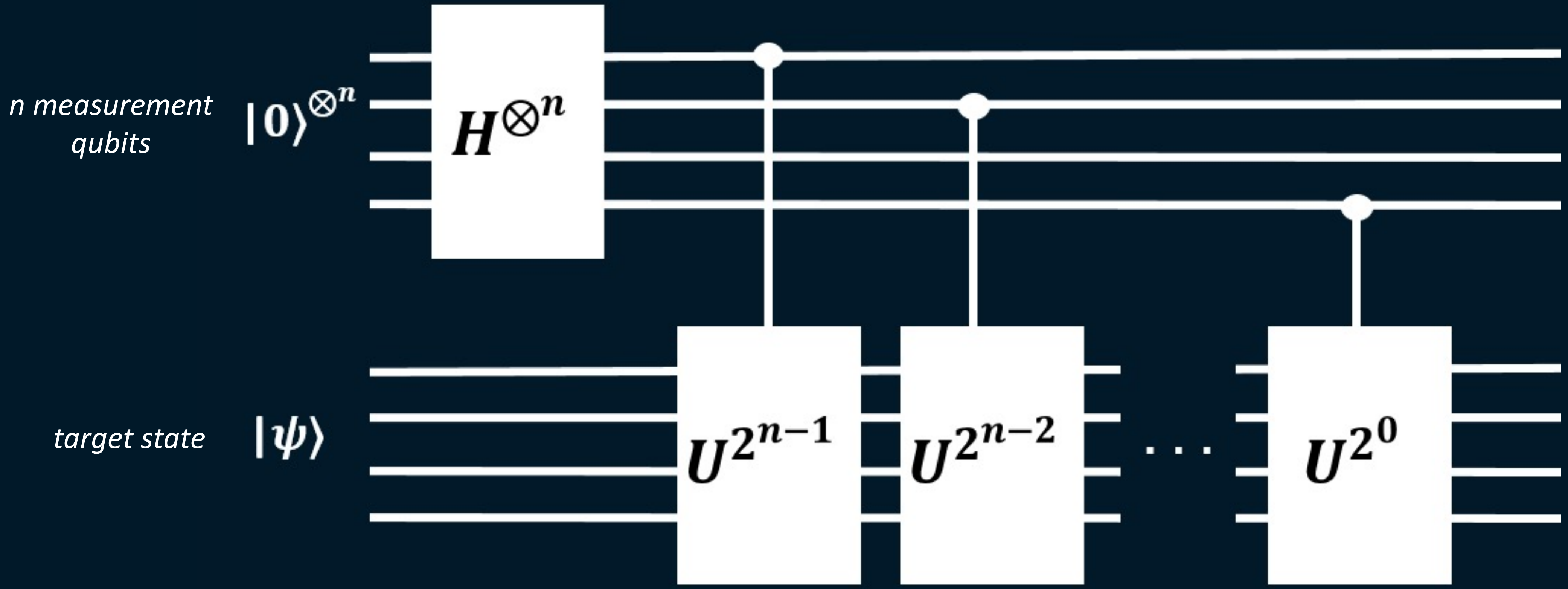
$\theta_\psi = 10°$ prob(0) , prob(1) = { 0,9924 , 0.007596}

This experiment uses 1 qubit to measure θ_ψ but, what happen if we use more qubits?

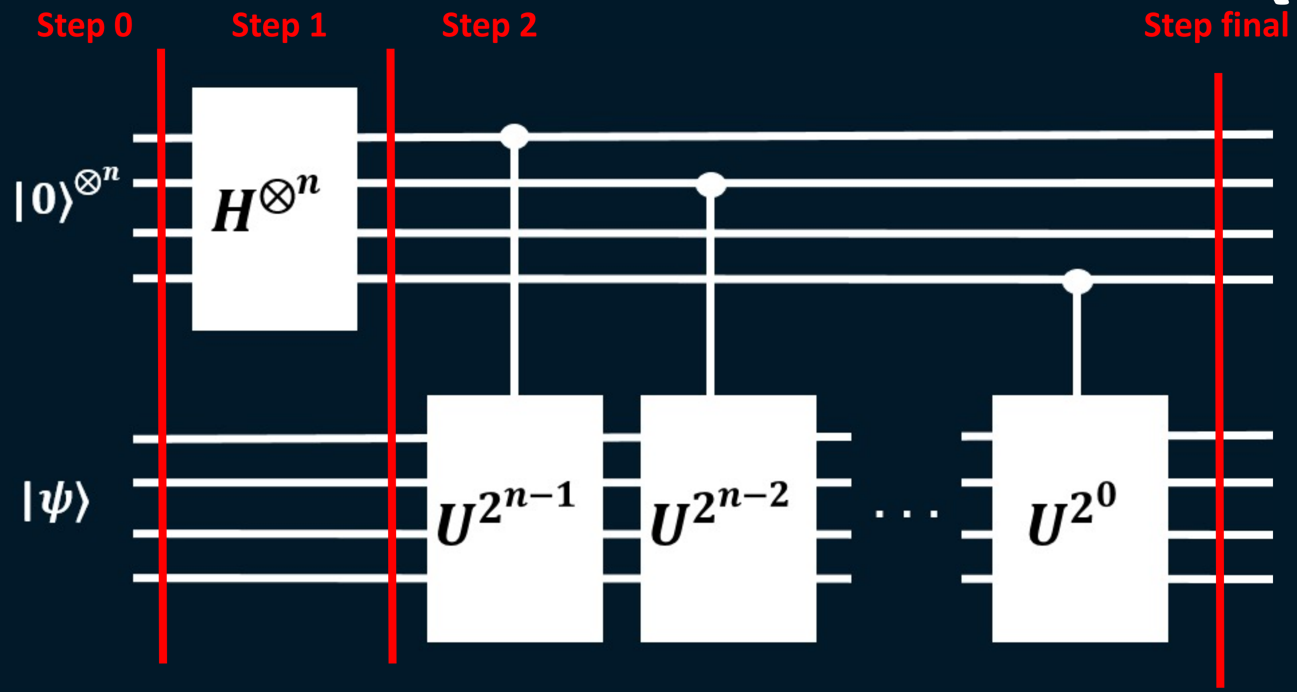
So the picture turns form the previous one where we have used only one qubit to a different one which is going to be several qubits.

Quantum Phase Estimation (QPE)

Notice how we have now extended the picture to have n measurement qubits in the top and a targe state in the bottom.



Quantum Phase Estimation (QPE)



Step 0: $|0\rangle^{\otimes n}|\psi\rangle$

Step 1: $[\frac{1}{\sqrt{2}}]^n\ [|0\rangle+|1\rangle]^{\otimes n}|\psi\rangle$

Step 2: $U^{2^x}|\psi\rangle = U^{2^x-1}U|\psi\rangle = U^{2^x-1}e^{i\theta_\psi}|\psi\rangle = U^{2^x-2}e^{i\theta_\psi}e^{i\theta_\psi}|\psi\rangle$

Step final: $[\frac{1}{\sqrt{2}}]^n\left[|0\rangle+e^{i\theta_\psi 2^{x-1}}|1\rangle\right]\otimes\left[|0\rangle+e^{i\theta_\psi 2^{x-2}}|1\rangle\right]\otimes\ldots\otimes\left[|0\rangle+e^{i\theta_\psi 2^{0}}|1\rangle\right]|\psi\rangle$ ➡ **To what do we remind us this form?**

Quantum Fourier Transform (QFT) vs Quantum Phase Estimation (QPE)

QFT ➡ $\frac{1}{\sqrt{N}}\left[|0\rangle+e^{\frac{2\pi i x}{2}}|1\rangle\right]\otimes\left[|0\rangle+e^{\frac{2\pi i x}{2^2}}|1\rangle\right]\otimes \ldots \otimes\left[|0\rangle+e^{\frac{2\pi i x}{2^n}}|1\rangle\right]$

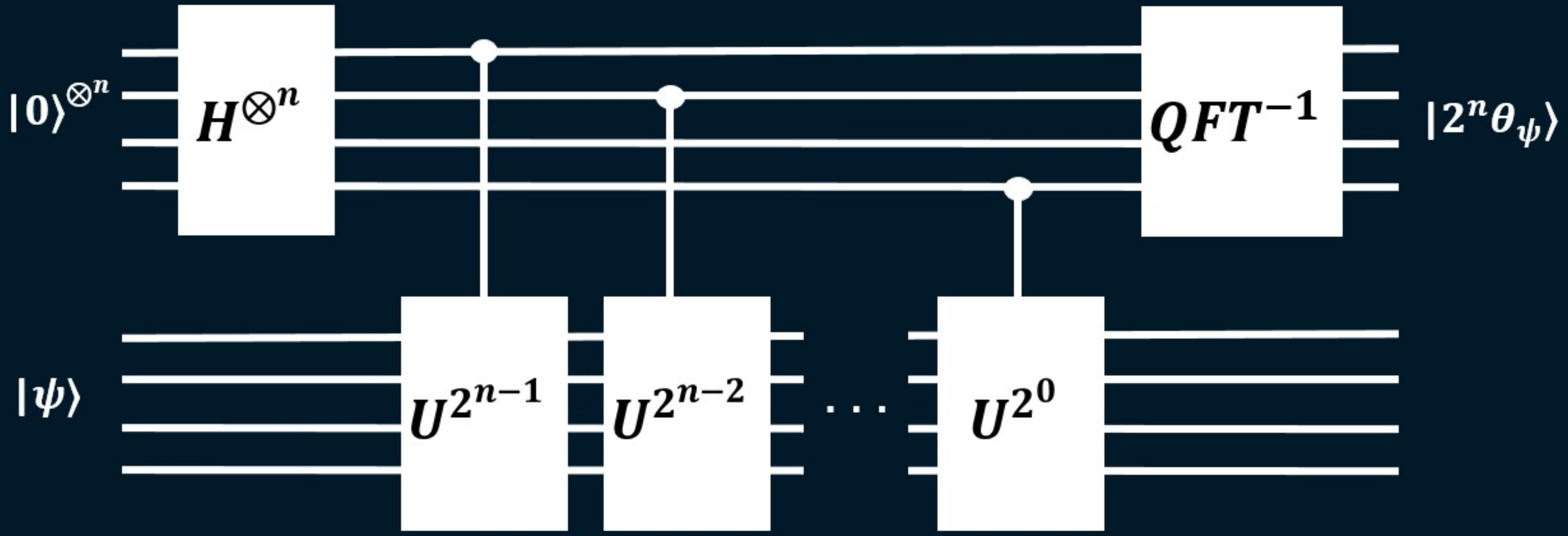
QPE ➡ $\frac{1}{\sqrt{N}}\left[|0\rangle+e^{i\theta_\psi 2^{x-1}}|1\rangle\right]\otimes\left[|0\rangle+e^{i\theta_\psi 2^{x-2}}|1\rangle\right]\otimes \ldots \otimes\left[|0\rangle+e^{i\theta_\psi 2^{0}}|1\rangle\right]|\psi\rangle$

QPE is the same as QFT except we have θ_ψ instead of 2π $\frac{\theta_\psi}{2^x}$

Therefore, we can conclude QPE is exactly like QTF with a different phase.

It seems like at output of circuite we have the QFT of something, so if we apply a box called QFT inverts, we will be able to measure the final state.

Quantum Phase Estimation (QPE)



At the beginnig of QPE, with 1 qubits as input we did not have enough precision to do our measurement. Notices how in this particular case where we have multiple qubits as input we have multiplied the phase $\boldsymbol{\theta_\psi}$ by $\boldsymbol{2^n}$, it allows to have more precision in the end.

Quantum Phase Estimation (QPE)

With 1 qubit we have the measuremt below:

$\theta_{\psi} = 1°$ prob(0) , prob(1) = { 0,9999 , 7.6x10^{-5}}

$\theta_{\psi} = 10°$ prob(0) , prob(1) = { 0,9924 , 0.007596}

With multiple qubits (eg 10 qubits) now we have the measuremt below:

$\theta_{\psi} = 1°$ prob(0) , prob(1) = { 1023.89 , 0.07782}

$\theta_{\psi} = 10°$ prob(0) , prob(1) = { 1016.21 , 7.7783}

The question to answer here is: which case is more easier to tell us the difference between these two numbers?

With multiple qubits! Especially if we have a signal to noise limitations.

Shor’s algorithm

Problem to solve: factoring a number N which factors are *q* and *p*, where each of them are primes and larges.

This problems could solve by a classical computer but it would take a very long time, while with quantum computers it could be litter faster.

If we pretend to understand Shor’s algorithm, first we need to now how QFT and QPE works.

In fact, shor’s algorithm is really just QPE in disguise.

Shor’s algorithm

Quick primer on modular arithmetic

If we compute the following $\boldsymbol{\frac{5}{3}}$

We have 1 as quotient and 2 as remainder, so
5 is equivalent to two modular 3.

$$\boldsymbol{5 \ \equiv 2\ (mod\ 3)}$$

So let’s say x is the following number, if I said module
three, what is X equivalent to?

X =	1	2	3	4	5	6	7	8	9	(mod 3)
X ≡	1	2	0	1	2	0	1	2	0	

We can notice the periodicity of modular arithmetic.

Shor’s algorithm

Now that we have seen modular arithmetic, the question becames, how do we factor two numbers out of big number that we are given?

Protocol for Shor’s algorithm

Where N is a number
and N = qp

1. Pick a number “a” that is coprime with N.
2. Find the “order” r of the function a^r (mod N). The order is simply the period of this function.
3. If r is even, then we create a new variable which is x $\equiv a^{\frac{r}{2}}$ (mod N). If not, go to step 1.
4. If x+1$\not\equiv$0 (mod N), it means we have a situation where the factor p and q are. If not, go to step 1.
5. Do the greatest common divisor (gcd) of (x+1) and N, and (x-1) and N. Then, we will have q and p factors. Finally, the problem have been result!

Shor’s algorithm

Concrete example: factor 15

15 = [1111] (four bits)

1. Pick a number that is coprime with 15. We pick a = 13

2. Find the period of $13^{r}(mod\ 15)$

X =	0	1	2	3	4	5	6	7	(mod 15)
X ≡	1	13	4	7	1	13	4	7	

$\boldsymbol{13^{r} \equiv 1\ (mod\ 15)}$ **= 4**

$\boldsymbol{r}$ **= 4**

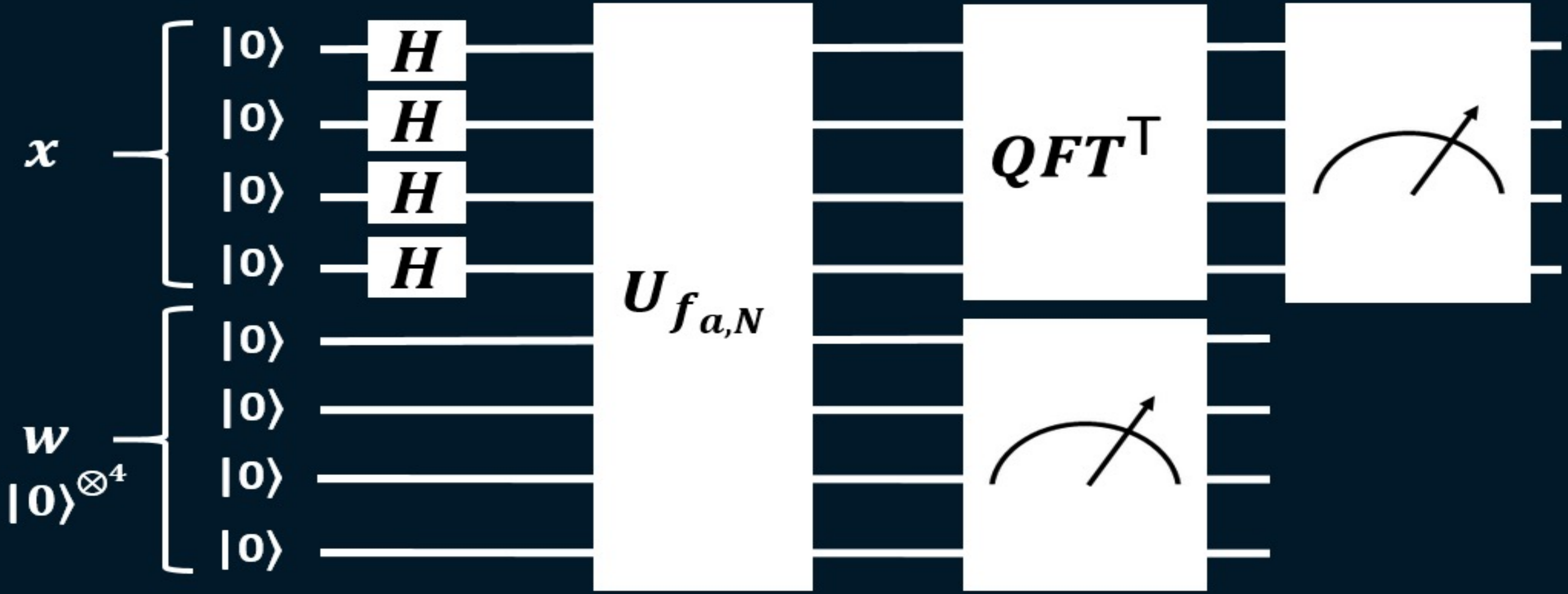
3. $x = a^{\frac{r}{2}}(mod\ 15) = 13^{r}(mod\ 15) = 4\ (mod\ 15)$

4. $x + 1 = 4 + 1 = 5 \equiv \mathbf{5}\ (mod\ 15)$

5. gcd (x+1,N) = gdc(5,15)= 5 = p
gcd (x-1,N) = gdc(3,15)= 3 =q

Shor’s algorithm

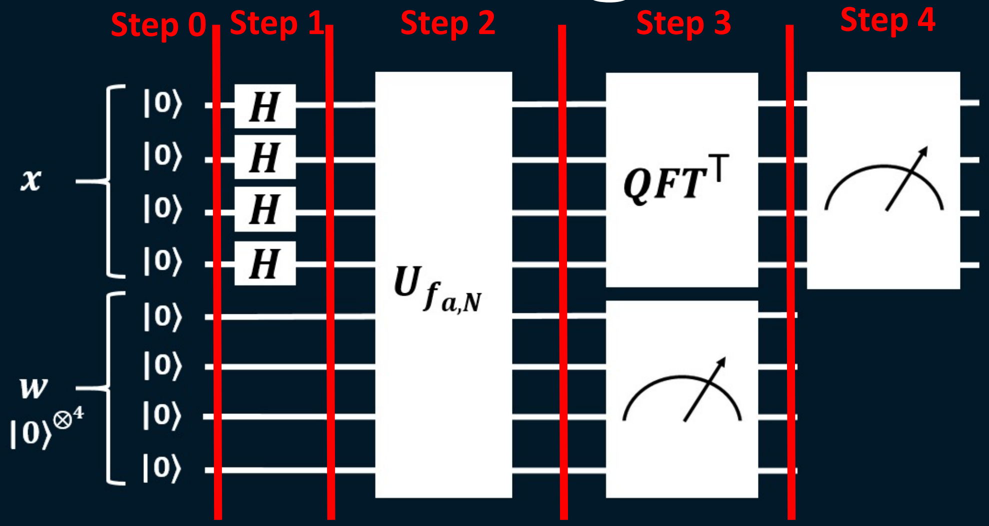
Quantum circuit for factoring N=qp, N=15



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

$$|x\rangle|w\rangle \longrightarrow |x\rangle|w \oplus f_{a,N}(x)\rangle$$

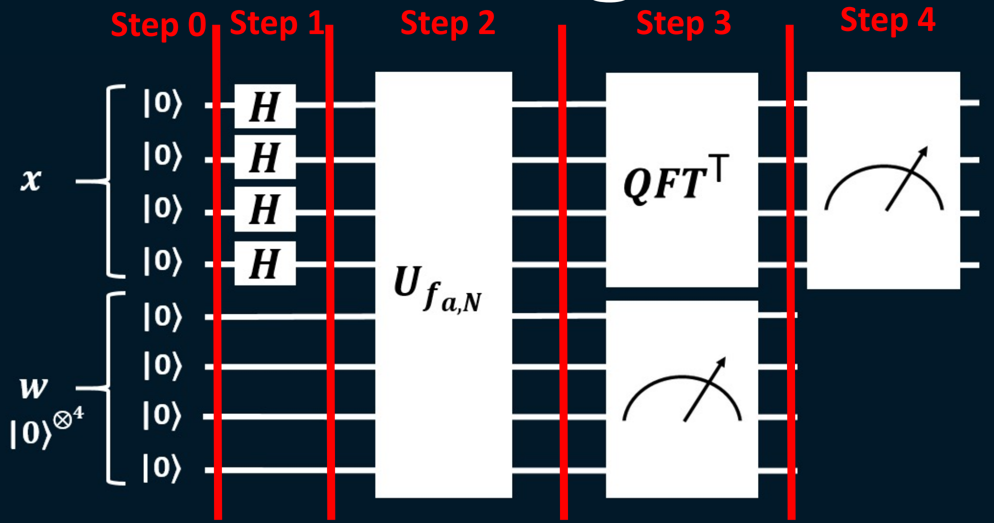
Shor's algorithm



Step 0: $\underset{x}{|0\rangle^{\otimes 4}}\,\underset{w}{|0\rangle^{\otimes 4}}$

Step 1: $[H^{\otimes 4}|0\rangle]|0\rangle^{\otimes 4} = \frac{1}{4}[|0\rangle_4 + |1\rangle_4 + |2\rangle_4 + \cdots + |15\rangle_4]|0\rangle^{\otimes 4}$

Shor’s algorithm



$$|xw\rangle \longrightarrow |x\rangle|w \oplus f_{a,N}(x)\rangle$$

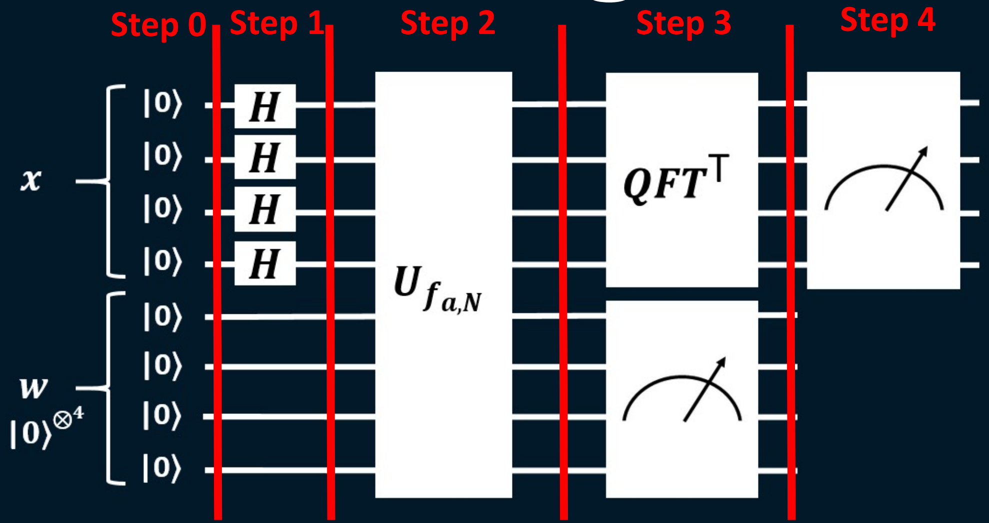
Step 2: $\frac{1}{4}[|0\rangle_4|0 \oplus 13^0(mod\ 15)\rangle_4 + |1\rangle_4|0 \oplus 13^1(mod\ 15)\rangle_4 + \cdots + |15\rangle_4|0 \oplus 13^{15}(mod\ 15)\rangle_4]$

$$\boxed{\begin{array}{l} \oplus = addition\ modular\ 2, XOR \\ 0 \oplus z = z \end{array}}$$

$$= \frac{1}{4}[|0\rangle_4|13^0(mod\ 15)\rangle_4 + |1\rangle_4|13^1(mod\ 15)\rangle_4 + \cdots + |15\rangle_4|0 \oplus 13^{15}(mod\ 15)\rangle_4]$$

$$\begin{aligned} = \frac{1}{4}[&|0\rangle_4|1\rangle_4 + |1\rangle_4|13\rangle_4 + |2\rangle_4|4\rangle_4 + |3\rangle_4|7\rangle_4 \\ &+ |4\rangle_4|1\rangle_4 + |5\rangle_4|13\rangle_4 + |6\rangle_4|4\rangle_4 + |7\rangle_4|7\rangle_4 \\ &+ |8\rangle_4|1\rangle_4 + |9\rangle_4|13\rangle_4 + |10\rangle_4|4\rangle_4 + |11\rangle_4|7\rangle_4 \\ &+ |12\rangle_4|1\rangle_4 + |13\rangle_4|13\rangle_4 + |14\rangle_4|4\rangle_4 + |15\rangle_4|7\rangle_4] \end{aligned}$$

Shor's algorithm



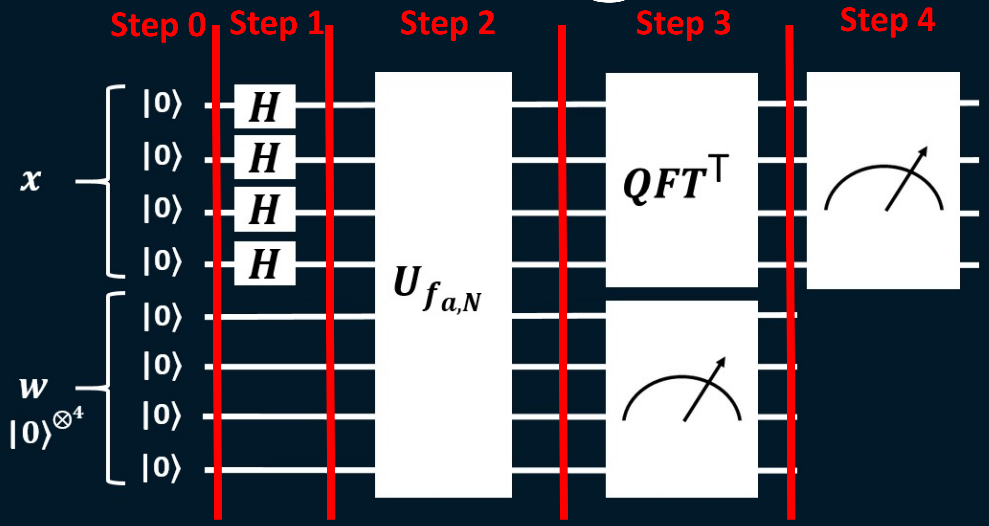
$$\frac{1}{4}[|0\rangle_4|1\rangle_4 + |1\rangle_4|13\rangle_4 + |2\rangle_4|4\rangle_4 + |3\rangle_4|7\rangle_4$$
$$+ |4\rangle_4|1\rangle_4 + |5\rangle_4|13\rangle_4 + |6\rangle_4|4\rangle_4 + |7\rangle_4|7\rangle_4$$
$$+ |8\rangle_4|1\rangle_4 + |9\rangle_4|13\rangle_4 + |10\rangle_4|4\rangle_4 + |11\rangle_4|7\rangle_4$$
$$+ |12\rangle_4|1\rangle_4 + |13\rangle_4|13\rangle_4 + |14\rangle_4|4\rangle_4 + |15\rangle_4|7\rangle_4]$$

Step 3: Measure the $\boldsymbol{w}$ register, let's say we measure "7"

after $|w\rangle$=$|7\rangle_4$, $|x\rangle$ becames

$$|x\rangle|w\rangle = \frac{1}{2}[|3\rangle_4 + |7\rangle_4 + |11\rangle_4 + |15\rangle_4] \otimes |7\rangle_4$$

Shor’s algorithm



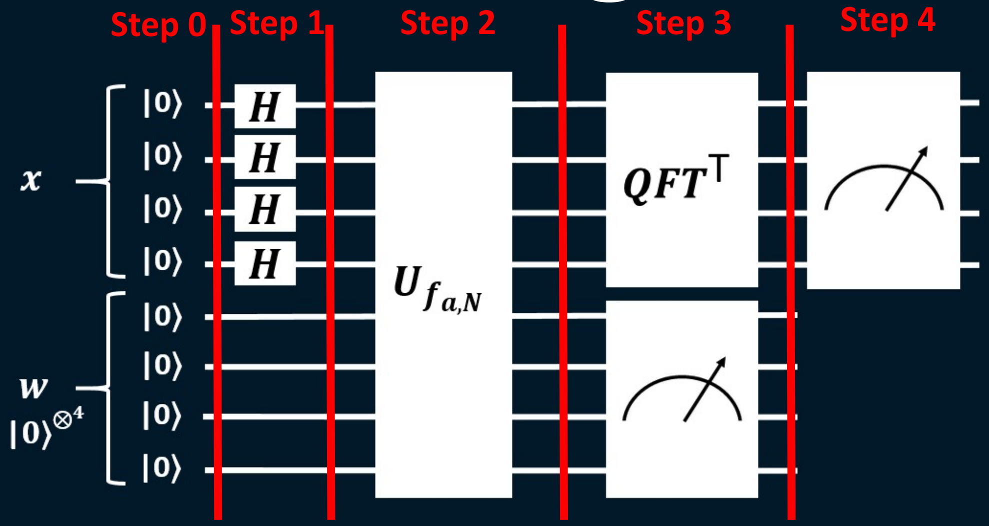
Step 3: Apply QFT^T on the $|\boldsymbol{x}\rangle$ register

Recall:

$$\text{QFT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |\text{y}\rangle$$ Quantum Fourier Transform

$$\text{QFT}^T|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{-2\pi i x y}{N}} |\text{y}\rangle$$ Quantum Fourier Transform dagger

Shor's algorithm



Step 3: Apply QFT^{T} on the $|x\rangle$ register

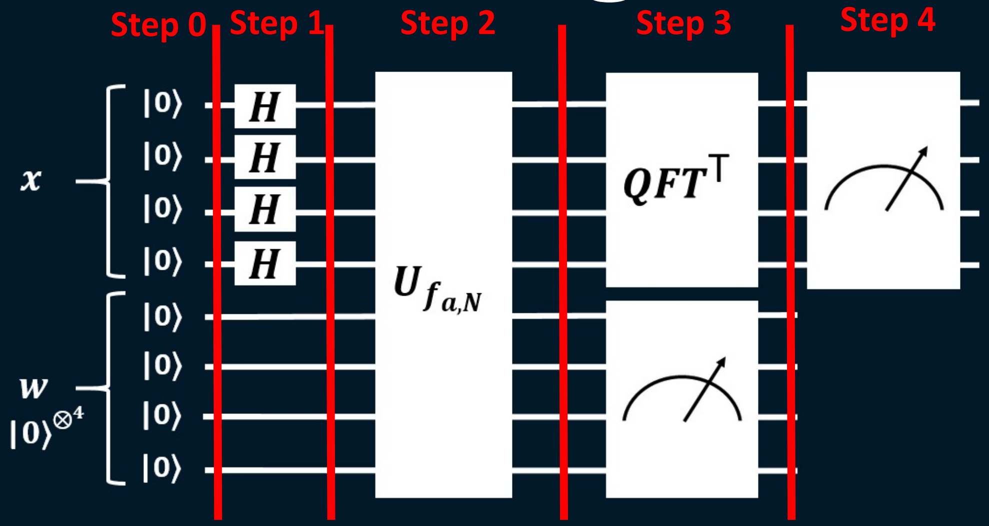
$$\mathrm{QFT}^{T}|3\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2\pi i 3y}{16}} |\mathrm{y}\rangle$$

$$\mathrm{QFT}^{T}|7\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2\pi i 7y}{16}} |\mathrm{y}\rangle$$

$$\mathrm{QFT}^{T}|11\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2\pi i 11y}{16}} |\mathrm{y}\rangle$$

$$\mathrm{QFT}^{T}|15\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2\pi i 15y}{16}} |\mathrm{y}\rangle$$

Shor's algorithm



Step 3: Apply QFT^T on the $|x\rangle$ register

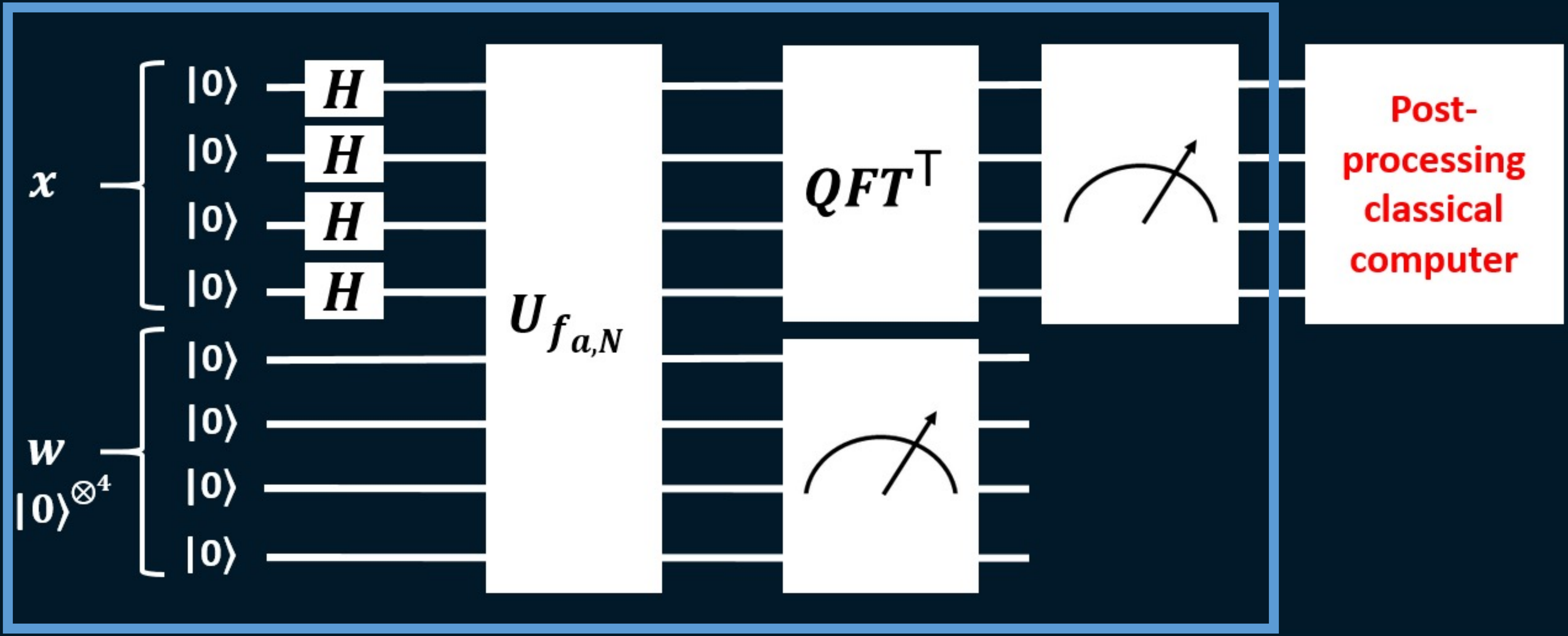
$$\mathrm{QFT}^T|x\rangle=\frac{1}{\sqrt{16}}\sum_{y=0}^{15}(e^{\frac{-2\pi i3y}{16}}+e^{\frac{-2\pi i7y}{16}}+e^{\frac{-2\pi i11y}{16}}+e^{\frac{-2\pi i15y}{16}})|\mathrm{y}\rangle$$

Step 4: Measure $|x\rangle$ register. We can get 0, 4, 8 and 12 at output with equal probability.

At this point, we have done the quantum part of Shor's algorithm!

Remaining steps on classical post-processig.

Shor's algorithm



Quantum computer part

Shor’s algorithm

Next steps on classical computer. We are going to analize what happen for each outcome.

It is important to note that the measurement results peak for Shor’s algorithm near j$\frac{N}{r}$ for some integer j.

For example, if we measuer $|\mathbf{4}\rangle_4$, then j$\frac{16}{r} = 4$ and this is only true if j=1 and r=4.

So, is r even? Yes.

Therefore

$$x \equiv a^{\frac{r}{2}} \text{ (mod N) } = 13^{\frac{4}{2}} \,(mod\ 15) = 4$$

We do the following greatest common divisor:

gcd (x+1,N) = gdc(5,15) = **5** = p

gcd (x-1,N) = gdc(3,15) = **3** = q

→ **Finally! We get the solution for the problem!**