Lecture 4:

Shor's Algorithm II: Factoring to period-finding and using QPE (and QFT) for factoring.

Quick Review

Yesterday, covered QFT and QPE

① QFT - basis change from the computation basis to Fourier basis.

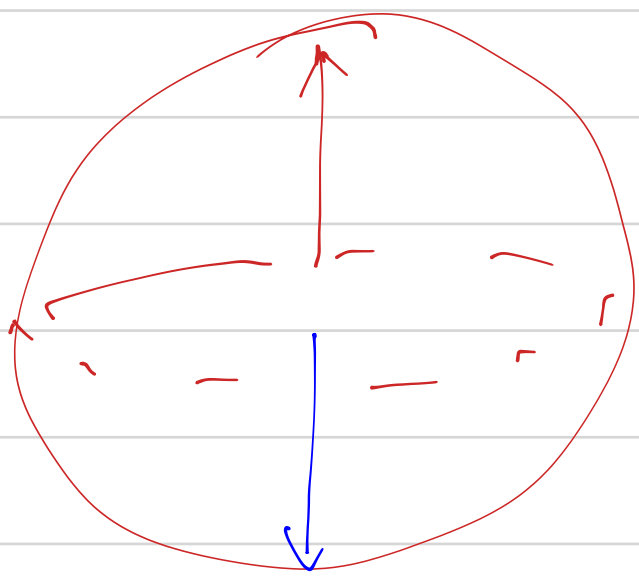
- One-qubit QFT is the H-gate

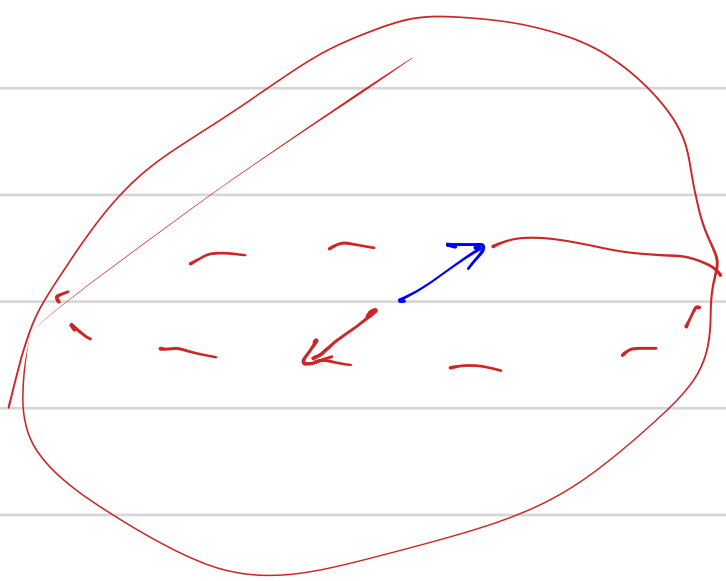
Computational basis

Fourier basis

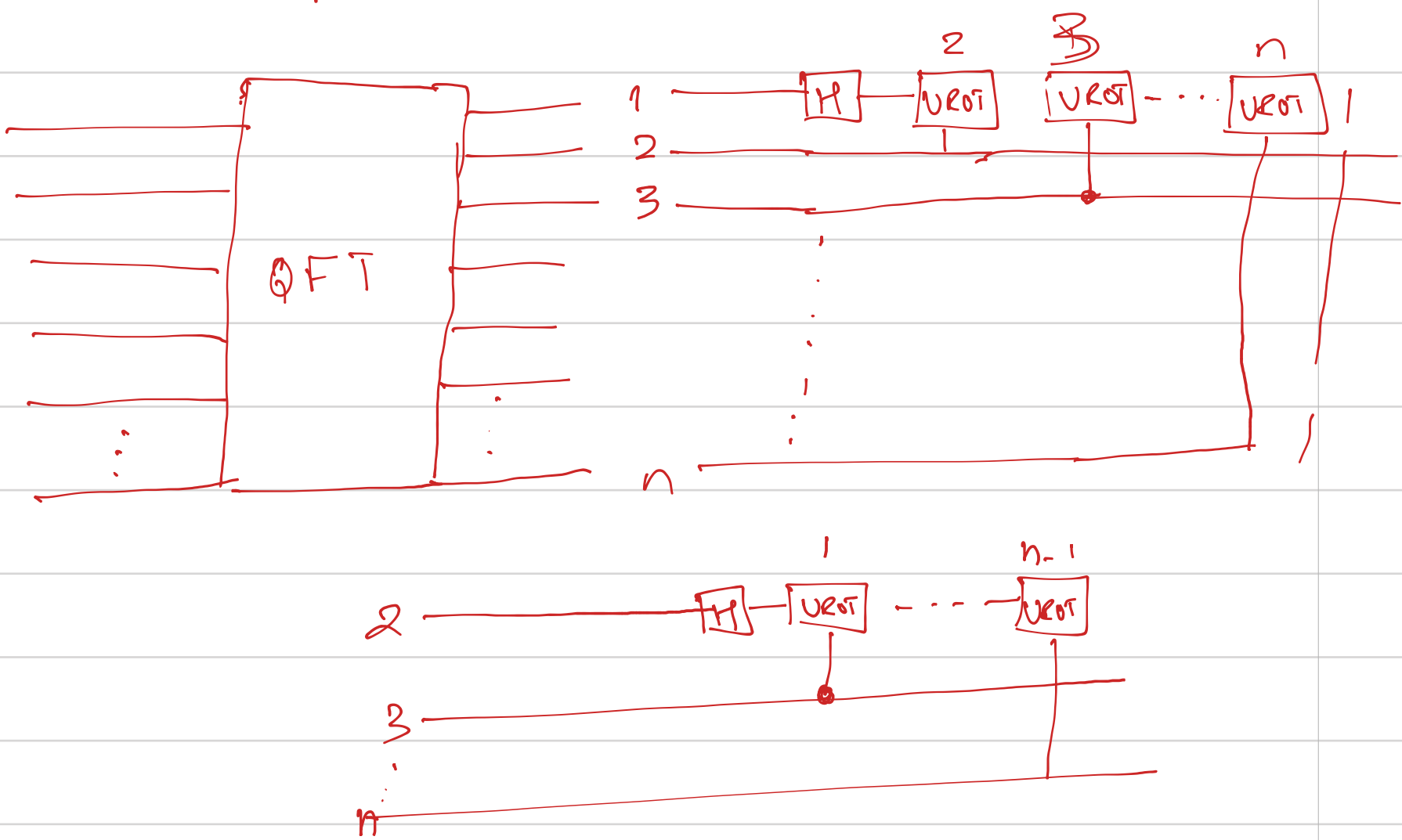
Single Qubit $|0\rangle$ — QFT → $|+\rangle$

Case $|1\rangle$ — QFT → $|-\rangle$





- circuit implementation



$$UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\left(\frac{2\pi i}{2^k}\right)} \end{bmatrix}$$

Controlled U-ROT Gate

$$CROT_k |1\rangle |x_j\rangle = e^{\frac{2\pi i}{2^k}}$$

control ↙ ↓ target

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

$$H|x_j\rangle = \frac{|0\rangle + e^{\frac{2\pi i x_j}{2}} |1\rangle}{\sqrt{2}}$$

nqubits

$$QFT_{N=2^n}|x\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right)$$

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

$$\vdots$$

$$|x\rangle = |x_1 x_2 \cdots x_n\rangle \qquad \left(|0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle\right) \equiv |\tilde{x}\rangle$$

$x = [x_1 x_2 \cdots x_n]$ converting b-n binary & decimal

$2^{n-1}x_1 + 2^{n-2}x_2 + \cdots 2^0 x_n$

case $n=5$ qubits, $x=3$

$$|0\rangle + \underbrace{e^{\frac{2\pi i 3}{2^2}}|1\rangle}$$

$$\frac{3}{2^2} = \frac{2^1+1}{2^2} = \frac{1}{2} + \frac{1}{2^2}$$

$$e^{2\pi i \frac{3}{2^2}} = e^{2\pi i\left[\frac{1}{2} + \frac{1}{2^2}\right]}$$

$n = 8$ qubits, $x = 5$

$$|0\rangle + \underbrace{e^{\frac{2\pi i 5}{2^2}}|1\rangle}$$

$$\frac{5}{2^2} = \frac{2^2+1}{2^2} = 1 + \frac{1}{2^2}$$

$$= e^{2\pi i\left[1 + \frac{1}{2^2}\right]} \quad \hookrightarrow e^{2\pi i z} = 1$$

$$= e^{2\pi i\left[1/2^2\right]}$$

(2) Quantum Phase Estimation

Objective: given a unitary U and its eigenstate/vector $|\psi\rangle$

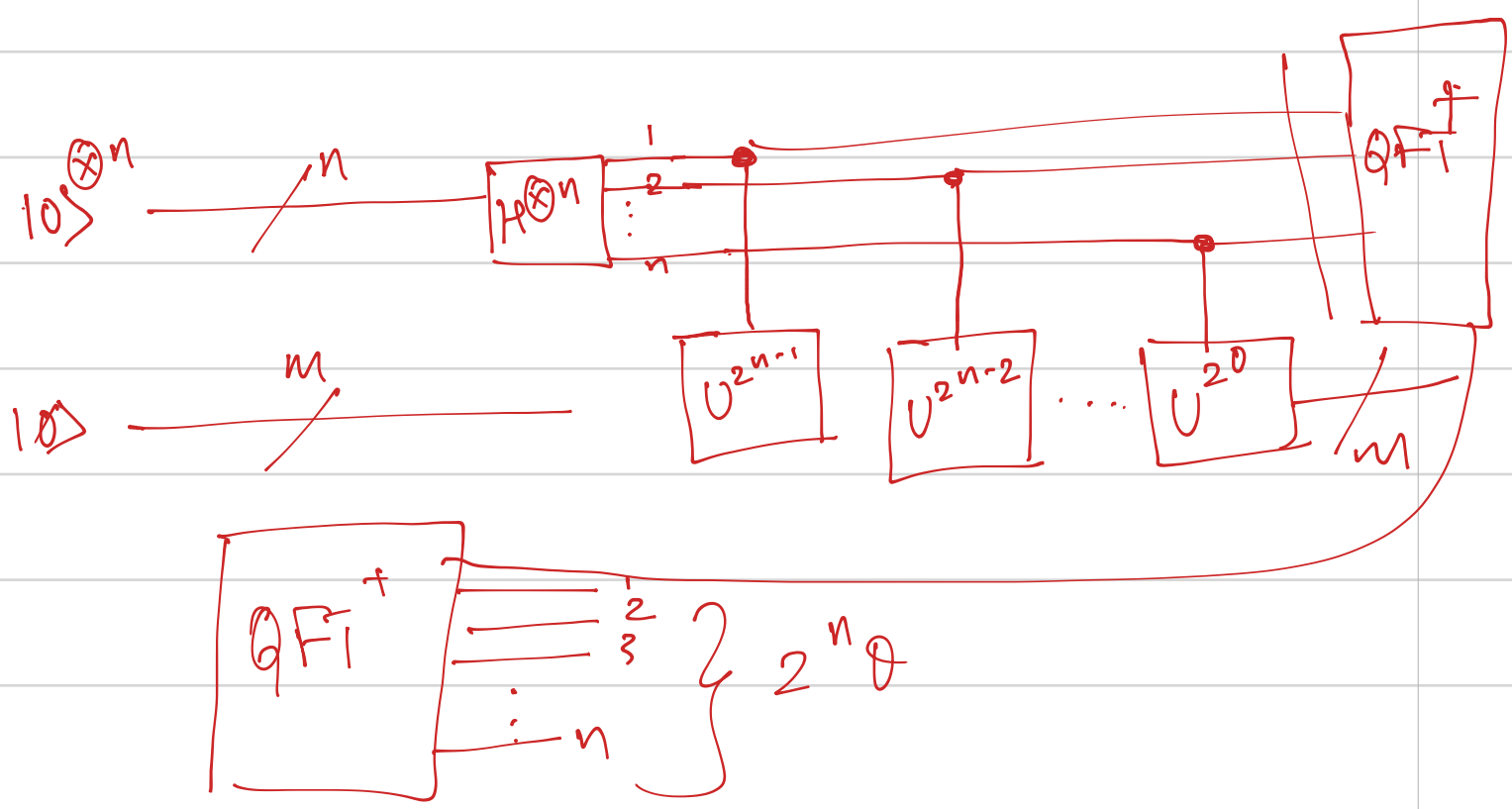
$$U|\psi\rangle = e^{i\theta_\psi}|\psi\rangle$$

- can we find θ_ψ?

- Assume that we can prepare $|\psi\rangle$
- Phase estimation allows us to convert phase information into amplitudes that we can measure

QPE protocol

given $U|\phi\rangle = e^{2\pi i\theta}|\phi\rangle$, QPE gives us $2^n\theta$, where n is the number of qubits used to estimate θ.



Subtleties:

(1) notice the $2\pi i * \theta$

(2) Notice that we are doing $QFT^\dagger$, not QFT

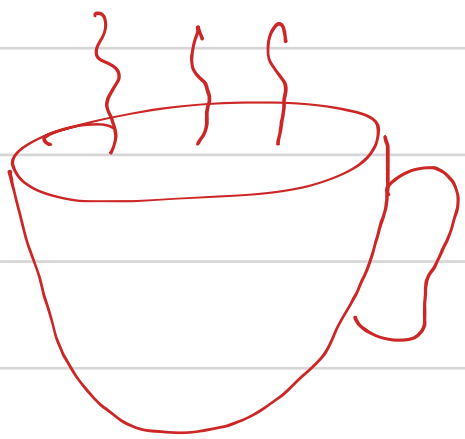
$$(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$$

(3) Yesterday's lab solution: use $U_1(\lambda)$

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix}$$

↑ doesn't have 2π

(4) Quantum counting in Qiskit Textbook



Break!!!

Shor's Algorithm

(1) Problem: factoring a number

$N = p \cdot q$ where p and q are prime and large

n = # bits needed to describe the factors

classically : $O\left(\exp\left[c \cdot n^{1/3} (\log n)^{2/3}\right]\right)$

Shor's Algorithm: little faster than $O(n^3)$

Exp gone!

(2) Quick primer on modular arithmetic

$5/3 \Rightarrow$ quotient = 1

remainder = 2

$5 \equiv 2 \pmod 3$

	x =	1	2	3	4	5	6	7	8	9
(mod 3)	$x \equiv$	1	2	0	1	2	0	1	2	0

Notice: $x \equiv 0 \pmod 3 \Rightarrow x$ is a multiple of 3

$x \equiv 1 \pmod 3 \Rightarrow x$ is a multiple of 3+1

$x \equiv 2 \pmod 3 \Rightarrow x$ is " " " 3+2

Generally: $x \equiv y \pmod 3 \Rightarrow x = 3k + y$ for some $k \in \mathbb{Z}$

Also, notice the periodicity of modular arithmetic

$x \equiv y \pmod N$ means $y \in \{0, \ldots, N-1\}$

$x \equiv y \pmod 3$ means $y \in \{0, 1, 2\}$

Protocol for Shor's Algorithm $\quad N = pq$

(1) Pick a number "a" that is coprime with N

(2) find the "order" r of the function $\underbrace{a^r \pmod N}$

$\equiv$ smallest r such that $a^r \equiv 1 \pmod N$

(3) if r is even: good news

$x \equiv a^{r/2} \pmod N$ $\quad 10, 15$ $\quad 1,2,5,10$ $\quad 1,3,5,15$

if $x + 1 \not\equiv 0 \pmod N$: good news

else: find another "a"

$\{p, q\}$ contained in $\{ \gcd(x+1; N), \gcd(x-1, N) \}$

(3) Concrete example: Factor 15

$15 = [1111]$ four bits

(1) Pick a number that is coprime with 15

$\downarrow$

13

$a = 13$

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

$x = 0, 1, 2, 3, 4, 5, 6, 7, \ldots,$

$\downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow$

$13^x \pmod{15} = 1, 13, 4, 7, 1, 13, 4, 7$

r = smallest number s.t $a^r \equiv 1 \pmod{N} = 4$

$r = 4$

3) $x = a^{r/2} \pmod{N} = 13^{4/2} \pmod{15} = 4 \pmod{15}$

$x + 1 = 4 + 1 = 5 \equiv \pmod{15}$

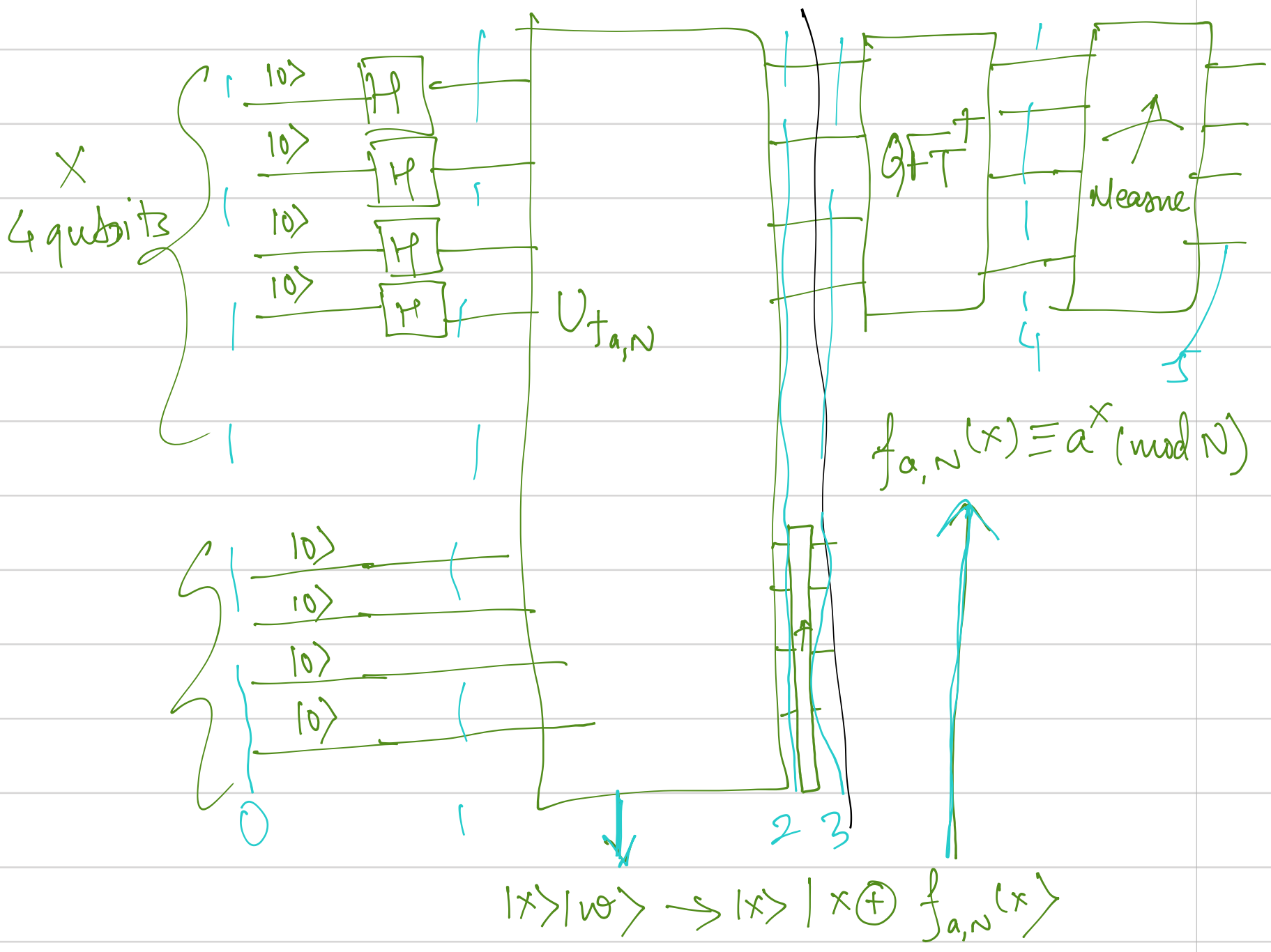
$\gcd(x+1, N) = \gcd(5, 15) = 5$

$\gcd(x-1, N) = \gcd(3, 15) = 3$

$\{p, q\} = \{5, 3\}$

(4) Quantum circuit for factoring $N = pq$, $N = 15$

$15 = [1111]$



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

$x \quad w$

Step 1: $[H^{\otimes 4}|0\rangle]\,|0\rangle^{\otimes 4}$

$= \frac{1}{4}[|0\rangle + |1\rangle + |2\rangle + \cdots + |15\rangle]\,|0\rangle_4$ ($|1111\rangle$)

$\oplus$

Step 2: $\frac{1}{4}\left[|0\rangle_4 \; |0 \oplus 13^0 \pmod{15}\rangle_4 + |1\rangle_4 |0 + 13^1 \pmod{15}\rangle + \right.$

$\left. \ldots \right]$

$\oplus$ = addition modulo 2, XOR

$0 \oplus z = z$

$= \frac{1}{4}\left[|0\rangle_4 |13^0 \pmod{15}\rangle + |1\rangle_4 |13^1 \pmod{15}\rangle_4 \right.$

$\left. + |2\rangle_4 |13^2 \pmod{15}\rangle_4 \ldots \right]$

$= \frac{1}{4}\Big[|0\rangle_4 |1\rangle_4 + |1\rangle_4 |13\rangle_4 + |2\rangle_4 |4\rangle_4 + |3\rangle_4 |7\rangle_4$

$|4\rangle_4 |1\rangle_4 + |5\rangle_4 |13\rangle_4 + |6\rangle_4 |4\rangle_4 + |7\rangle_4 |7\rangle_4$

$|8\rangle_4 |1\rangle_4 + |9\rangle_4 |13\rangle_4 + |10\rangle_4 |4\rangle_4 + |11\rangle_4 |7\rangle_4$

$|12\rangle_4 |1\rangle_4 + |13\rangle_4 |13\rangle_4 + |14\rangle_4 |4\rangle_4 + |15\rangle_4 |7\rangle_4 \Big]$

Step 3: measure the "w" register - say we measure "7"

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

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

↓

4 comb, note the change in normalization

Step 4: Apply $QFT^\dagger$ on the $|x\rangle$ register

recall:

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

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

$\dagger$ complex conj. transpose.

$n=4 \quad N=2^n$

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

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

$$QFT^{\dagger}|11\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{\frac{-2\pi i (11y)}{16}} |y\rangle$$

$$QFT^{\dagger}|15\rangle_4 = \frac{1}{\sqrt{16}} \sum_{y=0}^{N-1} e^{\frac{-2\pi i (15y)}{16}} |y\rangle$$

$$QFT^{\dagger}|x\rangle = \frac{1}{8} \sum_{y=0}^{15} \left[e^{-\frac{i3\pi y}{8}} + e^{-\frac{i7\pi}{8}y} + e^{-\frac{i11\pi}{8}y} + e^{-\frac{i15\pi}{8}y} \right] |y\rangle$$

$\cos\left(\frac{3\pi}{8}y\right) - i\sin\left(\frac{3\pi}{8}y\right)$

$$= \frac{1}{8}\left[4|0\rangle_4 + 4i\,|4\rangle_4 - 4|8\rangle_4 - 4i|12\rangle_4 \right]$$

Step 5:

measure $|x\rangle$ register $\underbrace{0, 4, 8, 12}_{4\ \ 4\ \ 4}$ w/ equal prob.

Remaining steps on classical post-processing

Analyze what happens for each outcome:

measurement results peak near

$j\frac{N}{r}$ for some integer $j \in \mathbb{Z}$ — period that we are looking for.

eg: measure $|4\rangle_4$: $j\frac{16}{r} = 4 \Rightarrow$ true if $j=1, r=4$

$r = 4$?

(1) is r even? yes

$$x \equiv a^{r/2} \pmod N = 13^{4/2} \pmod{15} = 4$$

$x+1 = 5$ $\quad gcd(x+1, N) = gcd(5, 15) = 5$

$x-1 = 3$ $\quad gcd(x-1, N) = gcd(3, 15) = 3$ ↑ works.

$r = 8$?

$j\frac{16}{r} = 8$ $\quad j=1, r=2$ $\quad$ or $\quad j=2$ & $r=4$

$x = 13^{2/2} \bmod (15) = 2$

$x+1 = 3$ $\quad gcd(3,15) = 3$

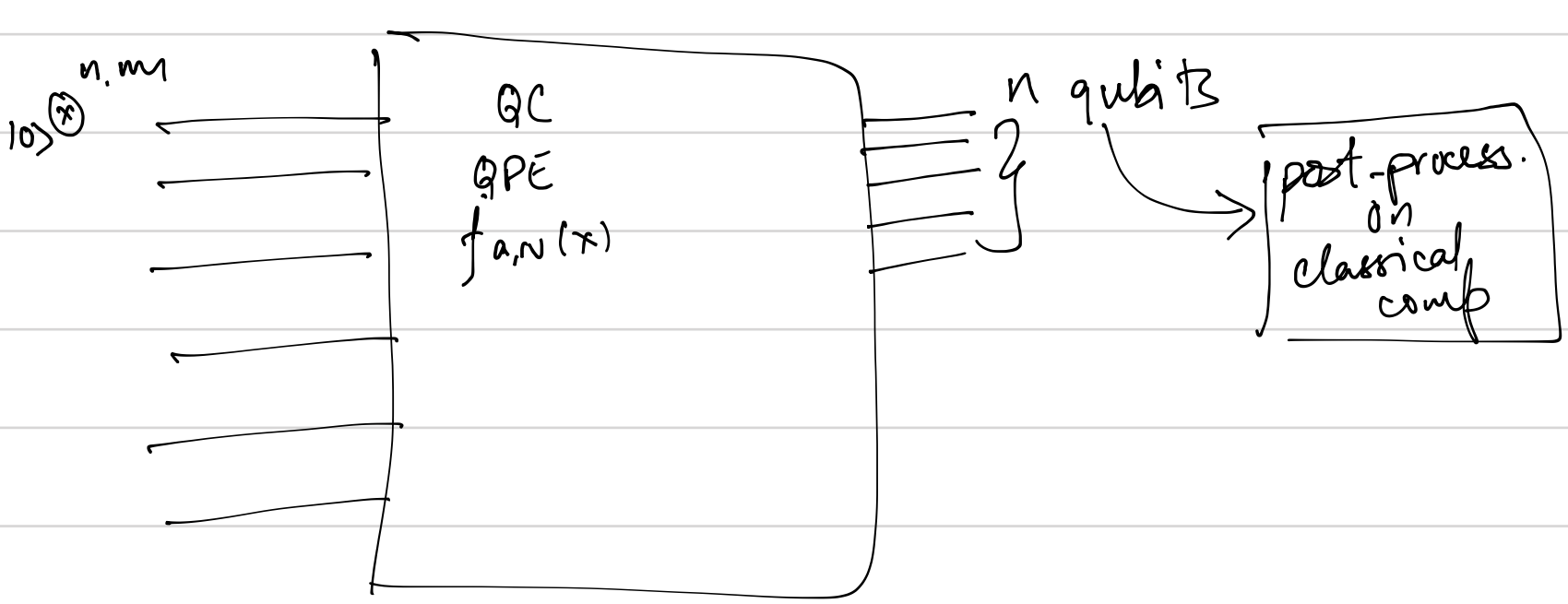
$x-1 = 1$ $\quad gcd(1,15) = 1$ } partial solution.

~~$j \neq 0$~~

Final result : QC told us $|0\rangle_4$, $|4\rangle_4$, $|8\rangle_4$, $|12\rangle_4$ (3,5 ↗ 3,5 ↗ 3,5)

$|0\rangle_4$ ↙ try again

$|4\rangle_4$, $|8\rangle_4$, $|12\rangle_4$ ↙ 3/4 result work here and we are able to extract the factors.



Caveats : register for $|x\rangle$ had n qubits above

$n = 4$

$N = 15 = [1111]$

General case : need $2 \times n$ qubits for input register

- with probability $> 1/2$, r will be even and

$a^{r/2} + 1 \neq 0 \pmod N$

How to implement $U_{f_{a,N}}$

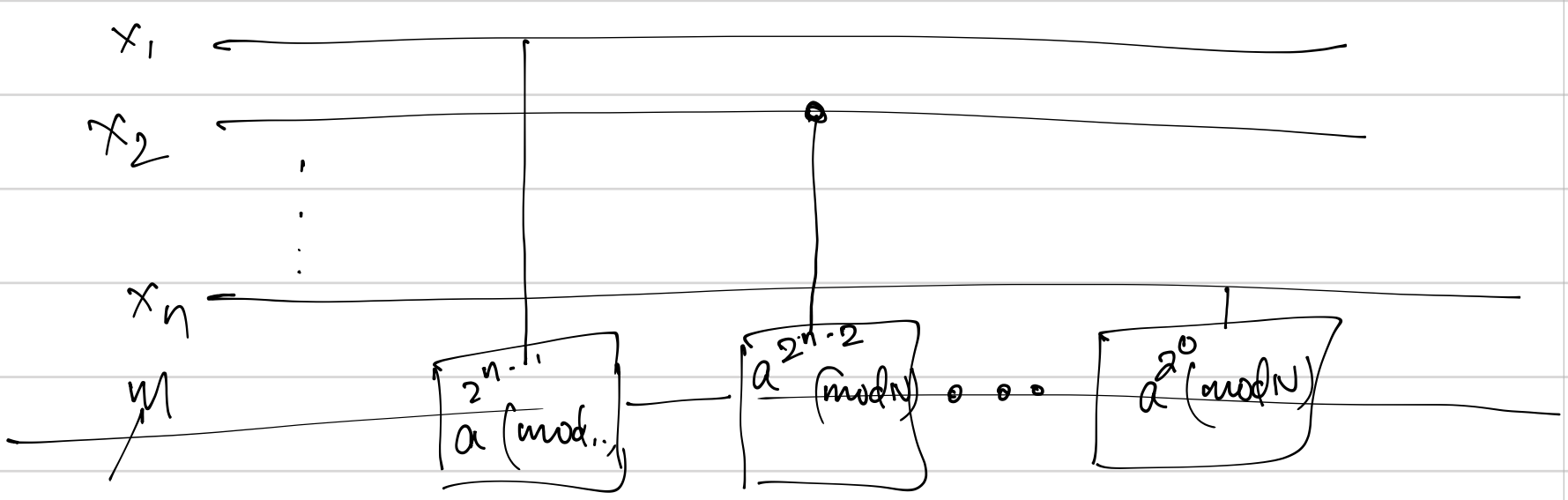
Recall $f_{a,N}(x) \equiv a^x \pmod N$

$x := [x_1 x_2 x_3 \dots x_n] = 2^{n-1} x_1 + 2^{n-2} x_2 + \dots + 2^0 x_n$

$f_{a,N}(x) \equiv a^x \pmod N$

$= a^{2^{n-1} x_1 + 2^{n-2} x_2 + 2^{n-3} x_3 + \dots + 2^0 x_n} \pmod N.$

$= a^{2^{n-1} x_1} \; a^{2^{n-2} x_2} \dots a^{2^0 x_n} \pmod N$



- Qiskit TB chapter on Shor's Algorithm to see how modular exponention is implemented using gates.

factoring 15!