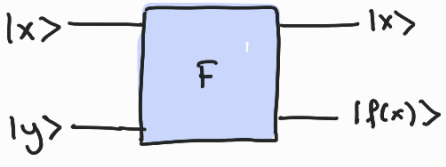
MICRO-435 Week 2 Review

How can we encode Boolean Functions into Unitaries? → norm-preserving

$|x\rangle \rightarrow |f(x)\rangle$

$|x'\rangle \rightarrow |f(x')\rangle$

$\langle x|x'\rangle = 0 \overset{?}{\Leftrightarrow} \langle f(x)|f(x')\rangle = 0$ → Not necessarily, since $f(x)$ may be equal to $f(x')$ yielding 1.



$|x,y\rangle \longrightarrow |x, f(x)\rangle$

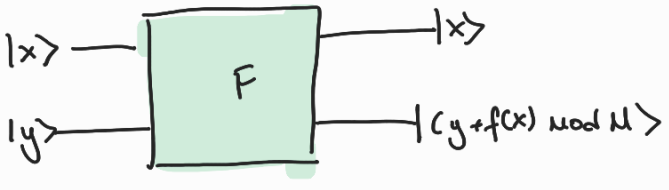
$|x',y'\rangle \longrightarrow |x', f(x')\rangle$

where $x = x'$ copy of each other

$\langle x,y|x',y'\rangle = 0 \Leftrightarrow \langle x, f(x)|x', f(x')\rangle = 0$

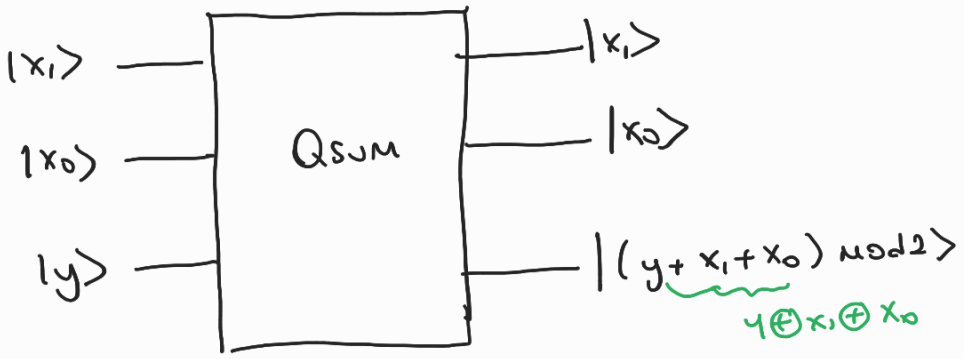
May be $y = y'$. → Thus F is not unitary

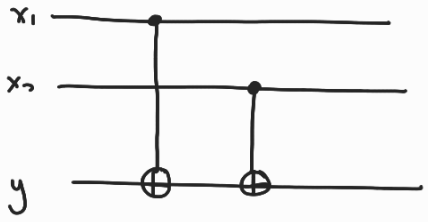
$x = x'$, $f(x) = f(x')$



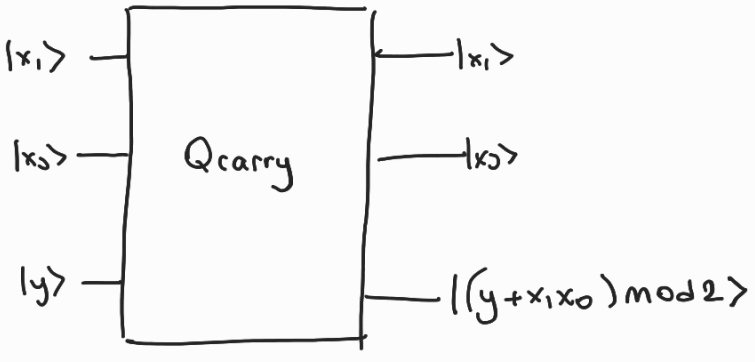
F is Unitary

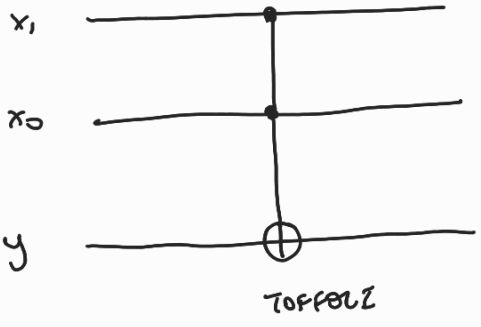
$\langle xy|x',y'\rangle = 0 \Leftrightarrow \langle x', (y+f(x)) \bmod M | x', (y'+f(x')) \bmod M\rangle = 0$





y	x1	x0	f (mod2)
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1





y	x1	x0	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

① Deutsch - Jozsa Algorithm

Problem Statement: $f: \{0,1\}^N \longrightarrow \{0,1\}$

Takes N bits to 1 bits.

CONSTANT
↓
$f(x) = C$ for all x

BALANCED
↓
$f(x) = 0$ for exactly half of the possible input

Example N = 2

f(00)	0	0
f(01)	0	1
f(10)	0	0
f(11)	0	1

What is F ? → Constant / Balanced

Best case

↳ Need 2 queries of the f.

Ex 1st query gives the output 0
2nd " " " 1
} f must be BALANCED

Worst case

Ex

input	output
000	0
001	0
010	0
011	0
...	...
100	
101	
110	
111	

$2^{N/2}$ queries

0 → CONSTANT
1 → BALANCED

$\frac{2^N}{2} + 1$ queries are needed to be 100% certain

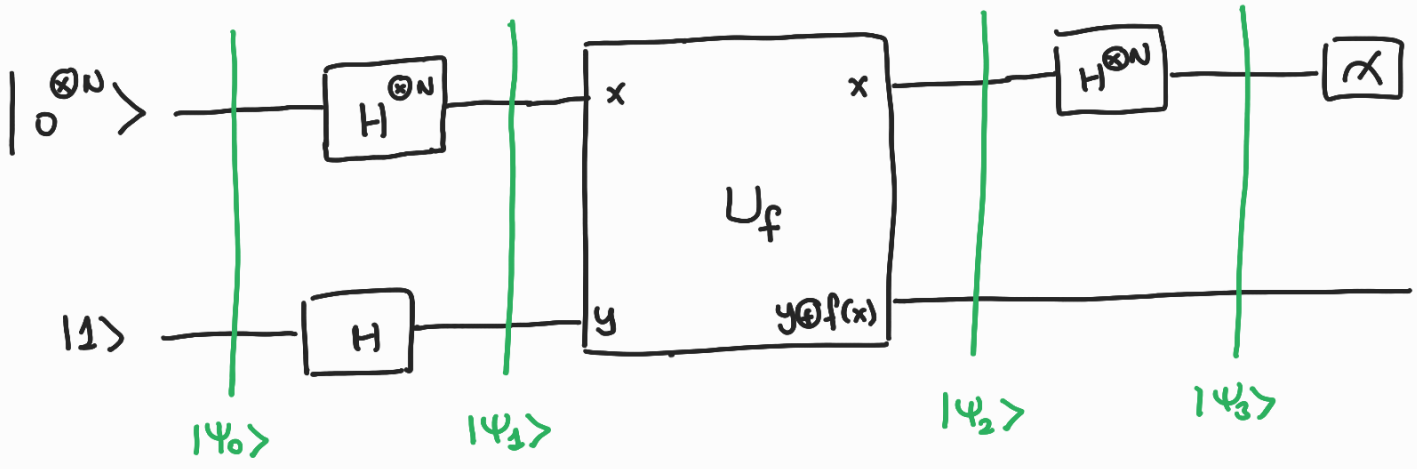
Quantum Solution

Only 1 query of the function f is needed!

Implement f as the quantum oracle that maps

$$|x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle$$

$\oplus$ addition Modulo 2



$$|\psi_0\rangle = |0^{\otimes N}\rangle \otimes |1\rangle$$

$$|\psi_1\rangle = H^{\otimes N} |0^{\otimes N}\rangle \otimes H|1\rangle$$

$$= \left[\left(\frac{1}{\sqrt{2}}\right)^N \sum_{x=0}^{2^N-1} |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle \left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle \right)$$

$$\begin{cases} |0\rangle - |1\rangle & \text{if } f(x)=0 \\ -(|0\rangle - |1\rangle) & f(x)=1 \end{cases}$$

$$(-1)^{f(x)} [\,|0\rangle - |1\rangle\,]$$

1st register

$$|\psi_2\rangle = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

ancilla

$$H^{\otimes N}|x\rangle = \frac{1}{2^{N/2}} \sum_{y=0}^{2^N-1} (-1)^{x \odot y} |y\rangle$$

where $x \odot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{N-1} y_{N-1}$

Example with $N = 2$

$H^{\otimes 2}|x\rangle$ where x can be

	$x_1 x_0$
$0 \longleftrightarrow$	00
$1 \longleftrightarrow$	01
$2 \longleftrightarrow$	10
$3 \longleftrightarrow$	11

for 2 → $|1\rangle \otimes |2\rangle = H \otimes H|10\rangle = H|1\rangle \otimes H|0\rangle$

$$= \left(\frac{1}{\sqrt{2}}\right)^2 [\,|00\rangle + |01\rangle - |10\rangle - |11\rangle\,]$$

$$= \left(\frac{1}{\sqrt{2}}\right)^2 [\,|0\rangle + |1\rangle - |2\rangle - |3\rangle\,]$$

$x_1 x_0 = 10$

$x \odot y$ when $N = 2$ and $X = 2$

$$x \odot y = x_0 y_0 \oplus x_1 y_1 = 0 \cdot y_0 \oplus 1 \cdot y_1 = 0 \oplus y_1 = y_1$$

Same result

$$\frac{1}{2^{N/2}} \sum_{y=0}^{2^N-1} (-1)^{x \odot y} |y\rangle = \frac{1}{2^{N/2}} \sum_{y=0}^{3} (-1)^{y_1} |y\rangle$$

$$\left(\frac{1}{\sqrt{2}}\right)^2 \sum_{y=0}^{3} \{\,|0\rangle + |1\rangle - |2\rangle - |3\rangle\,\}$$

1st register N bit

$$|\psi_2\rangle = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

ancilla

$$|\psi_3\rangle = H^{\otimes N}\left[\frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}(-1)^{f(x)}|x\rangle\right]\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\underbrace{\left[H^{\otimes N}|x\rangle\right]}_{\frac{1}{2^{N/2}}\sum_{y=0}^{N-1}(-1)^{x\odot y}|y\rangle}\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^N}\sum_{y=0}^{2^N-1}\left[\sum_{x=0}^{2^N-1}(-1)^{f(x)}(-1)^{x\odot y}\right]|y\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Measure the 1st qubit

Probability to obtain outcome $|y=0\rangle \equiv |0^{\otimes N}\rangle$

$$\left|\frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}(-1)^{x\odot 0}\right|^2 = \left|\frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\right|^2$$

If $f(x)$ is constant

$$\left|\frac{1}{2^N}(-1)^{f(x)}\sum_{x=0}^{2^N-1}1\right|^2 = \underbrace{\left|(-1)^{f(x)}\right|^2}_{1}\underbrace{\left|\frac{1}{2^N}\sum_{x=0}^{2^N-1}1\right|}_{1} = 1 \;//$$

If $f(x)$ is balanced

$$\left|\frac{1}{2^N}\left(\overbrace{1+1+1+\dots}^{\text{half}}\overbrace{-1-1-1-\dots-1}^{\text{half}}\right)\right|^2 = 0 \;//$$

(0)

* If we measure the outcome $|y=0\rangle$, then $f(x)$ is CONSTANT

any other measurement result means, that $f(x)$ is BALANCED.

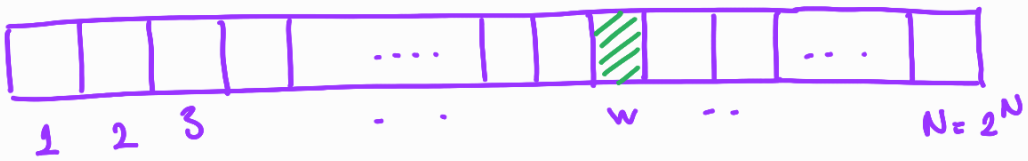
② Grover Search Algorithm

from Qiskit

Search Problem

$$f(x) = \begin{cases} 1 & \text{for } x = x^* \\ 0 & \text{for } x \neq x^* \end{cases}$$

Find x^*



classical average $\frac{N}{2} \longrightarrow O(N)$

Creating an Oracle

$$U_w |x\rangle = \begin{cases} |x\rangle & \text{if } x \neq w \\ -|x\rangle & \text{if } x = w \end{cases}$$

$f(x) = 0$ when $x \neq w$; $f(x) = 1$ when $x = w$

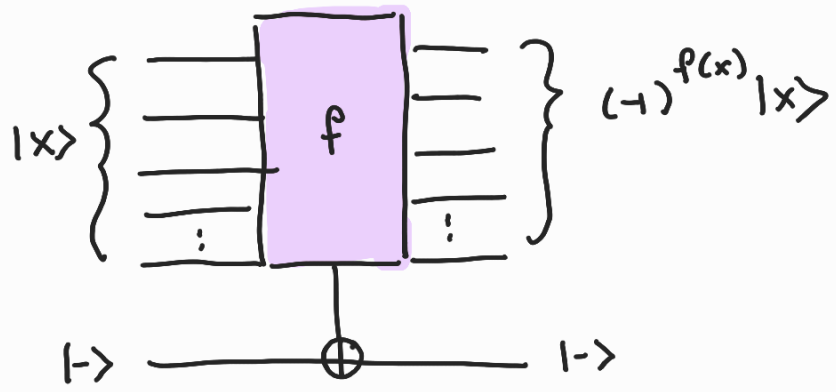
$$= (-1)^{f(x)} |x\rangle$$

$$U_w = \begin{bmatrix} (-1)^{f(0)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(1)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(2^n-1)} \end{bmatrix}$$

diagonal matrix

$$|-\rangle \oplus |1\rangle \qquad ?$$

$$(|0\rangle - |1\rangle) \oplus |1\rangle = |1\rangle - |0\rangle = -|-\rangle = -|-\rangle$$



We will create example oracles where we know w beforehand, and not worry ourselves with whether these oracles are useful or not.

Amplitude Amplification

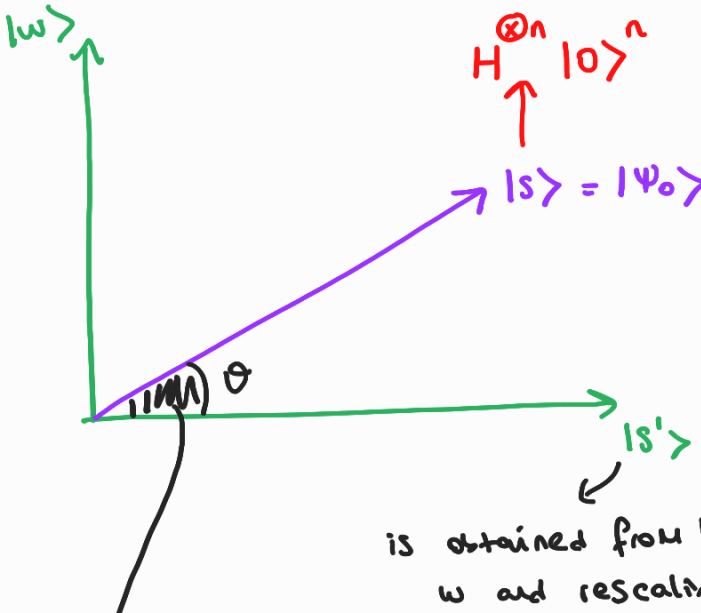
Before looking at the list of items, we have no idea where the marked item is.

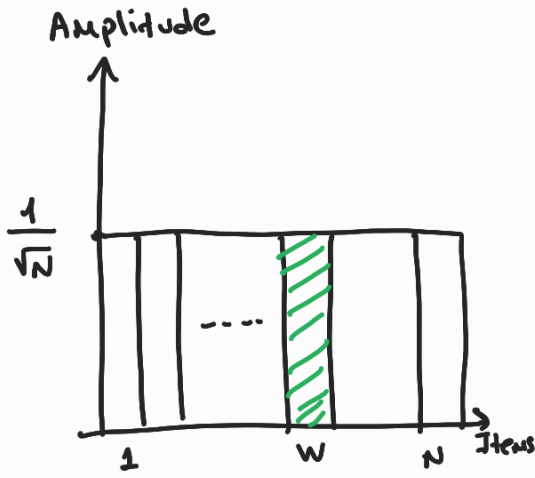
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$|s\rangle$: any guess

Step 1

Amp. amplification process streches out the amplitude of the marked item (w) and shrinks the other item's amplitude.





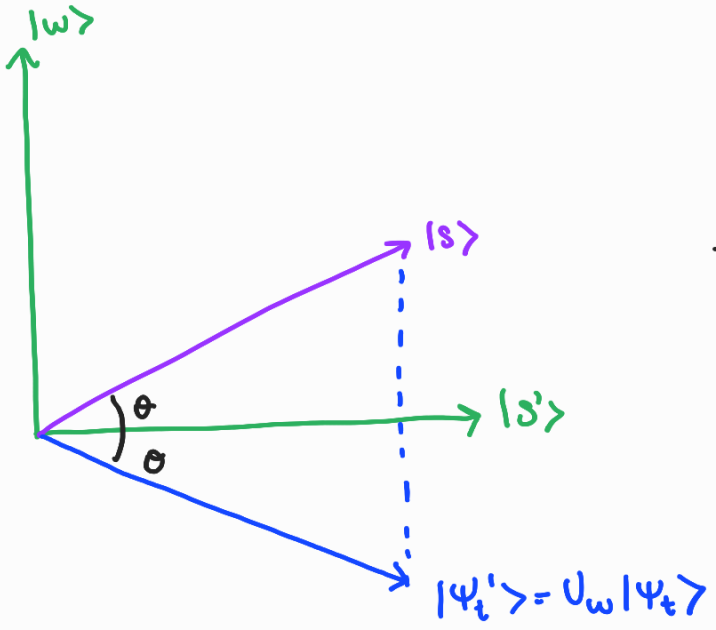
$$|s\rangle = \cos\theta\,|s'\rangle + \sin\theta\,|w\rangle$$

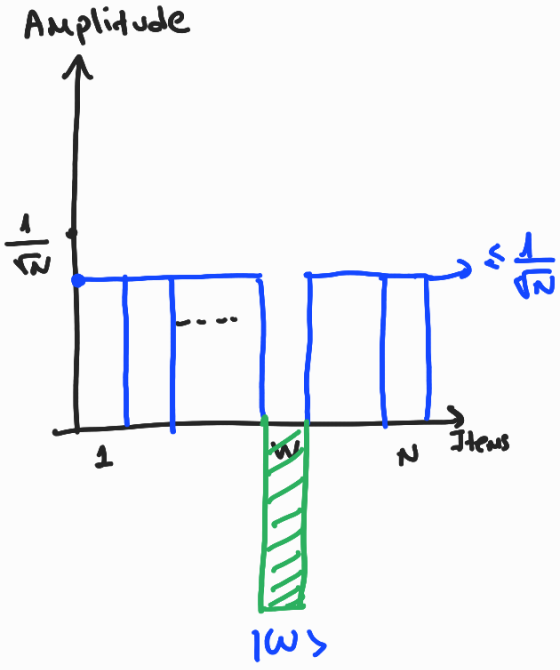
$$\langle s|w\rangle = \cos\theta \underbrace{\langle s'|w\rangle}_{0} + \sin\theta \underbrace{\langle w|w\rangle}_{1}$$

$$\arcsin\langle s|w\rangle = \theta \longrightarrow \arcsin\frac{1}{\sqrt{N}}$$

Step 2

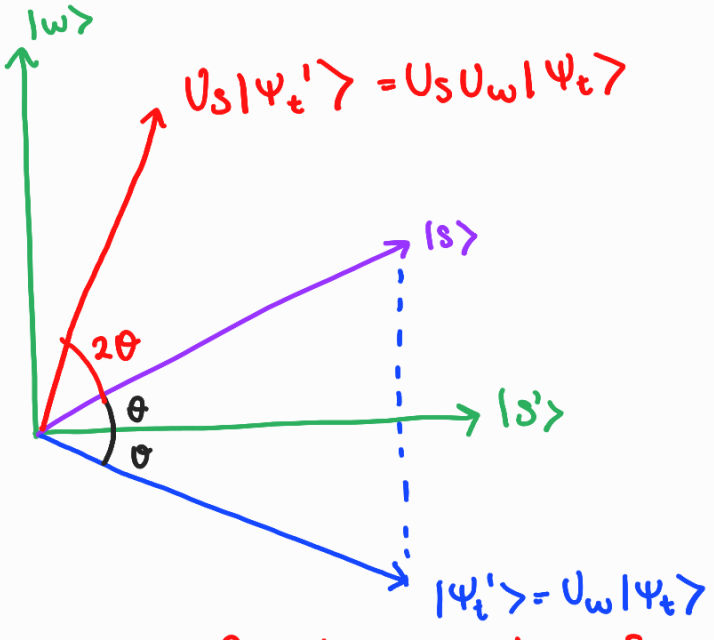
Oracle reflection U_f to the $|s\rangle$

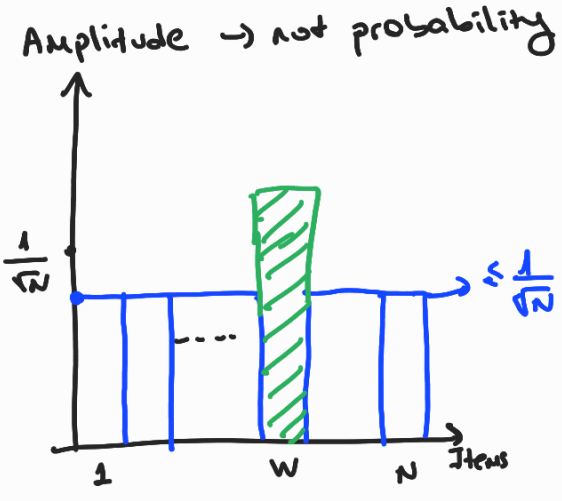




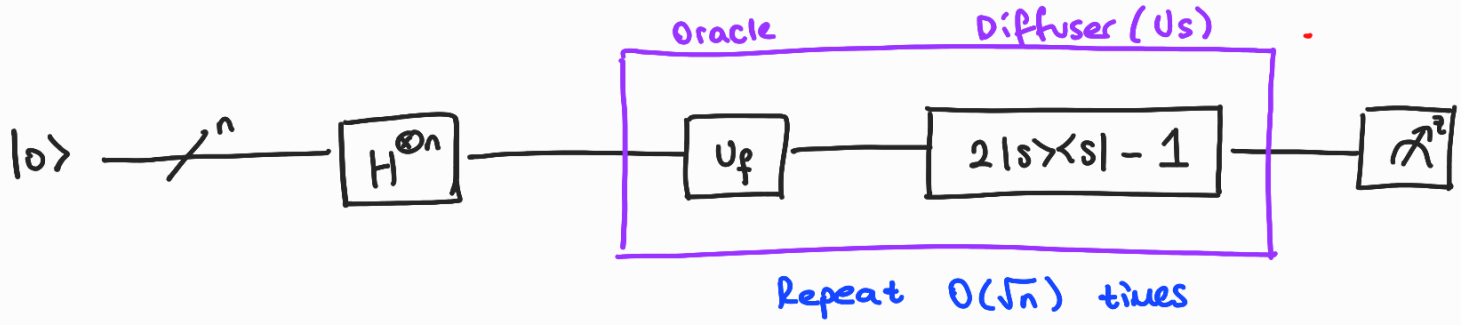
Step 3

Apply an additional reflection $U_s = 2|s\rangle\langle s| - 1$





★ Two reflections always correspond to a rotation

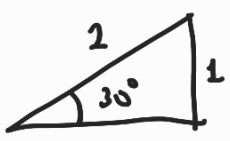


Example: 2 Qubits

$N=4 \rightarrow$ realized with 2 qubits, $|\omega\rangle = |11\rangle = [3]$,

for this case only 1 rotation is enough.

1. $\theta = \arcsin\frac{1}{\sqrt{N}} = \arcsin\frac{1}{2} = \frac{\pi}{6}$ //



2. After t steps

$$(U_s U_\omega)^t |s\rangle = \sin\theta_t |\omega\rangle + \cos\theta_t |s'\rangle$$

$$\theta_t = (2t+1)\theta$$

$|\omega\rangle \leftarrow \frac{\pi}{2}$; $t = 1$; $\frac{\pi}{6}$

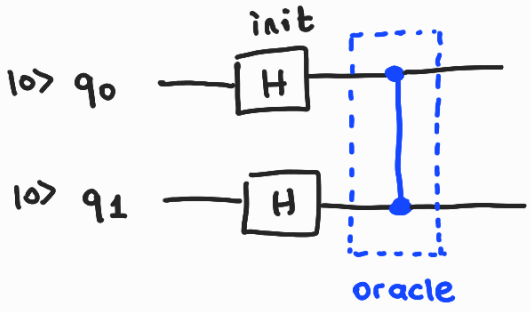
oracle for $|\omega\rangle = |11\rangle$

$$U_\omega |s\rangle = U_\omega \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$$

for this case it's controlled Z gate



Reflection U_s

$U_s = 2|s\rangle\langle s| - 1$. Since this is a reflection about $|s\rangle$, we want to add a negative phase to every state orthogonal to $|s\rangle$.

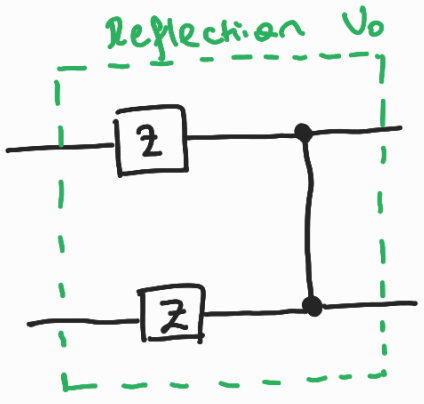
Initially all qubits were $|0\rangle$

$H^{\otimes n}|0\rangle = |s\rangle$

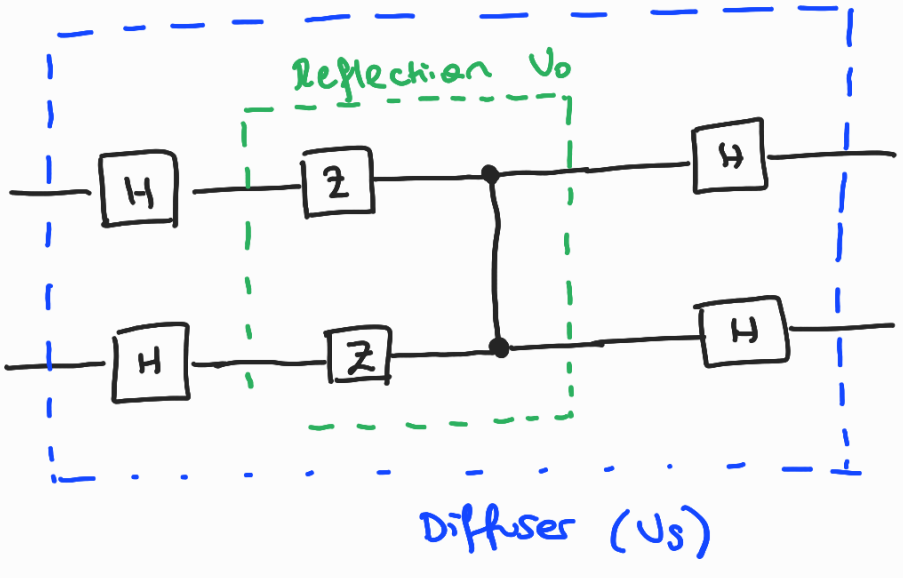
Again $H^{\otimes n}|s\rangle \longrightarrow |0\rangle$

Then we apply a circuit that adds a negative phase to the states orthogonal to $|0\rangle$.

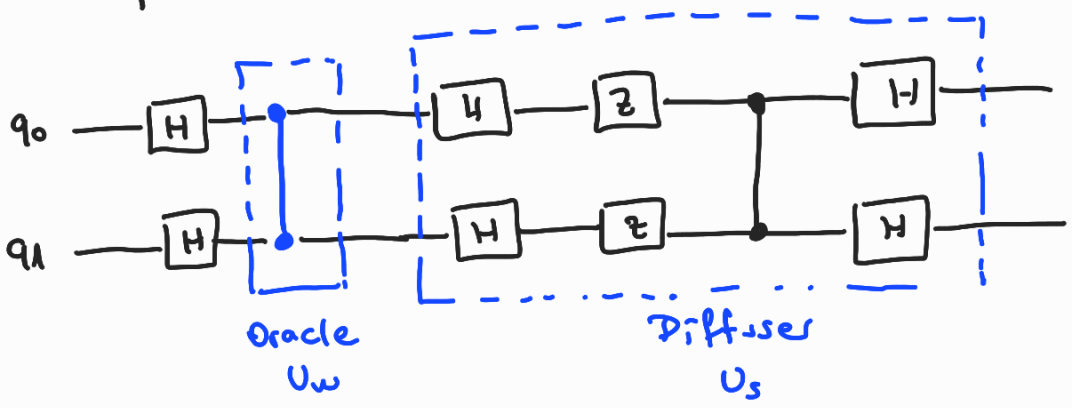
$U_0 \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)$



To return $|s\rangle$ we need to apply Hadamard again.



Full circuit for $|\omega\rangle = |11\rangle$



This is the case for the 2 qubits, for other cases (2↑) circuit is different.

③ Quantum Fourier Transform (QFT)

It is the quantum implementation of the discrete FT over the amplitudes of a wavefunction.

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, \omega_N^{jk}, \qquad \omega_N^{jk} = e^{\frac{2\pi i jk}{N}}$$

$(y_0, \ldots, y_{N-1})$ $\quad$ $(x_0, \ldots, x_{N-1})$

$$|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow |Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$$

(x_j: amplitudes)

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle$$

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle\langle j|$$

$$|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle = \begin{pmatrix} a_0 \\ \vdots \\ a_{N-1} \end{pmatrix}$$

$$DFT\,|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle = \begin{pmatrix} b_0 \\ \vdots \\ b_{N-1} \end{pmatrix}$$

$$b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi i jk/N}$$

Example 2 qubits:

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

$$N = 4 = 2^2$$

$$\rightarrow b_k = \frac{1}{2} \sum_{j=0}^{3} a_j e^{2\pi i jk/4}$$

$$b_0 = \frac{1}{2} \sum_{j=0}^{3} a_j = \frac{1}{2}\left(a_{00} + a_{01} + a_{10} + a_{11}\right)$$

$$b_1 = \frac{1}{2}\left(a_{00} + a_{01} e^{i\pi/2} + a_{10} e^{i\pi} + a_{11} e^{\frac{3i\pi}{2}}\right)$$

$$b_2 = \frac{1}{2}\left(a_{00} + a_{01} e^{i\pi} + a_{10} e^{2i\pi} + a_{11} e^{3i\pi}\right)$$

$$b_3 = \frac{1}{2}\left(a_{00} + a_{01} e^{i3\pi/2} + a_{10} e^{3i\pi} + a_{11} e^{9i\pi/2}\right)$$

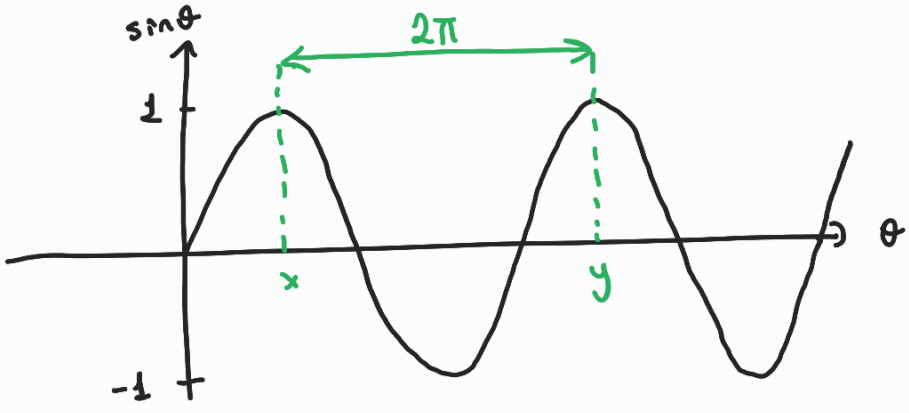
$|$ State in Computational Basis$\rangle$ $\xrightarrow{QFT}$ $|$ State in Fourier Basis$\rangle$

Preliminaries for Shor's Algorithm

Problem: given a function that is periodic, find its period.

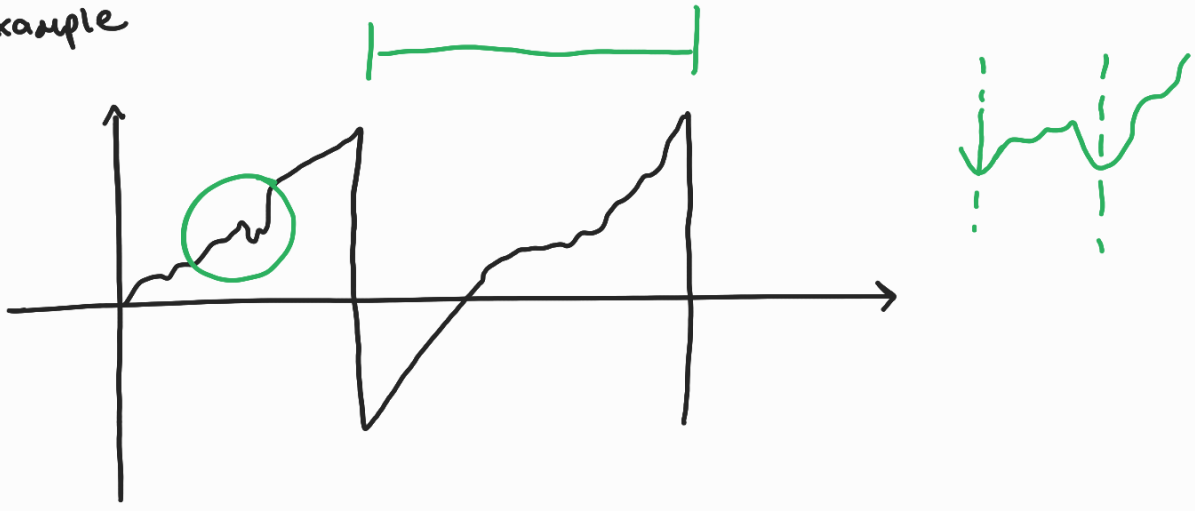
$f(x) = f(y)$ for $x \neq y$ iff $|x-y| = kp$ → period

easy example

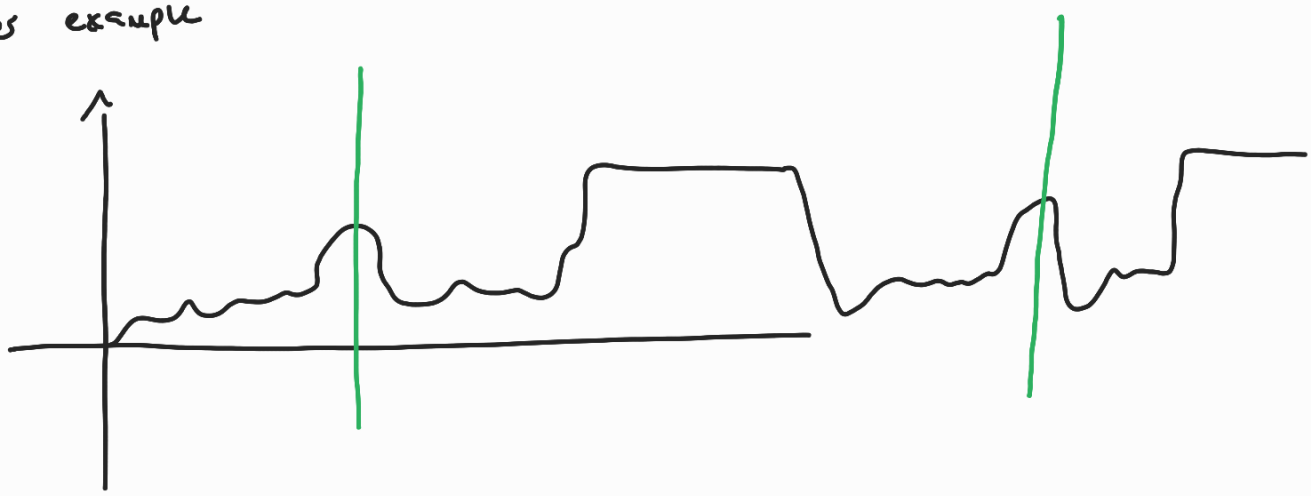


$|x-y| = 2\pi k, \; k \in \mathbb{Z}$

hard example



even harder example



classically: $O\left(\exp c\, n^{1/3} (\log n)^{2/3}\right) = e^{cn^{1/3}(\log n)^{2/3}}$

n: # of bits needed to describe the period.

quantum: Shor's Algorithm $O(n^2 \log n \log(\log n))$

no exponential :)
little faster than $O(n^3)$

Reason why this works: (1) Quantum Fourier Transform

(2) Modular exponentiation

The problem of factoring a number which is a product of two prime numbers is the basis for the security on our computers. → not easily accessible today.

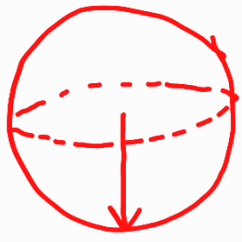
Quantum Fourier Transform (QFT)

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

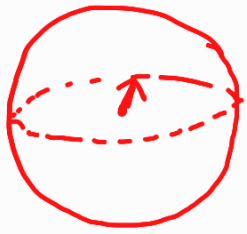
Ex. 1-qubit: comp. basis states are $\{|0\rangle, |1\rangle\}$

Fourier basis for one qubit $\{|+\rangle, |-\rangle\}$

$|0\rangle =$ 

$|1\rangle =$ 

Hadamard Gate

$|\vec{0}\rangle =$  $|\vec{1}\rangle =$ 

Building the quantum circuit that applies QFT

(1) Show QFT rigorously

(2) Show circuit to implement QFT expression that comes from (1)

(1) n qubits

1 qubit: $\{\underbrace{|0\rangle, |1\rangle}_{\text{2 basis states}}\}$

2 qubits: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ → 4 basis states

⋮

n qubits: 2^n basis states → $N = 2^n$

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

$|\tilde{x}\rangle$: Fourier basis; $|x\rangle$: Comp. basis; → DFT

Ex. 1 qubit case $[N = 2^1 = 2]$

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

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

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

$QFT|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi \cdot 0}|1\rangle) = |+\rangle$ $\quad QFT|1\rangle = |-\rangle$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle \quad ; \; N = 2^n : \quad y = [y_1 y_2 \cdots y_n]$$

$$= 2^{n-1} y_1 + 2^{n-2} y_2 + \cdots + 2^0 y_n$$

$$y = 3 = [11] = 2^1 \cdot 1 + 2^0 \cdot 1 = 2 + 1 = 3$$

let's write $y = \sum_{k=1}^{n} y_k \, 2^{n-k}$

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

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

$$\sum_{y=0} \rightarrow \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1}$$

$$= \frac{1}{\sqrt{N}} \left(\sum_{y_1=0}^{1} e^{\frac{2\pi i x y_1}{2^1}} |y_1\rangle \otimes \sum_{y_2=0}^{1} e^{\frac{2\pi i x y_2}{2^2}} |y_2\rangle \otimes \cdots \right.$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2^1}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^3}} |1\rangle \right) \otimes \cdots$$

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

$$|x\rangle = |x_1 x_2 x_3 \cdots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \cdots \otimes |x_n\rangle$$

$\downarrow$ QFT

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

Example: $n=3$ qubits, $N=2^3=8$

$|x\rangle = |5\rangle = |101\rangle$

$$QFT|x\rangle = |\tilde{x}\rangle = |\tilde{5}\rangle = \frac{1}{\sqrt{8}}\left(|0\rangle + e^{\frac{2\pi i 5}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i 5}{2^2}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i 5}{2^3}}|1\rangle\right)$$

(2) The Quantum Circuit that implements QFT

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

each qubit $|x_k\rangle$ to $|0\rangle + e^{\frac{2\pi i x}{2^k}}|1\rangle$

Two observations

(1) $|\tilde{x}\rangle$ contains terms like

$|00\ldots\ldots0\rangle$

$e^{2\pi i x/2^n}|00\ldots\ldots1\rangle$

$e^{2\pi i x/2^{n-1}}|00\ldots\ldots10\rangle$

(2) $e^{\frac{2\pi i \cdot x}{2^1}} + e^{\frac{2\pi i x}{2^2}} + \ldots + e^{\frac{2\pi i x}{2^n}}|11\ldots1\rangle$

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

* Hints:
- phase is qubit-dependent
- need to add up more components with more "1"s

Two ingredients

(1) Hadamard

$$H|x_k\rangle = \begin{cases} x_k=0 \rightarrow (|0\rangle + |1\rangle)/\sqrt{2} \\ x_k=1 \rightarrow (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$$

x_k: 0 or 1

$$= \left(|0\rangle + e^{\frac{2\pi i x_k}{2}}|1\rangle\right)/\sqrt{2}$$

(2) UROT

$x_j = 0 \Rightarrow e^{2\pi i \cdot 0/2^k} |x_j\rangle = |0\rangle$

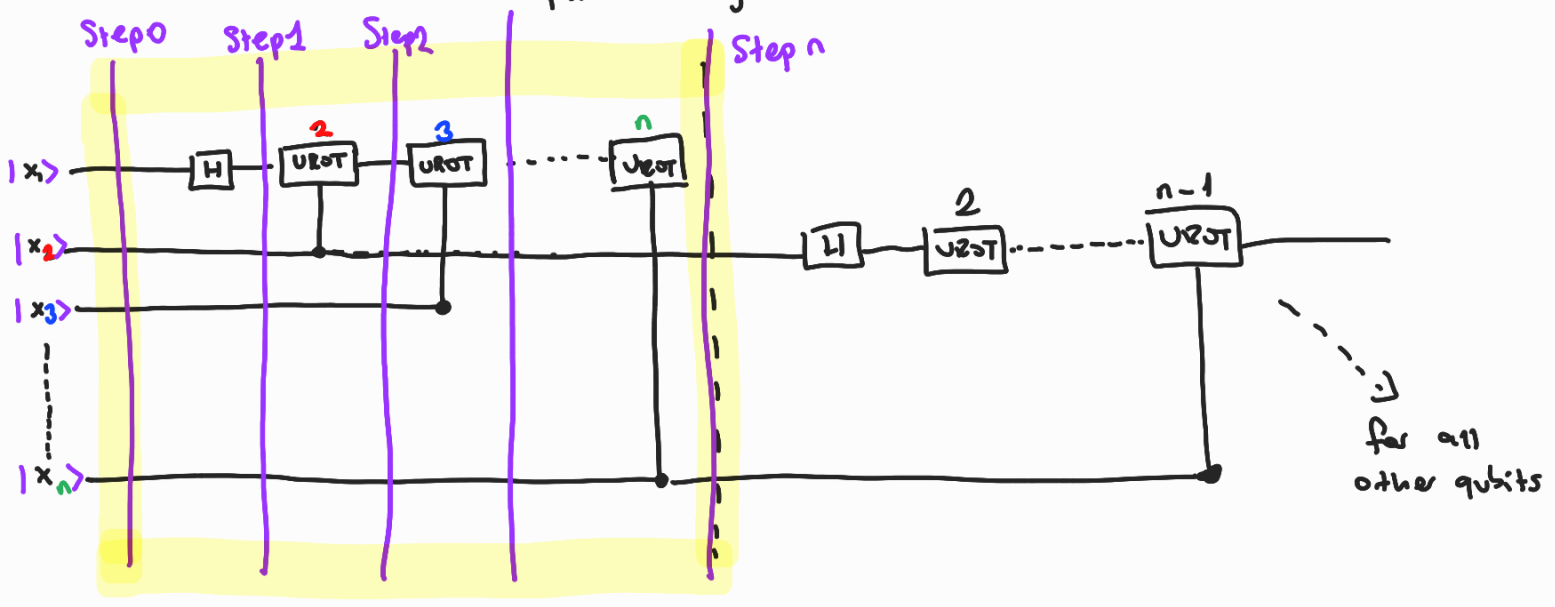
$x_j = 1 \rightarrow e^{2\pi i \cdot 1/2^k} |1\rangle$

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

$$= \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$$

apply phase $e^{\frac{2\pi i}{2^k}}$ for state $|1\rangle$

for a single qubit



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

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

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

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

$\vdots$

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

This circuit implements QFT (except in reverse order of qubits) at output

11/10/22

Quantum Phase Estimation

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

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

Can we extract θ_ψ given the ability to prepare $|\psi\rangle$ and the ability to apply U?

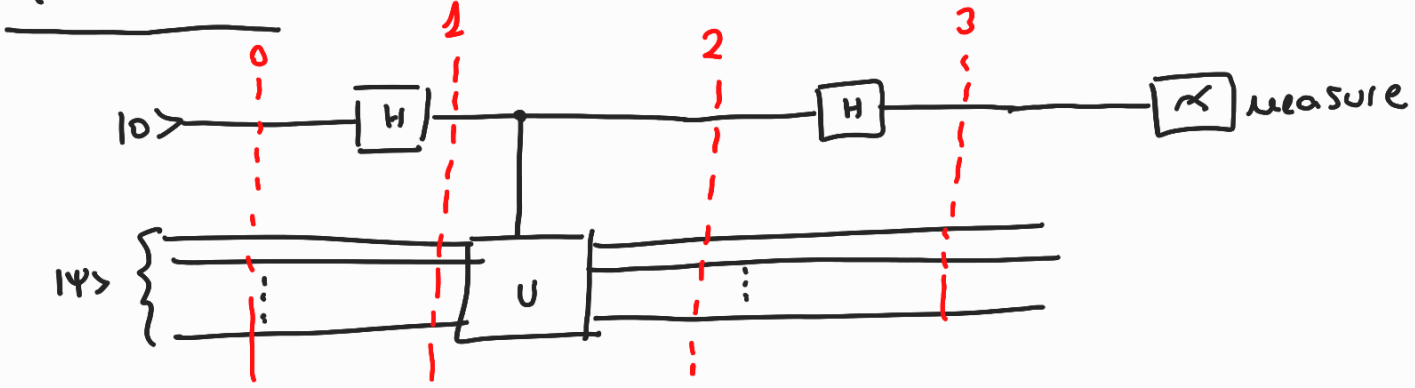
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \begin{cases} 0 & \text{with pr } 1/2 \\ 1 & \text{with pr. } 1/2 \end{cases}$$

$$e^{i\pi/2}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \begin{cases} 0 & 1/2 \\ 1 & 1/2 \end{cases}$$

Solution: Yes, use QPE.

Why do we care? Hamiltonian evolution (time evolution of real system) is unitary.

QPE trick



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: $\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle e^{i\theta_\psi}|\psi\rangle\right)$

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

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

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

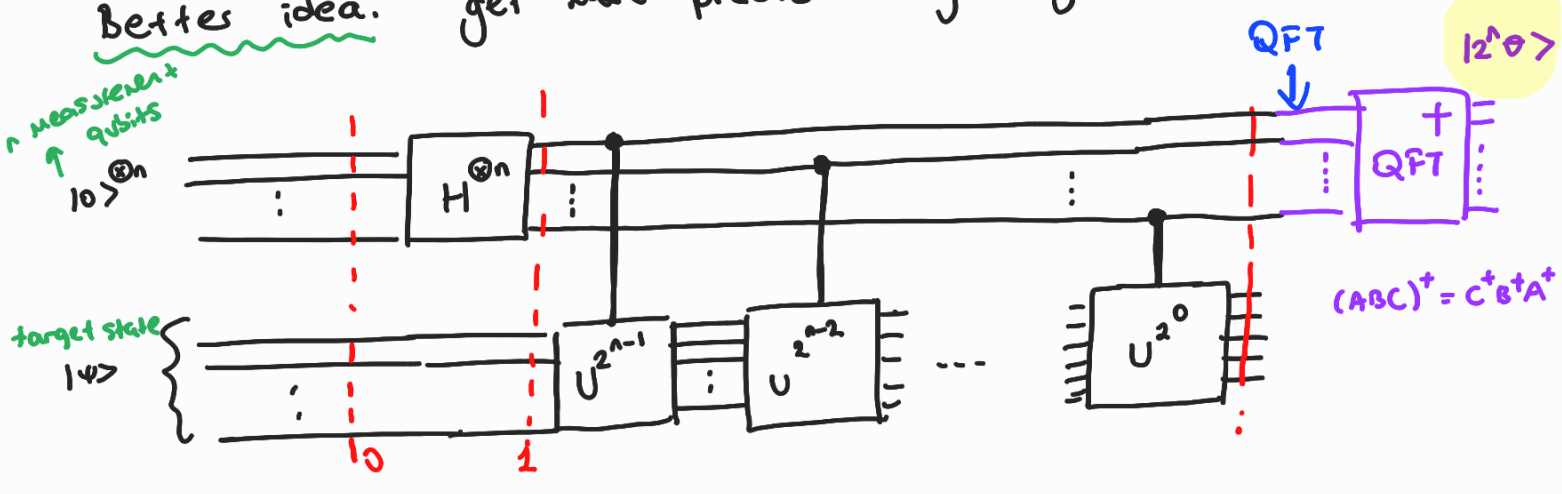
$|1\rangle \rightarrow \left|\frac{1}{2}(1-e^{i\theta_\psi})\right|^2$

Ex $\theta_\psi = 1^\circ$ prob(0), prob(1) = $\{0.9999, 7.6\times10^{-5}\}$

$\theta_\psi = 10^\circ$ prob(0), prob(1) = $\{0.9924, 0.007596\}$

This experiment uses 1 qubit to measure θ_ψ

Better idea: get more precision by using more qubits



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

Step 1: $\left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle)^{\otimes n} \; |\psi\rangle$

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

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

$$\otimes \left(|0\rangle + e^{i\theta_\psi 2^{n-2}} |1\rangle\right) \otimes \cdots$$

$$\otimes \left(|0\rangle + e^{i\theta_\psi 2^{0}} |1\rangle\right)$$

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

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

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

QPE is same as QFT except $\theta_\psi = \frac{2\pi}{2^n} \theta_\psi$

④ Shor's Algorithm: factoring to period-finding and using QPE (and QFT) for factoring

Problem: factoring a number

$N = p \cdot q$ where p and q are prime and big.

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

Shor's algorithm: $O(n^3)$

↘ no exp.! 

Quick primer on modular arithmetic

$5 \equiv 2 \pmod 3$

$x =$	1	2	3	4	5	6	7	8	9	
$x =$	1	2	0	1	2	0	1	2	0	$\pmod 3$

$x \equiv 0 \pmod 3 \Rightarrow x = 3k$

$x \equiv 1 \pmod 3 \Rightarrow x = 3k+1$

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

Notice the periodicity of modular arithmetic

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

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

Protocol for Shor's Algorithm $N = pq$

(1) pick a number "a" coprime with N

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

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

(3) if r is even: good news :)

new variable ← $x \equiv a^{r/2} \pmod N$

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

$\{p, q\}$ contained in { gcd (x+1, N) (greatest common divisor), gcd (x−1, N) }

at least one

else: find another "a"

Ex. Concrete example $N = 15$

$15 = [1111]$ four bits

(1) pick a number that is coprime with 15

pick 13 → a = 13

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

x = 0, 1, 2, 3, 4, 5, 6, 7, ...

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

r = smallest # s.t $a^r \equiv 1 \pmod N \Rightarrow r = 4$

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

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

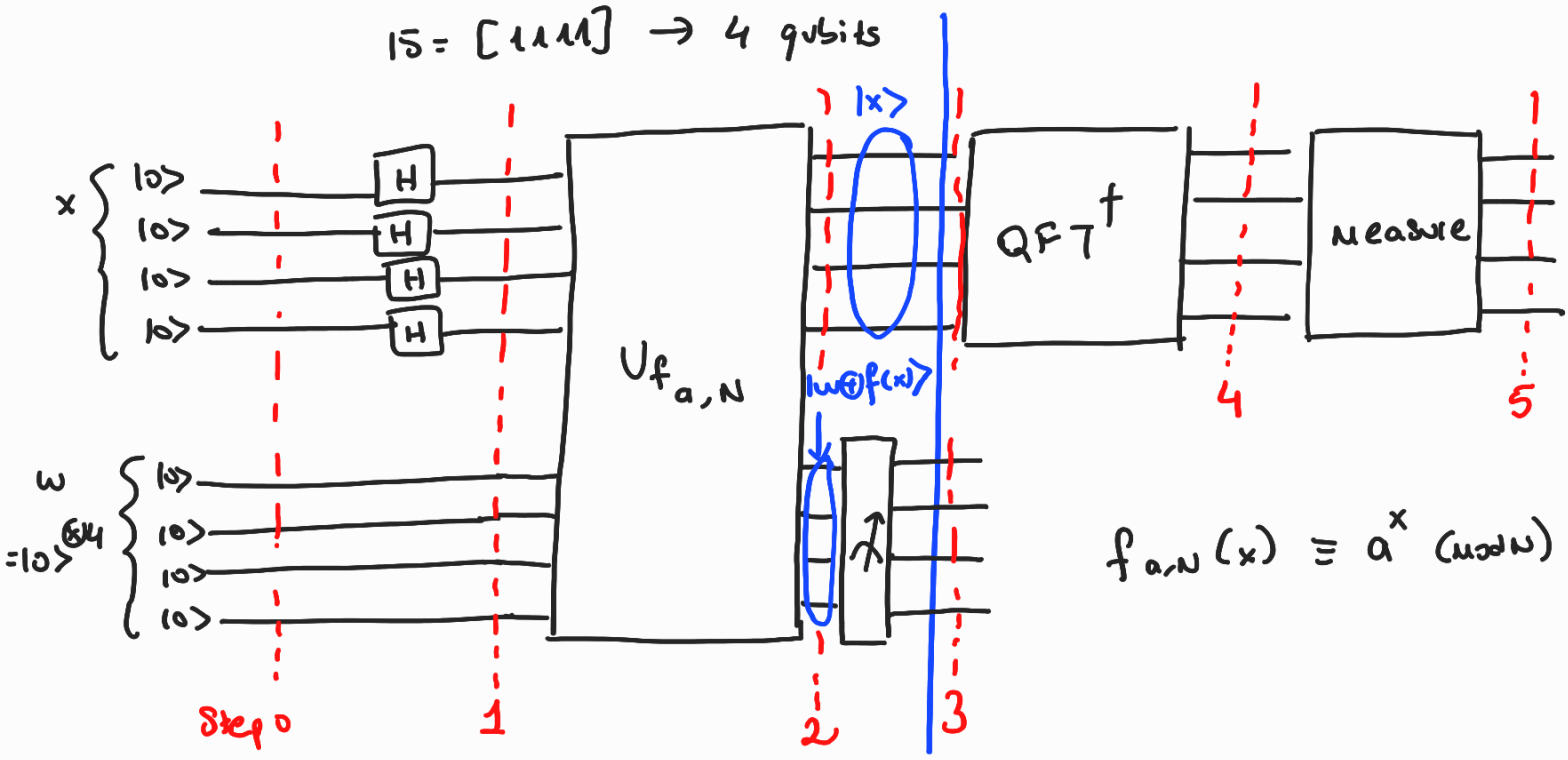
$\gcd(x+1, N) = \gcd(5, 15) = 5$

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

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

Quantum circuit for factoring $N = pq$ $N = 15$

$15 = [1111] \rightarrow$ 4 qubits



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

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

Step 0: $|0\rangle^{\otimes 4}_{x} \; |0\rangle^{\otimes 4}_{w}$

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

Step 2: $\frac{1}{4}\left[|0\rangle_4 \underbrace{|0 \oplus 13^0 \pmod{15}\rangle_4}_{13^0 \pmod{15}} + |1\rangle_4 \underbrace{|0 \oplus 13^1 \pmod{15}\rangle_4}_{13^1 \pmod{15}} + \cdots\right]$ (xor)

$$= \frac{1}{4}\left[|0\rangle_4 \, |13^0 \pmod{15}\rangle_4 + |1\rangle_4 \, |13^1 \pmod{15}\rangle_4 + |2\rangle_4 \, |13^2 \pmod{15}\rangle_4 + \cdots\right]$$

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

Step 3: Measure the "w" register $\rightarrow \{1, 13, 4, 7\}$

Say we measure "7" $\rightarrow x \rightarrow \{3, 7, 11, 15\}$

$$|x\rangle|w\rangle = \frac{1}{2}\left[|13\rangle_4 + |7\rangle_4 + |11\rangle_4 + |15\rangle_4\right] \otimes |7\rangle_4$$

↳ Normalization changed!

Step 4: apply QFT^+ on the $|x\rangle$ register

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

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

QFT^+: complex conjugate

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

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

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

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

$$QFT^+ |x\rangle = \frac{1}{8} \sum_{y=0}^{15} \left[e^{\frac{-i3\pi}{8} y} + e^{\frac{-i7\pi}{8} y} + e^{\frac{-i(11)\pi}{8} y} + e^{\frac{-i(15)\pi}{8} y} \right] |y\rangle$$

$e^{\frac{-i3\pi}{8} y} = \cos\left(\frac{3\pi}{8} y\right) - i \sin\left(\frac{3\pi}{8} y\right)$

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

↑ survived terms

12 terms were vanished :)

Steps: Measure $|x\rangle$ register $\longrightarrow$ $\underbrace{0}_{4}, \underbrace{4}_{4}, \underbrace{8}_{4}, \underbrace{12}_{4}$ with equal probability

Remaining Steps on classical post-processing

Analyze what happens for each outcome:

Measurement results peak near $j\frac{N}{r}$ for some integer $j \in \mathbb{Z}$

($\frac{N}{r}$: period that we're looking for)

Ex Measure $|4\rangle_4$ $\quad j\frac{16}{r} = 4 \Rightarrow$ True if $j=1, r=4$

$r=4$?

↓

(1) is r even? yes

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

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

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

$r=8$?

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

$$x = 13^{2/2} \pmod{15} = 13$$

$x+1 = 14 \quad \gcd(14, 15) = 1$

$x-1 = 12 \quad \boxed{\gcd(12, 15) = 3}$ } partial solution

$r = 12$?

$j \frac{16}{r} = 12$ $\quad j=3, (r=4)$ ✓

Final Result: QC told us $|0\rangle_4$, $|4\rangle_4$, $|8\rangle_4$, $|12\rangle_4$

$|0\rangle_4$ → try again

$|4\rangle_4$ → 3,5 ; $|8\rangle_4$ → 3,5 ; $|12\rangle_4$ → 3,5

3/4 results work here, and we are able to extract it

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

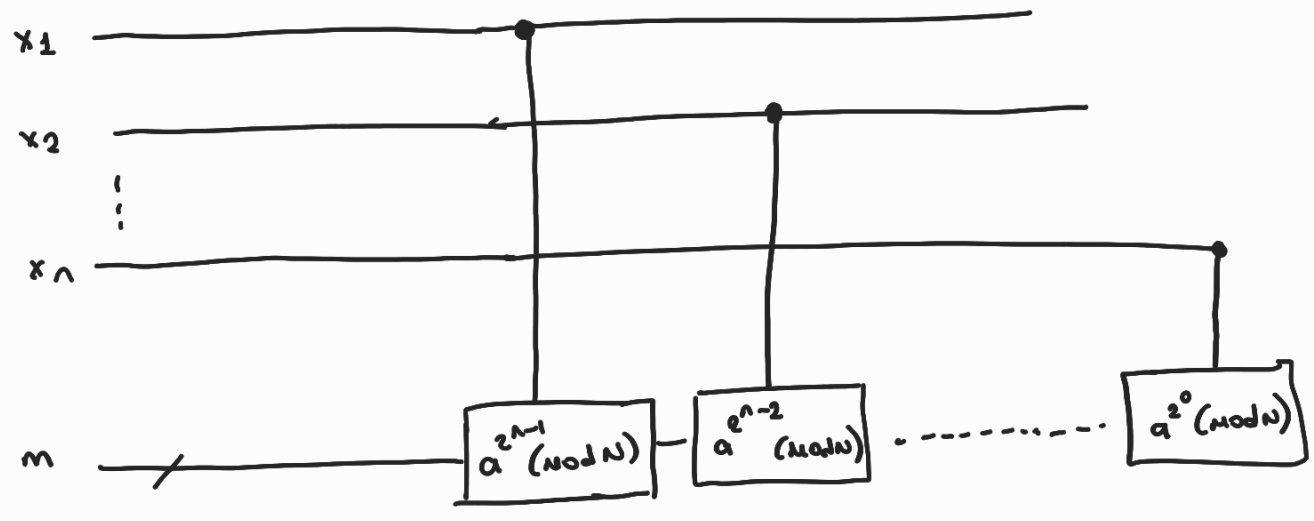
Recall : $f_{a,N}(x) \equiv a^x \pmod N$

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

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

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

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



Shor's Algorithm is QPE in disguise

$$U^{2^x} = a^{2^x} \pmod{N}$$

* Take a look at the Qiskit textbook chapter on Shor's algorithm to see how modular exponentiation is implemented using gates.