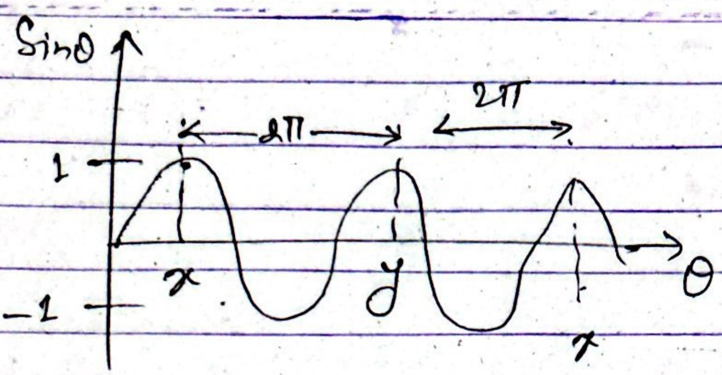
Period function

Given function f(x) that is periodic, find its period

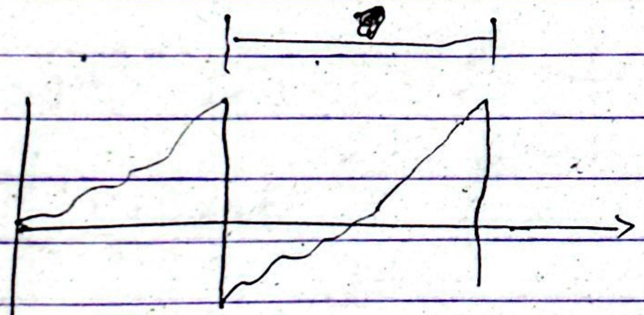
$f(x) = f(y)$ for $x \neq y$ iff $|x-y| = k\, p_{\text{period}}$

eg:



$|x-y| = 2\pi k,\ k \in \mathbb{Z}_{k=0}$

eg.



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

n = # bits needed to describe the period

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

(little faster than $O(n^3)$

The problem of factoring a number which is a ~~period~~ product of two prime numbers is the basis for the security on our computers

What is QFT ?

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

Shor's Algorithm

QFT — use (1) tool for Shor's algorithm for factoring large (2) finding quantum phase estimation for eigenvalue operators.

(1) n qubits

1 qubits : $\{|0\rangle, |1\rangle\} \Rightarrow 2$ basis set

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

n qubits : 2^n basis sets , $N = 2^n$

$|\tilde{x}\rangle$ = QFT of x = QFT $|x\rangle$

$|\tilde{x}\rangle$ — fourier basis; $|x\rangle$ — computational basis

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

eg. 1-Qubit case $[N = 2^1 = 2]$

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

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

$\text{QFT}|0\rangle = |+\rangle$

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

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

Scanned with CamScanner

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

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

A note on notation for multiple qubits (eg $n=3$)

$$|\tilde{x}\rangle = \frac{1}{\sqrt{8}}\sum_{y=0}^{7} e^{2\pi i x y/2^3}|y\rangle \qquad |y\rangle = |100\rangle$$

$$\sum_{y=0}^{7} \rightarrow \sum_{y_1=0}^{1}\sum_{y_2=0}^{1}\sum_{y_3=0}^{1}\cdots\sum_{y_n=0}^{1} |y\rangle = |y_1 y_2 y_3 \cdots y_n\rangle$$

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

$$y = [y_1 y_2 y_3 \cdots y_n]$$

binary to decimal

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

let's write,

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

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

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

$$\Downarrow$$

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

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

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

Our,

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

$$\downarrow QFT$$

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

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

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

$$QFT|x\rangle = |\tilde{x}\rangle = |\tilde{5}\rangle = \frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i 5/2}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 5/4}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i 5}{8}}|1\rangle\right)$$

The quantum Circuit that implements QFT.

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

$|x\rangle = |x_1\rangle |x_2\rangle \cdots |x_n\rangle$.

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

Observation

① $|\tilde{x}\rangle$ Contains terms like

$|000\ldots0\rangle$

$e^{2\pi i x/2^n} \; |000\ldots1\rangle$

$e^{2\pi i x/2^{n-1}} \; |000\ldots10\rangle$

②

$e^{2\pi i x/2^1 + 2\pi i x/2^2 + 2\pi i x/2^3 + \cdots 2\pi i x/2^n} |111\ldots1\rangle$

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

Hints of form of Circuit

Hints of form circuit:

- Phase is qubit dependent
- need to add up more Components with more "1"s

2

Two integredients

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

0 or 1

$e^{\frac{2\pi i x_k}{2}}$: $x_k = 0 \rightarrow 1$

$x_k = 1 \rightarrow -1$

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

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

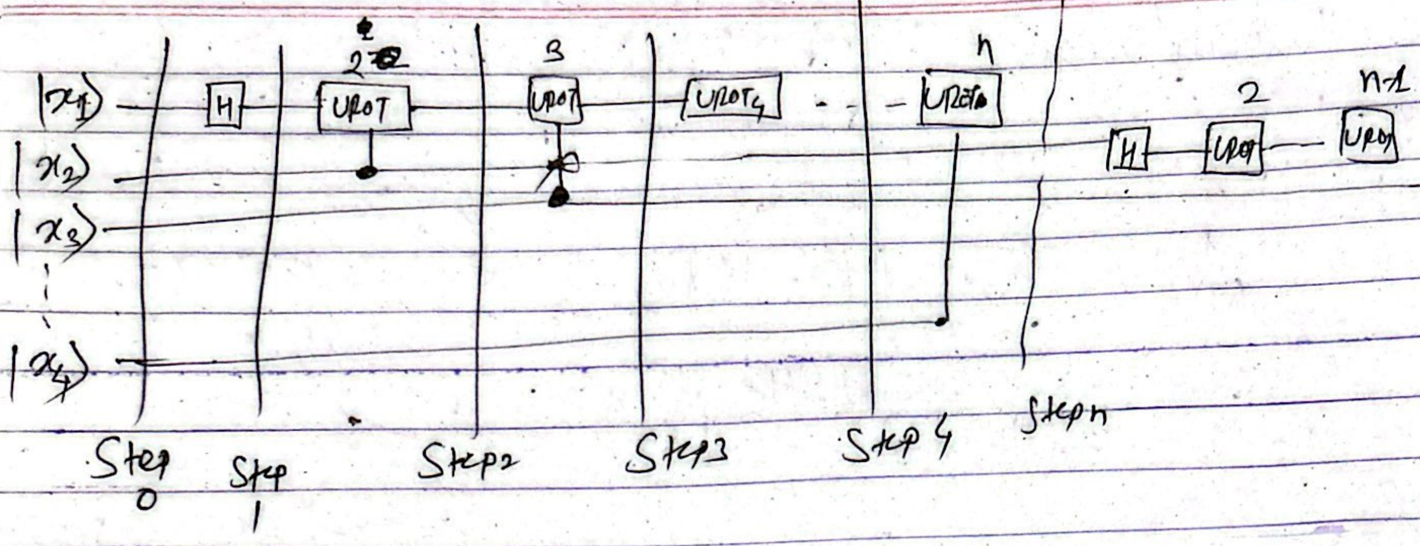
Unitary rotation
(rotation means apply phase)

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

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

Single qubit matrix $= \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$

← applies phase $e^{2\pi i/2^k}$ for state $|1\rangle$



<u>Step 0</u> : $|x_1 x_2 x_3 \cdots x_4\rangle$

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

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

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

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

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

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

$|4\rangle = |100\rangle$

$4 = 2^2 \times 1 + 2^1 \times 0 + 2^0 \times 0$

$\frac{4}{2^3} = \frac{2^2 \times 1 + 2^1 \times 0 + 2^0 \times 0}{2^3}$

Scanned with CamScanner