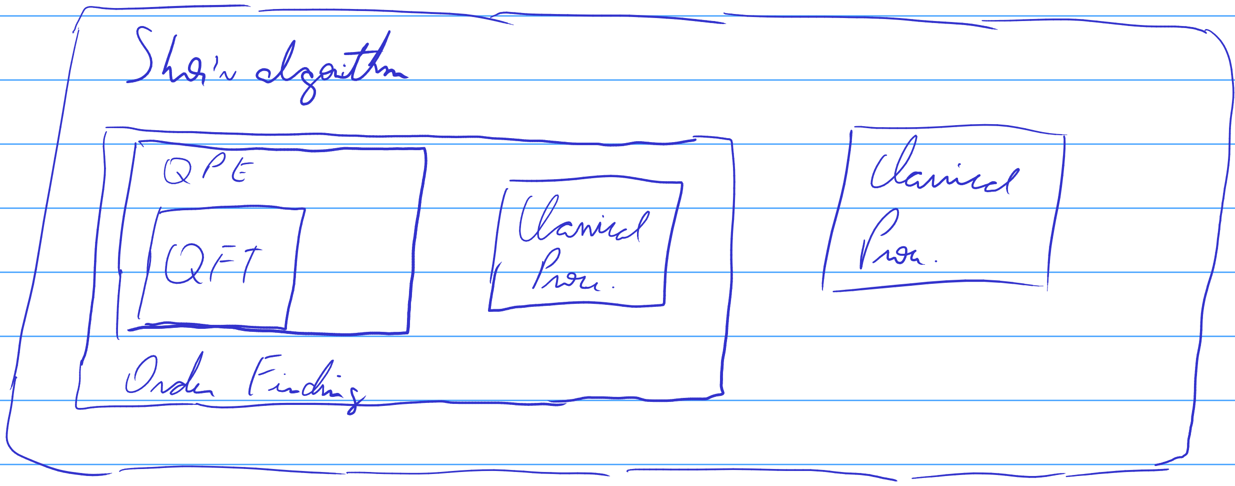
Shor's algorithm

→ Takes an integer N and returns its prime factors

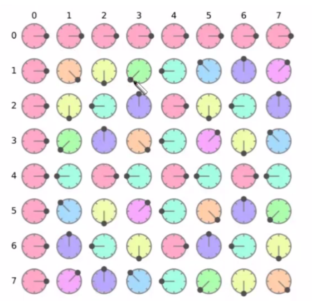


Discrete Fourier Transformation (DFT)

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2N-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3N-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2N-1} & \omega^{3N-1} \; \omega^{4N-1} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

$\omega = e^{i\frac{2\pi}{N}}$ ← some rotation

$DFT_{jk} = \frac{\omega^{jk}}{\sqrt{N}}$ ← it takes a signal vector $\vec{v} = (x_0, x_1, \dots x_{N-1})$, $x_i \in \mathbb{C}$ and returns $DFT \cdot \vec{v}$



← as rotações na matrix com $N=8$

→ Using $\vec{y} = DFT\ \vec{v}$ you find some periods in $\vec{v}$

$\vec{v} = (1, 0, 0, 1, 0, 0, 1, 0, 0)$

period $r = 3$
$N = 9$

→ if we use DFT here, will get some peak at multiples of $\frac{N}{r}$

if we have $\vec{v} \rightarrow$ period r_1
$\vec{V} \rightarrow$ period r_2

DFT $(\vec{v}+\vec{V})$ will picture peaks at multiples of $\frac{N}{r_1}$ and $\frac{N}{r_2}$

QFT

→ DFT on quantum states

$$|\psi\rangle \xrightarrow{QFT} DFT\,|\psi\rangle$$

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$$

$$DFT\,|\psi\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j\, w^{kj} |k\rangle$$

→ QFT is exponentially faster than DFT

Binary expansion of integer

→ Transform an int. to a sum of powers of 2

$$9 = 1.2^3 + 0.2^2 + 0.2^1 + 1.2^0 = 1001$$

$$0,75 = \frac{1}{2} + \frac{1}{4} = 1.2^{-1} + 1.2^{-2} = 0,11$$

$$9 + 0,75 = 1001,11$$

$$2.1001,11 \rightarrow 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 1.2^0 + 1.2^{-1}$$

$$\rightarrow 10011,1 \leftarrow \text{shift left}$$

integer binary i

$$i = 2^n \sum_{l=1}^{n} 2^{-l} i_l$$

↳ the biggest factor 2^n being mult. by the index l

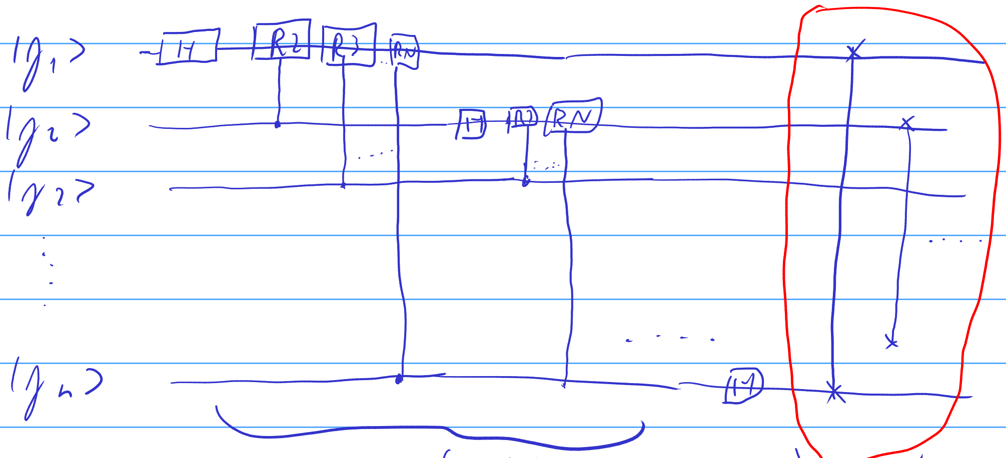
QFT on basis states

$$QFT|j_1 j_2 \dots j_n\rangle = \frac{1}{2^{n/2}}\Big((|0\rangle + e^{2\pi i j 2^{-1}}|1\rangle) \otimes (|0\rangle + e^{2\pi i j 2^{-2}}|1\rangle) \otimes \dots\Big)$$

QFT circuit

gate $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$

$$CR_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{pmatrix}$$



reverse the qubits order

$O\left(\frac{n(n+1)}{2} + \frac{n}{2}\right)$

$\frac{n(n+1)}{2}$ gates

$n/2$ gates

classically $O(n \underbrace{2^n}_{\text{expon. factor}})$ → quantum $O(n^2)$

Inverse QFT

→ QFT is unitary so $QFT\ QFT^{\dagger} = I$

→ run QFT backwards

→ get the periods result and recreate the input vector

QPE

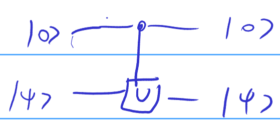
→ any U has an eigenvector

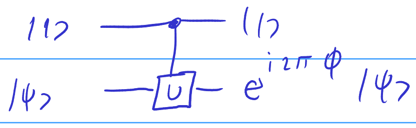
$U|\lambda\rangle = \lambda|\lambda_k\rangle$ $\qquad \lambda_k = e^{i\theta}$ or $e^{i2\pi\phi_k}$

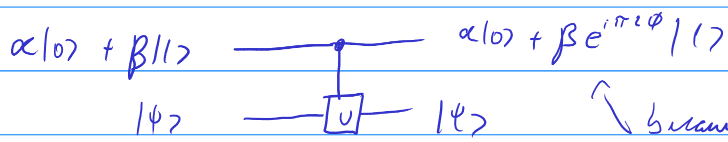
$0 \le \phi_k < 1$

→ take an oracle U and an eigenvector of U $|\psi\rangle$ → $U|\psi\rangle = e^{i2\pi\phi}|\psi\rangle$ it returns ϕ

idea behind QPE

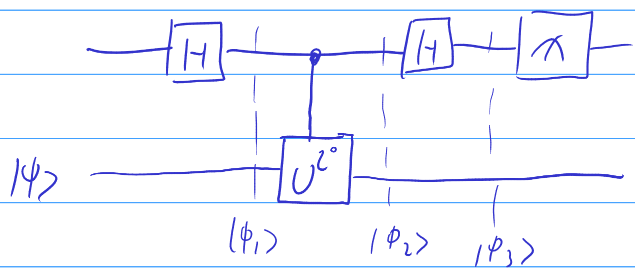






because

$(\alpha|0\rangle + \beta|1\rangle)|\psi\rangle \xrightarrow{CU} \underbrace{\alpha|0\rangle|\psi\rangle + \beta e^{i2\pi\phi}|1\rangle|\psi\rangle}_{|\psi\rangle \text{ is not affected}}$



$|\varphi_1\rangle = |+\rangle|\psi\rangle$ $\qquad$ $|\varphi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi\phi}|1\rangle\right)|\psi\rangle$

$|\varphi_3\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + e^{i2\pi\phi}|-\rangle\right)|\psi\rangle$

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) + e^{i2\pi\phi}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)|\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left((|0\rangle+|1\rangle) + e^{i2\pi\phi}(|0\rangle-|1\rangle)\right)\right)|\psi\rangle$$

$$\frac{1}{2}\left(|0\rangle+|1\rangle + e^{i2\pi\phi}|0\rangle - e^{i2\pi\phi}|1\rangle\right)|\psi\rangle$$

$$\frac{1}{2}\left((1+e^{i2\pi\phi})|0\rangle + (1-e^{i2\pi\phi})|1\rangle\right)|\psi\rangle$$

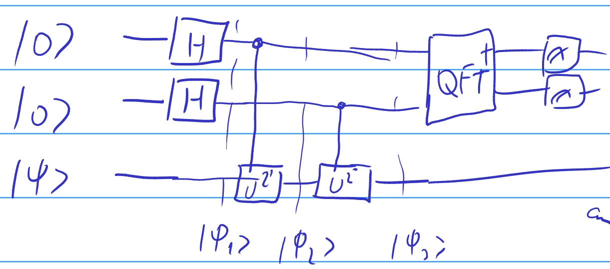
if $\phi = 0 \rightarrow |0\rangle|\psi\rangle$

$\phi = \frac{1}{2} \rightarrow |1\rangle|\psi\rangle$

the only 2 possible values for 1 bit

$0.0 \rightarrow 0$

$0.1 \rightarrow 1/2 \ (2^{-1})$



the multi values and then phase

the 4 possible values

$0.00 \rightarrow 0$

$0.01 \rightarrow 0.25$

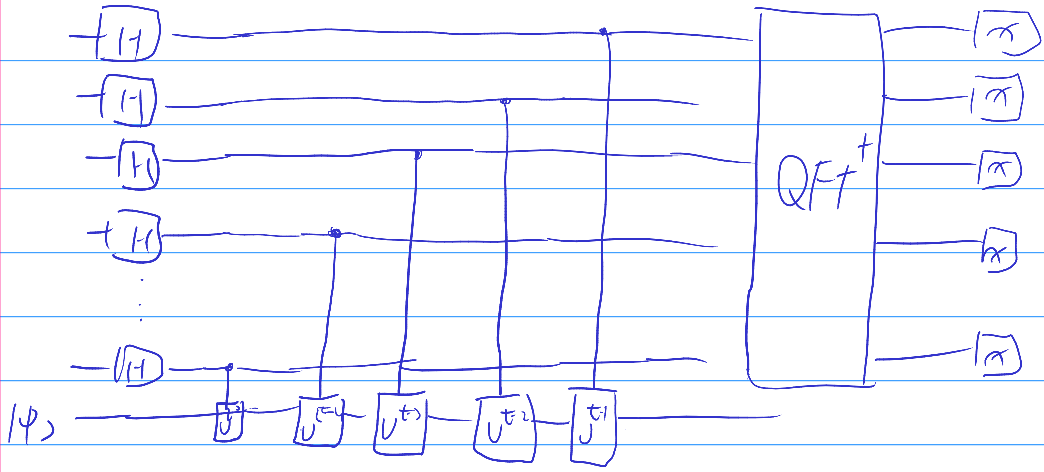
$0.10 \rightarrow 0.5$

$0.11 \rightarrow 0.75$

$|\varphi_1\rangle = |+\rangle|+\rangle|\psi\rangle$

$|\varphi_2\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{i4\pi\phi}|1\rangle)\right)|+\rangle|\psi\rangle$

$|\varphi_3\rangle = (|0\rangle + e^{i4\pi\phi}|1\rangle)(|0\rangle + e^{i2\pi\phi}|1\rangle)|\psi\rangle$



H
H
H
H
H
|ψ⟩
U
U
U
U
U
QFT†