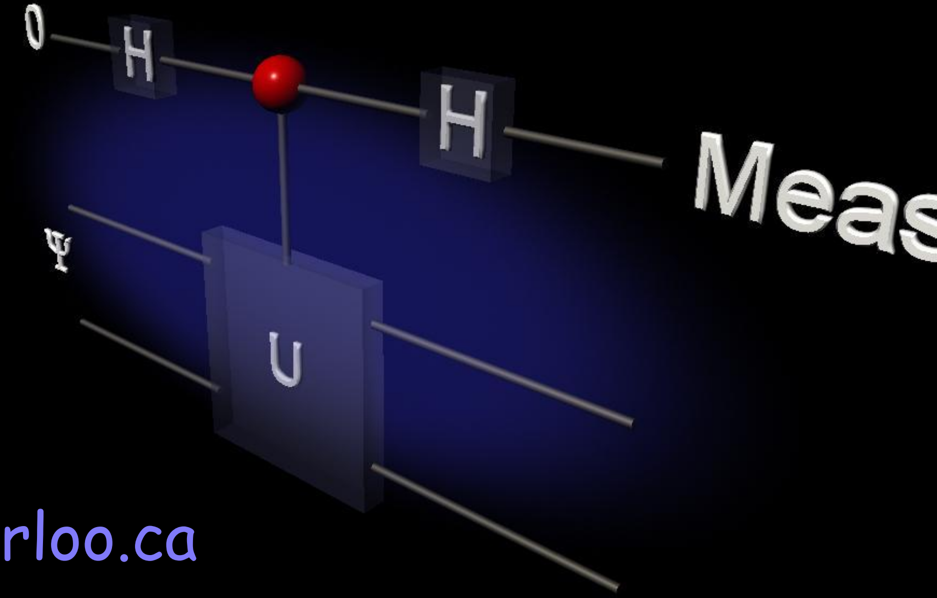
Introduction to Quantum Information Processing



CO481 CS467 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

Institute for Quantum Computing

UNIVERSITY OF WATERLOO

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Shor's factoring algorithm

•Peter Shor first discovered a polynomial time quantum algorithm for factoring integers

•Main idea:

$$\sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |x\rangle |a^x \bmod N\rangle$$

$$= \sum_{b=0}^{r-1} \left(\sum_{z} \frac{1}{\sqrt{2^n}} |zr+b\rangle \right) |a^b \bmod N\rangle$$

Shor's factoring algorithm

•Main idea:

$$\sum_{b=0}^{r-1}\left(\sum_{z}\frac{1}{\sqrt{2^n}}\left|zr+b\right\rangle\right)\left|a^b \bmod N\right\rangle$$

Suppose we measure the second register, to get $a^b \bmod N$ for some random b. The first register will be in the state (renormalized):

$$\sum_{z=0}^{\left\lfloor \frac{2^n-b-1}{r}\right\rfloor}\left|zr+b\right\rangle$$

Extracting r

Suppose we have $\sum_{z=0}^{m-1} \frac{1}{\sqrt{m}} |zr+b\rangle$ then applying QFT_{mr} gives:

$$\sum_{z=0}^{m-1} \frac{1}{\sqrt{m}} |zr+b\rangle \mapsto \sum_{z=0}^{m-1} \frac{1}{m\sqrt{r}} \sum_{x=0}^{mr-1} e^{2\pi i \frac{x(zr+b)}{mr}} |x\rangle$$

$$= \frac{1}{m\sqrt{r}} \sum_{x=0}^{mr-1} \left(\sum_{z=0}^{m-1} e^{2\pi i \frac{x(zr+b)}{mr}} \right) |x\rangle$$

$$= \frac{1}{m\sqrt{r}} \sum_{k=0}^{r-1} \left(\sum_{z=0}^{m-1} e^{2\pi i \frac{kb}{r}} \right) |mk\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{kb}{r}} |mk\rangle$$

Extracting r

Thus measuring gives a value w satisfying $w \cdot r = 0 \bmod mr$

If we know mr, then it is easy to recover r given w (with high probability, given a constant number of samples of such w)

However, we don't know the value *mr* and thus cannot implement QFT_{mr}

Careful calculation shows that implementing QFT_{2^n} (where $2^n > 2r^2$) is good enough, in the sense that one is likely to get a value x such that, for some integer k,

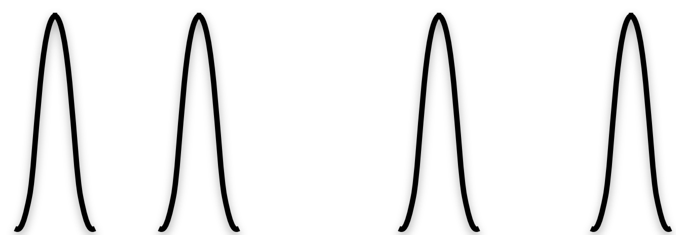
$$\left| \frac{x}{2^n} - \frac{k}{r} \right| \leq \frac{1}{2^n} < \frac{1}{2r^2}$$

Shor's Factoring Algorithm

$$\sum_x |x\rangle|1\rangle \mapsto \sum_x |x\rangle\left|a^x\right\rangle$$

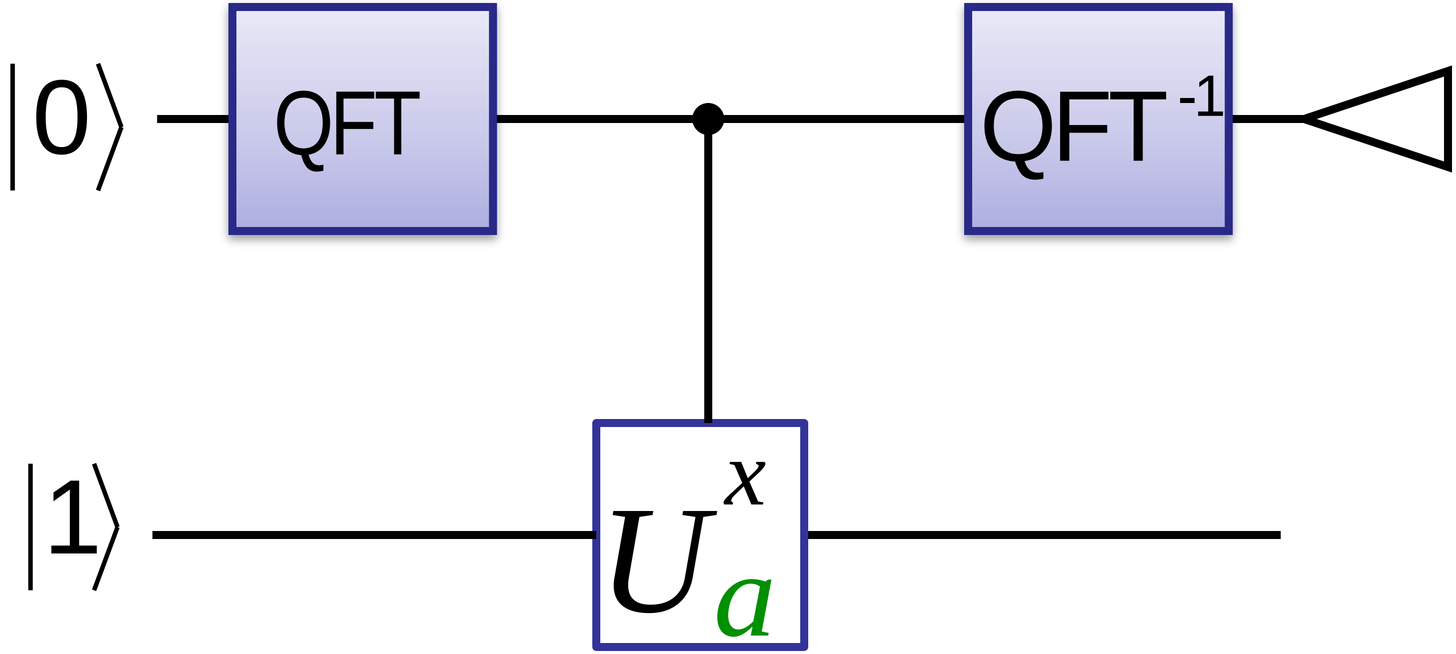
$$= \sum_{b=0}^{r-1}\sum_z |b+zr\rangle\left|a^b\right\rangle$$

$$\xrightarrow{\text{QFT}^{-1}} \sum_z \Big(\quad \Big) \left|a^b\right\rangle$$



$\frac{0}{r}$ $\frac{1}{r}$ $\frac{k}{r}$

A circuit for Shor's Factoring Algorithm

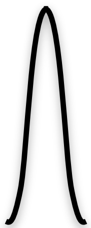


Eigenvalue Estimation
Factoring Algorithm

$$|0\rangle|1\rangle \mapsto \sum_{k=0}^{r-1}\sum_{x}|x\rangle|\psi_k\rangle$$

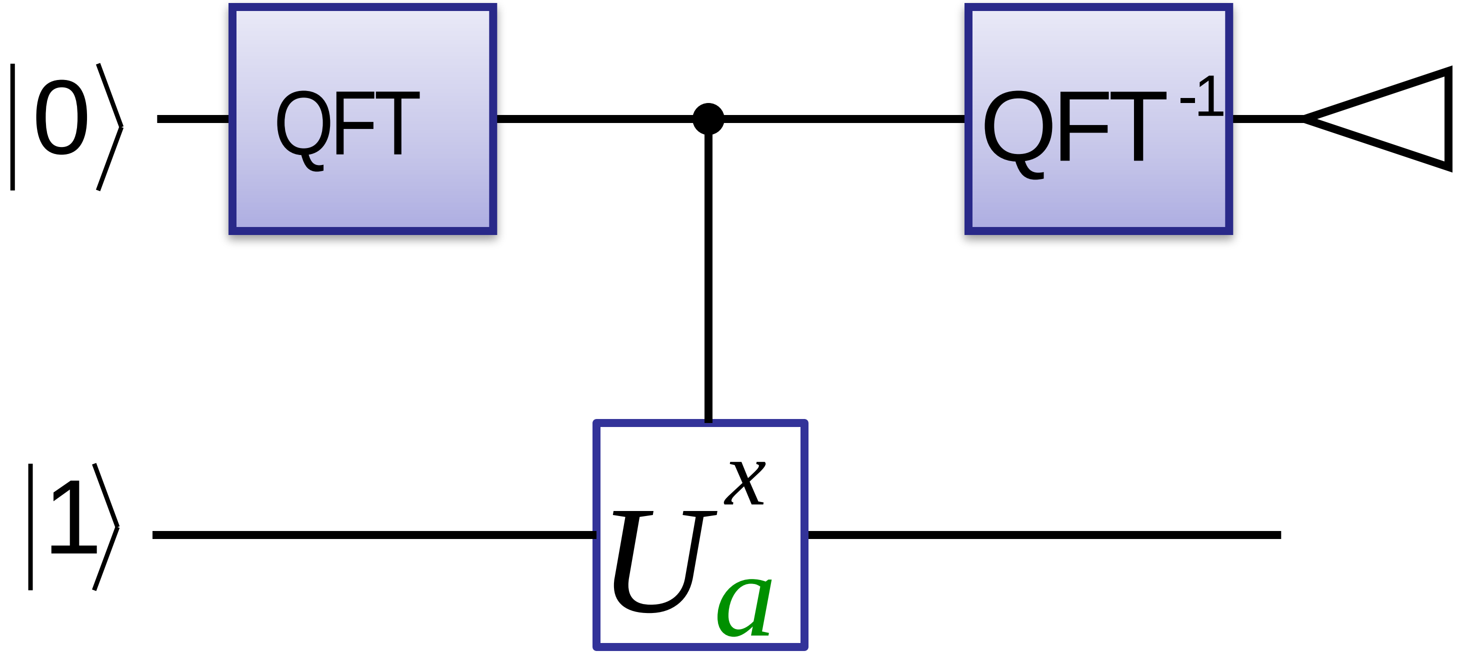
$$\mapsto \sum_{k=0}^{r-1}\sum_{x} e^{2\pi i k x/r}|x\rangle|\psi_k\rangle$$

$$\Rightarrow \sum_{k}\Bigg(\qquad \Bigg)|\psi_k\rangle$$



$$\frac{k}{r}$$

Circuit for Eigenvalue Estimation
Factoring Algorithm



Equivalence

$$\sum_{x} |x\rangle |1\rangle = \sum_{k=0}^{r-1} \sum_{x} |x\rangle |\psi_k\rangle$$

$$\sum_{b=0}^{r=1} \sum_{z} |b + zr\rangle |a^b\rangle = \sum_{k=0}^{r-1} \sum_{x} e^{2\pi ikx/r} |x\rangle |\psi_k\rangle$$

$$\sum_{b} \Big(\quad \Big) |a^b\rangle = \sum_{k} \Big(\quad \Big) |\psi_k\rangle$$