

Shor's Algorithm

- ✚ Equivalent Question of Factorization

- ✚ Quantum Parallelism

- ✚ Quantum Fourier Transformation

Equivalent Question of Factorization

$$n=ab, a? b?$$

$$\Leftrightarrow$$

For arbitrary x , $(x,n)=1$, what is r such that $x^r=1(\text{mod } n)$

Since

$$(x^{r/2})^2 = 1(\text{mod } n) \Leftrightarrow (x^{r/2} - 1)(x^{r/2} + 1) = 0 (\text{mod } n)$$

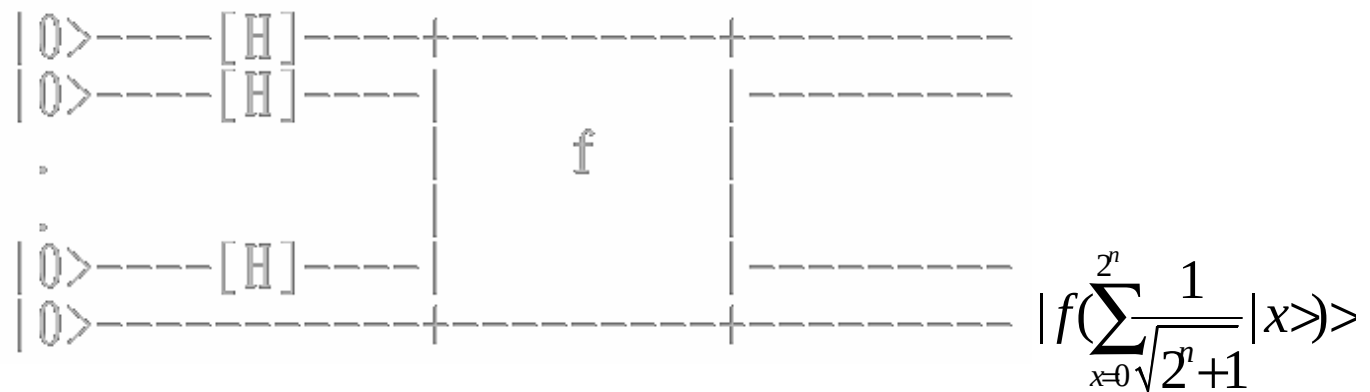
So, factor of n , say $a = \gcd(x^{r/2} - 1, n)$ or $\gcd(x^{r/2} + 1, n)$

Quantum Parallelism

f

If $|x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle,$

The circuit



can perform all possible calculation **at the same time** !

For example, a 2+1 qubits system:

$$\begin{aligned}
 & \hat{F}\hat{H}_2\hat{H}_1 |00\rangle \\
 &= \hat{F}\hat{H}_2 \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle |0\rangle \\
 &= \hat{F} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle \\
 &= \hat{F} \left(\frac{|00\rangle |0\rangle + |01\rangle |0\rangle + |10\rangle |0\rangle + |11\rangle |0\rangle}{2} \right) \\
 &= \frac{|00\rangle |f(00)\rangle + |01\rangle |f(01)\rangle + |10\rangle |f(10)\rangle + |11\rangle |f(11)\rangle}{2}
 \end{aligned}$$

This parallel design seems good, **but** ...

Quantum Fourier Transformation

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

can extract period information as the classical case.

Mechanism of QFT

(Assume $r|2^L$)

$$\sqrt{\frac{r}{2^L}} \sum_{j=0}^{2^L/r-1} |jr + \ell\rangle \longrightarrow \sum_{y=0}^{2^L-1} C_y |y\rangle$$

$$C_y = \frac{\sqrt{r}}{2^L} e^{2\pi i \ell y / 2^L} \left[\sum_{j=0}^{2^L/r-1} e^{2\pi i j r y / 2^L} \right] = \begin{cases} \frac{1}{\sqrt{r}} e^{2\pi i \ell y / 2^L}, & y = k \frac{2^L}{r} \\ 0, & \text{otherwise} \end{cases}$$

$$\Rightarrow |C_y|^2 = \begin{cases} \frac{1}{r}, & y = k \frac{2^L}{r} \\ 0, & \text{otherwise} \end{cases}$$

Shor's Algorithm

✚ Prepare the state for parallelism:

$$|y\rangle = |0\rangle|0\rangle \rightarrow |y'\rangle = \frac{1}{2^{L/2}} \sum_{x=0}^{2^L-1} |x\rangle|0\rangle \rightarrow |y''\rangle = \frac{1}{2^{L/2}} \sum_{x=0}^{2^L-1} |x\rangle|a^x \pmod n\rangle$$

✚ After measure the last bit: $|y_\ell\rangle = \frac{1}{\sqrt{2^L/r+1}} \sum_{j=0}^{2^L/r} |jr+\ell\rangle$

✚ By QFT, then measure: $|\tilde{y}\rangle = |k \frac{2^L}{r}\rangle$ appear with probability $1/r$ for $k=1,2,\dots,r$

✚ Repeat the above procedure

✚ Get r = the denominator of $\frac{\tilde{y}}{2^L}$ by continued fraction expansion

or r = the number of the peaks of measurement by direct counting.