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(mod n)

Since

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

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

Quantum Parallelism

If $|x\rangle|0\rangle \xrightarrow{\quad f \quad} |x\rangle|f(x)\rangle$,

The circuit

```
|0>----[H]----+----------+----------
|0>----[H]----|          |----------
 .            |    f     |
 .            |          |
|0>----[H]----|          |----------
|0>-----------+----------+----------
```

$$|f(\sum_{x=0}^{2^n}\frac{1}{\sqrt{2^n+1}}|x>)>$$

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

For example, a 2+1 qubits system:

$$\hat{F}\hat{H}_2\hat{H}_1 |00>$$
$$= \hat{F}\hat{H}_2(\frac{|0>+|1>}{\sqrt{2}})|0>|0>$$
$$= \hat{F}(\frac{|0>+|1>}{\sqrt{2}})(\frac{|0>+|1>}{\sqrt{2}})|0>$$
$$= \hat{F}(\frac{|00>|0>+|01>|0>+|10>|0>+|11>|0>}{2})$$
$$= \frac{|00>|f(00)>+|01>|f(01)>+|10>|f(10)>+|11>|f(11)>}{2}$$

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

Quantum Fourier Transformation

$$U_{QFT} \mid x >= \frac{1}{2^{L/2}} \sum_{y=0}^{2^L-1} e^{2p ixy/2^L} \mid y >$$

can extract period information as the classical case.

Mechanism of QFT

(Assume $r|2^L$)

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

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

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

Shor’s Algorithm

- Prepare the state for parallelism:

$$|y>=|0>|0> \;\longrightarrow\; |y'>=\frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x>|0> \;\longrightarrow\; |y''>=\frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x>|a^x(\mathrm{mod}\,n)>$$

- After measure the last bit: $|y_\ell>=\frac{1}{\sqrt{2^L/r+1}}\sum_{j=0}^{2^L/r}|jr+\ell>$
- By QFT, then measure: $|\tilde{y}>=|k\frac{2^L}{r}>$ appear with probability 1/r for k=1,2…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.