Shor's Algorithm – 1994

M – find prime factors  size problem $m = \lceil \log M \rceil$

classical alg. $O(e^{m^{1/3}})$

quantum alg. $O(m^3) \sim O(m^2 \log m \log\log m)$

Combined classical / quantum

↓ GCD
math operations

↳ period finding

$M$ $a$ — order of $a$ modulo $M$

$a^r \equiv 1 \bmod M$ $a, M$ relatively prime

$f(k) = a^k \bmod M$

$a^k = a^{k+r} \bmod M \rightarrow r$ is the period of $f(k)$

if $r$ is even,

$$\frac{(a^{r/2}+1)(a^{r/2}-1)}{a^r - 1} = 0 \bmod M$$

$a^r - 1$

$\uparrow$

1

1. choose arbitrary $a$ $\quad 0 < a < M$
   - make sure that $a$, $M$ rel. prime

2. Quantum : ~~find~~
   compute $f(x) = a^x \bmod M$ for $x = \{0, \cdots, 2^{n-1}\}$
   then QFT

   $M^2 \leq 2^n < 2M^2$

3. Measure :
   With high prob., a value $v$ close to mult. of $\frac{2^n}{r}$

4. Classically : guess of $q$ from $v$

5. $q$ is even : check if $(a^{q/2} + 1)$ has a factor in common with $M$

6. repeat if necessary

$\Downarrow$

a factor of $M$

$$f(x) = a^x \bmod M$$

$$U_f : |x\rangle_n |0\rangle_m \rightarrow |x\rangle_n |f(x)\rangle_m$$

superposition

$$\frac{1}{\sqrt{2^n}} \sum_{0}^{2^{n-1}} |x\rangle |f(x)\rangle$$

↓ measure

$$C \sum g(x) |x\rangle |u\rangle$$

$$g(x) = \begin{cases} 1, & \text{if } f(x) = u \\ 0, & \text{otherwise} \end{cases}$$

---

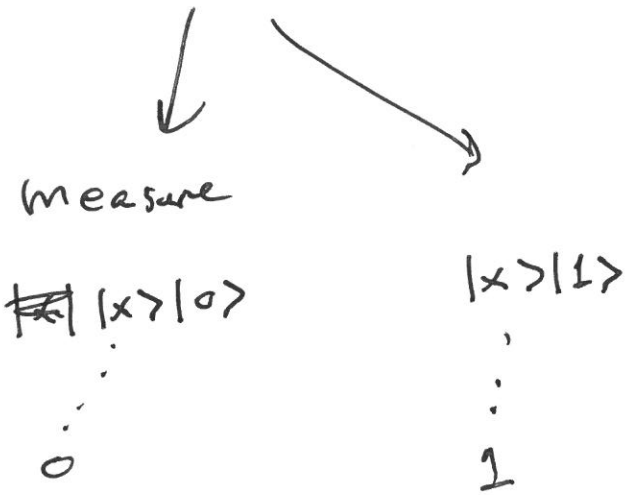
$$\sum |x\rangle |f(x)\rangle = \sum_{x \in X_0} |x\rangle |0\rangle + \sum_{x \in X_1} |x\rangle |1\rangle + \sum_{x \in X_2} |x\rangle |2\rangle + \dots$$

$$X_0 = \{x : f(x) = 0\}$$

$|00\rangle + |11\rangle$

~~$|x\rangle|f(x)\rangle$~~

$|x\rangle|f(x)\rangle$ $\quad f(x) = x$



$C \sum g(x)|x\rangle$

$QFT \longrightarrow C' \sum G(x)|x\rangle$

$\Downarrow$

measure $\longrightarrow$ $v$ close to multiple of $\frac{2^n}{r}$

$v = j\frac{2^n}{r}$ $\rightarrow$ usually $j, r$ rel. prime

then $\frac{v}{2^n}$ $\rightarrow$ reduce to lowest terms

$\frac{j}{r}$

Example $M = 21$

$$M^2 \leq 2^n < 2M^2$$

$441 \quad 512 \quad 882$

$n = 9$

$$\frac{1}{\sqrt{2^9}} \sum_{x=0}^{2^9-1} |x\rangle |f(x)\rangle$$

choose $a = 11$

suppose we measure $|f(x)\rangle \longrightarrow 8$

measure : $v = 427$

$q = 6$

$$\frac{v}{2^n} = \frac{427}{512} \approx \frac{5}{6}$$

$$a^{6/2} - 1 = 11^3 - 1 = 1330$$

$$a^{6/2} + 1 = 1332$$

$\gcd(21, 1330) = 7 \qquad \gcd(1332) = 3$