Shor's algorithm

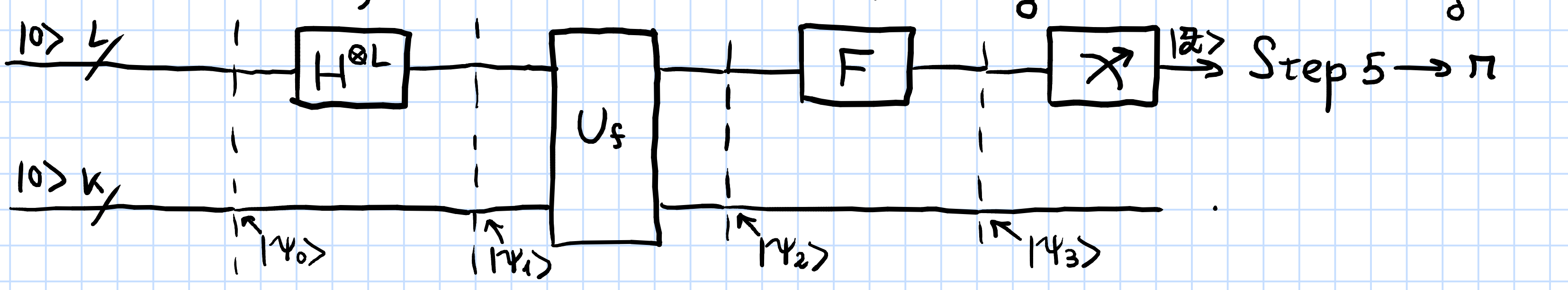
Problem: given $N = p\cdot q$, $p \neq q$ primes, find p and q.
Best classical algorithm (NFS) requires $O(\exp(c(\log N)^{1/3} \log\log N))$.
Shor's algorithm (1994) requires only $O((\log N)^3 \log\log N)$ of classical and quantum elementary operations using $O(\log N)$ qubits.
By comparison, to check whether $b | N$ for some $b < N$ requires $O(\log N)$ steps; to compute $\gcd(b,N)$ requires (by Euclid's algorithm) $O((\log N)^2)$ steps.
The output is random, so one can prove that $\forall \varepsilon(0,1)$ using $O(C_\varepsilon \log\log N (\log N)^3)$ steps we obtain the factors of $N = p\cdot q$ with probability $\geqslant 1-\varepsilon$.
Notice that we can always assume N odd.
Key idea: we reduce the factorization problem to that of determining the period r of a function $f: \mathbb{N} \to \mathbb{N}$.
The function f will be $f_{b,N}(m) = b^m \bmod N$, $f_{b,N}: \mathbb{N} \to \{0,1,\dots,N-1\}$ for some $b<N$. The period of $f_{b,N}$ is $r = \mathrm{ord}_N(b)$ (we need $\gcd(b,N)=1$). In a classical way, it requires $O(N)$ steps to find r.
Shor's algorithm requires $O((\log N)^3 \log\log N)$ quantum and classical steps to find r with probability $\geqslant 1-\varepsilon$.

Full Shor's algorithm

Input: N (with at least two distinct prime factors).
Output: two non-trivial factors of N.
Step 1 (selection of b): pick randomly $1<b<N$ and compute $\gcd(b,N)$. If it is >1, we're done; otherwise, go to Step 2.
Step 2: use a quantum routine to compute the period r of $f_{b,N}$. If r is odd, go back to Step 1; otherwise, go to Step 3.
Step 3: compute $\gcd(b^{r/2}+1, N)$. If it is $=N$, go back to Step 1; otherwise, we found a non-trivial factor: output $\gcd(b^{r/2}+1,N)$, $\gcd(b^{r/2}-1,N)$.
Why Step 3: we found $b^r \equiv 1 \bmod N \Rightarrow (b^{r/2}+1)(b^{r/2}-1) \equiv 0 \bmod N$, but $b^{r/2} \not\equiv 1 \bmod N$ because $r/2 < r = \mathrm{ord}_N(b)$, so $N | (b^{r/2}+1)(b^{r/2}-1)$ but $N \nmid b^{r/2}-1 \Rightarrow \gcd(b^{r/2}+1,N) > 1$.
Theorem (6.11 of the book): let $N = \prod_{j=1}^{J} p_j^{\nu_j}$, p_j different odd primes, $\nu_j \geqslant 1$.
Let $\Omega = \{c \in \{0,1,\dots,N-1\} \mid \gcd(c,N)=1\}$. We have:
- $\#\Omega = \phi(N)$; ϕ: Euler's totient function
- $\#\{b \in \mathbb{N} \mid \mathrm{ord}_N(b) = r \text{ is even and } N \nmid (b^{r/2}+1)\} \geqslant \phi(N)(1-1/2^{J-1})$.

Fact: $\exists c>0$ s.t. $\phi(m)/m \geqslant \frac{c}{\log\log m}$ for large m.
Let's focus on Step 2.
Problem: given $f: \mathbb{N} \to \mathbb{N}$ periodic with unknown period r, compute it assuming:
i) $L \geqslant 2$ s.t. $r < 2^{L/2}$ (in our case, $L = \lfloor 2\log_2 N \rfloor + 1$);
ii) $f|_{\{0,1,\dots,r-1\}}$ injective (in our case, ok) and $\exists K \geqslant 1$ s.t. $f(m) < 2^K$ (in our case, $K \approx \log N$);
iii) $U_f: \mathbb{H}^L \otimes \mathbb{H}^K \to \mathbb{H}^L \otimes \mathbb{H}^K$, $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$ is implemented using $O(L^c)$ elementary gates (in our case $f = f_{b,N}$ requires $O((\log N)^3)$ steps).

Then we can find the period r of f with probability at least $c'/\log L$ using $O(L^{\max\{c,3\}})$ elementary gates and classical elementary operations (where $c' = 1/10$ is a universal constant).
Remark: to find r with probability $\geqslant 1/2$, we repeat until we succeed; we need s trials s.t. $(1-c'/\log L)^s \leqslant 1/2 \Longrightarrow s \gtrsim \log L$.



Do the calculations $\rightsquigarrow z \in \{0,1,\dots,2^{L/2}-1\}$ with probability
$P(z) = (A_z)_{|\psi_3\rangle} = \| A_z |\psi_3\rangle \|^2$, $A_z = |z\rangle\langle z| \otimes \mathbb{1}_K$.

$$P(z) = \begin{cases} \frac{1}{2^{2L}} \sum_{k=0}^{r-1} (J_k+1)^2 & \text{if } \frac{zr}{2^L} \in \mathbb{N} \quad (J_k \text{ defined as needed}) \\ \text{monster} & \text{otherwise.} \end{cases}$$

In the first case, we have $P(z) \gtrsim \frac{1}{2^{2L}} \cdot r \left(\frac{2^L}{r}\right)^2 \approx \frac{1}{r}$.
Similarly, if z is s.t. $|zr/2^L - \ell| \overset{(*)}{\leqslant} \frac{r}{2\cdot 2^L}$ for some $\ell \in \mathbb{N}$, we have $P(z) \geqslant c/r$ for some constant $c>0$.
Step 5: from the theory of continued fractions

$$\frac{P}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}} = [a_0, a_1, \dots, a_m]$$

we have that if z is s.t. $(*)$ holds, then ℓ/r will be one among the numbers $\{[a_0,a_1,\dots,a_j]\}_{j=0}^{m}$ where $[a_0,a_1,\dots,a_m] = \frac{z}{2^L}$.
So r will be one of the denominators in this set provided that $\gcd(\ell, r) \overset{(**)}{=} 1$.
Lemma: $\sum_{z \text{ s.t. } (*),(**)} P(z) \geqslant \frac{C}{\log L}$.