Implementation of Shor's Algorithm

516030910587 Keda Shen

August 21, 2018

1 Lemma

First we prove that :

If $x^r\ mod\ n = 1(riseven)$ and $x^{r/2} \neq \pm 1\ mod\ n$, then we can factorize n.

Prove:

$$x^r\ mod\ n = 1$$

we have

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

Since $x^{r/2} \neq \pm 1\ mod\ n$, we have $gcd(x^{r/2}+1, n)$ is nontrivial factor of n, and we can factorize n.

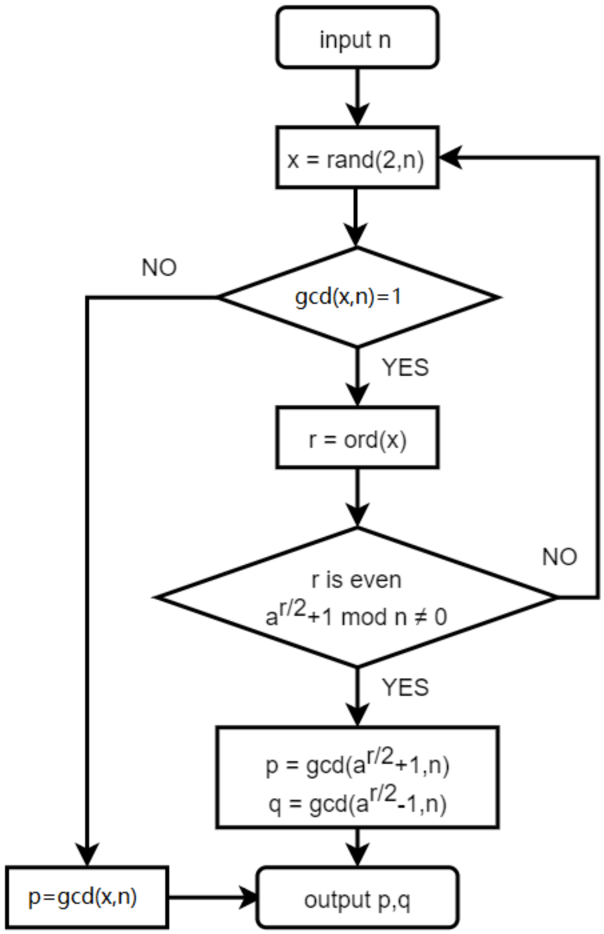
When n = pq(p and q are distrinct primes), for a random $x \in [2, n]$ we have

$$P(r\ mod\ 2 = 0, x^{r/2}+1 \neq 1\ mod\ n) \geq \frac{3}{4}$$

Repeat random x, we have large probability to find the factorization of n.

2 Shor's Algorithm

Here comes the Shor's Algorithm for n = pq:



3 Quantum Order Finding Algorithm

Now the only problem left is to efficiently find ord(x), and we can solve it by using quantum order finding algorithm.

It's just the phase estimation algorithm applied to the unitary operator

$$U|y\rangle \equiv |xy(modN)\rangle$$

where $y \in \{0,1\}^L$.Hence the eigensates of U is

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} exp\left[\frac{-2\pi isk}{r}\right]|x^k \ mod \ N\rangle$$

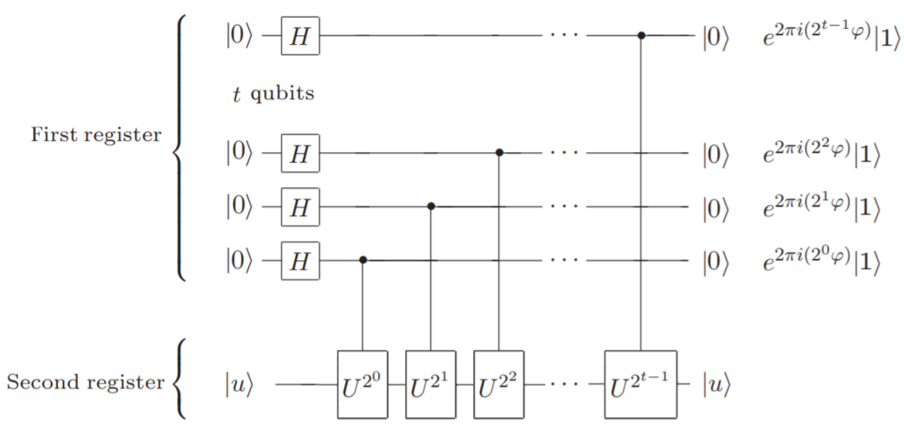
While preparing $|u_s\rangle$ requires we know r, we can circumvent the problem by using that

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

In performing the phase estimation procedure, use $t = 2L+1+\left[log(2+\frac{1}{2\epsilon})\right]$ qubits in the first register,prepare the second register in the state $|1\rangle$, and we will obtain an estimate of the phase $\phi \approx s/r$ accurate to $2L+1$ bits, with probability at least $(1-\epsilon)/r$.

3.1 Phase Estimation

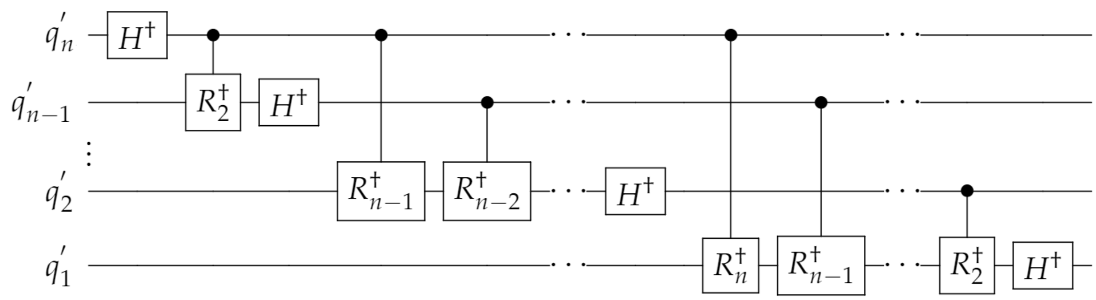
The first stage of the phase estimation procedure:



The second stage of phase estimation is to apply the inverse quantum Fourier transform on the first register.

3.2 Inverse Quantum Fourier Transform

Just the inverse of QFT.



Where $q_1, q_2, ..., q_n$ are output from first stage and The gate R_k denotes the same transformation as in Quantum Fourier Transform.

4 Test

Just test N = 15 with code in $Q^{\#}$, and succeed.