QIP Course 11: Quantum Factorization Algorithm (Part 4)

Ryutaroh Matsumoto

Nagoya University, Japan
Send your comments to ryutaroh.matsumoto@nagoya-u.jp

September 2017
@ Tokyo Tech.

Acknowledgment and Copyright

Answers to Previous Exercises

1. Let $N = 5 \times 7$ and $x = 8$. Compute $r = \mathrm{ord}(x, N)$.
$r = 4$.
2. Tell whether or not $x^{r/2} \bmod N \neq N - 1$.
$8^2 \bmod 35 = 29 \neq 34$.
3. Tell whether either $\gcd(x^{r/2} - 1 \bmod N, N)$ or $\gcd(x^{r/2} + 1 \bmod N, N)$ is a factor of N or not.
Yes, thay are factors. Explain how to compute the gcd by the Euclidean algorithm.
The final report will be similar to Q4–6. 4. Compute $|u_s\rangle$ with above values and $s = 1$.

$$\frac{1}{\sqrt{4}} \sum_{k=0}^{3} \exp(-\pi i \frac{k}{2}) |8^k \bmod 35\rangle \quad = \quad \frac{1}{2}(|1\rangle - i|8\rangle + (-1)|29\rangle + i|22\rangle)$$

5. Let U be as defined in the lecture. With above x and N, what is the eigenvalue of U to which $|u_1\rangle$ belongs?
$\exp(\pi i/2) = i$.
6. Suppose that we execute the phase estimation procedure with the above U and $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$ with $t = 4$ qubits for recording the value of a phase s/r. There are $2^t = 16$ possible outcomes. Plot those 16 probabilities and observe that outcomes corresponding to s/r for $s = 0, \ldots, r-1$ have higher probabilities than the rest.
Read the hint given in the last unit. The quantum state immediately before the measurement in the phase estimation is

$$\sum_{s,s'} |v_s\rangle\langle v_{s'}| \otimes \frac{1}{r}|u_s\rangle\langle u_{s'}|,$$

whose partial trace is

$$\sum_{s,s'} |v_s\rangle\langle v_{s'}|\frac{1}{r} \underbrace{\mathrm{Tr}[|u_s\rangle\langle u_{s'}|]}_{=\delta_{s,s'}} = \frac{1}{r}\sum_{s=0}^{r-1} |v_s\rangle\langle v_s|,$$

which is the equal probabilistic mixture of $|v_0\rangle, \ldots, |v_{r-1}\rangle$.

Therefore, the probability of getting measurement outcome ℓ is $\frac{1}{r}\sum_{s=0}^{r-1}|\alpha_{s,\ell}|^2$, where $|v_s\rangle = \alpha_{s,0}|0\rangle + \alpha_{s,1}|1\rangle + \cdots + \alpha_{s,2^t-1}|2^t-1\rangle$, and

$$\begin{aligned}\alpha_{s,\ell} &= \frac{1}{2^t}\sum_{k=0}^{2^t-1}[\exp\left(2\pi i(\theta - \ell/2^t)\right)]^k \text{(by using Unit 9)} \\ &= \frac{1}{16}\sum_{k=0}^{15}[\exp(2\pi i(s/4 - \ell/16))]^k\end{aligned}$$

ℓ	probability
0	1/4
1	0
2	0
3	0
4	1/4
5	0
6	0
7	0

,

ℓ	probability
8	1/4
9	0
10	0
11	0
12	1/4
13	0
14	0
15	0

Observe that probabilities of ℓ near to $16s/4$ ($s = 0, \ldots, 3$) have larger values.

Continued fraction

r: the order of x' modulo N'.
We are given

$$x = 0.b_1 b_2 \ldots b_t$$

that is close to s/r with high probability. The remaining task is to compute r from $b_1 b_2 \ldots b_t$. r can be determined by the continued fraction algorithm.

A continued fraction is

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}, \tag{1}$$

where $a_1, \ldots, a_N$ are positive integers and $a_0 \geq 0$. Denote the value of Eq. (1) by $[a_0, a_1, \ldots, a_N]$.

Computation of a continued fraction

The representation of a continued fraction of rational x can be found, for example, as follows:

$$\begin{aligned}
\frac{31}{13} &= 2+\frac{5}{13} = 2+\frac{1}{\frac{13}{5}} \\
&= 2+\frac{1}{2+\frac{3}{5}} = 2+\frac{1}{2+\frac{1}{\frac{5}{3}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{2}{3}}} = 2+\frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}} \\
&= 2+\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}}
\end{aligned}$$

How to find the phase by the continued fraction

Recall that we have to find r from

$$x = 0.b_1 b_2 \dots b_t$$

such that x is close to s/r. We have the following theorem.
Theorem 1: Let $[a_0, \dots, a_N]$ be the continued fraction of x. If $|x - s/r| < \frac{1}{2r^2}$ and $\gcd(s, r) = 1$, then s/r is equal to $[a_0, \dots, a_n]$ for some $0 \leq n \leq N$.
Proof. Its proof is given in "Quantum Computation and Quantum Information," ISBN: 0521635039.

We can make $|x - s/r| < \frac{1}{2r^2}$ by increasing t (the number of qubits used for phase estimation). If we execute the order finding several times, we will eventually have $\gcd(s, r) = 1$. If we assume Theorem 1, the factorization can be found as follows: Compute the continued fraction of x as $[a_0, \dots, a_N]$. For each $0 \leq n \leq N$, write $[a_0, \dots, a_n]$ as p_n/q_n and check whether q_n satisfies that $(x')^{q_n} \bmod N' = 1$ and $\gcd(N', [(x')^{q_n/2} \pm 1])$ is a factor of N'. If it is the case, we found a factor of N'. Otherwise, try again.

Cost of continued fraction

Thus, if we assume Theorem 1, then what we have to do is to check the speed (required computational time) of continued fraction computation.

Theorem 2: Let $[a_0, \ldots, a_N]$ be the continued fraction of rational $x = p/q > 1$. Define $p_0 = a_0$, $q_0 = 1$, $p_1 = 1 + a_0 a_1$, $q_1 = a_1$,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

Then we have

$$\frac{p_n}{q_n} = [a_0, \ldots, a_n]$$

for $n = 0, \ldots, N$.

Its proof is given in "Quantum Computation and Quantum Information," ISBN: 0521635039.

From the above theorem we can evaluate the required number N of computational steps. Observe that $p_n > p_{n-1}$ and $q_n > q_{n-1}$. So we have $p_n \geq 2p_{n-2}$ and $q_n \geq 2q_{n-2}$. Therefore $N \leq 2 \log_2 \max\{p, q\}$.

Exercise (15 min.?)

Let $N' = 35$, $x' = 4$, and $x = 0.0010101 \simeq \frac{1}{6}$. This can be a measurement outcome of the phase estimation with $t = 7$.

1. Compute the continued fraction of x.
2. Let $[a_0, \ldots, a_N]$ be the continued fraction of x. Detemine an index n such that q_n is the order of x' modulo N', where $p_n/q_n = [a_0, \ldots, a_n]$.
3. Compute a factor of N' by using your answer to Q2.