QIP Course 10: Quantum Factorization Algorithm (Part 3)

Ryutaroh Matsumoto

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

September 2017
@ Tokyo Tech.

Acknowledgment and Copyright

Answers to the previous exercise

1. Let

$$U = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i 5/16) \end{pmatrix}$$

Find the all eigenvalues of U.
Answer: Obviously 1 and $\exp(2\pi i 5/16)$.
2. Let $|u\rangle$ be the eigenvector of U and assume $U|u\rangle \neq |u\rangle$. Assume that we do the phase estimation with $t = 3$. Then there are eight possible measurement outcomes. Compute the probability distiribution of outcomes. I recommend you to use Mathematica, Matlab, Maple, and so on.
Answer: By the formula, for $\ell = 0, \ldots, 7$, the coefficient of $|\ell\rangle$ after the IQFT is

$$\begin{aligned} \frac{1}{2^t}\sum_{k=0}^{2^t-1} \exp\left(\frac{-2\pi i k \ell}{2^t}\right)\exp(2\pi i k\theta) &= \frac{1}{2^t}\sum_{k=0}^{2^t-1} \exp(2\pi i k(\theta - \ell/2^t)) \\ &= \frac{1}{8}\sum_{k=0}^{7} \exp(2\pi i k(5-2\ell)/16) \end{aligned}$$

By cumbersome computation, we can see that the coefficients are

ℓ	squred norm of coefficient		$\lvert\ell - 2^t\theta\rvert > 3$
$-1 \equiv 7$	$\frac{1}{64}\left(1+\left(1+\sqrt{2}-2\cos\left(\frac{\pi}{8}\right)-2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.0162432	Yes
0	$\frac{1}{64}\left(1+\left(-1+\sqrt{2}-2\cos\left(\frac{\pi}{8}\right)+2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.022601	
1	$\frac{1}{64}\left(1+\left(-1+\sqrt{2}+2\cos\left(\frac{\pi}{8}\right)-2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.0506223	
$b = 2$	$\frac{1}{64}\left(1+\left(1+\sqrt{2}+2\cos\left(\frac{\pi}{8}\right)+2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.410533	
$2^t\theta = 2.5$			
3	$\frac{1}{64}\left(1+\left(1+\sqrt{2}+2\cos\left(\frac{\pi}{8}\right)+2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.410533	
4	$\frac{1}{64}\left(1+\left(-1+\sqrt{2}+2\cos\left(\frac{\pi}{8}\right)-2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.0506223	
5	$\frac{1}{64}\left(1+\left(-1+\sqrt{2}-2\cos\left(\frac{\pi}{8}\right)+2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.022601	
6	$\frac{1}{64}\left(1+\left(1+\sqrt{2}-2\cos\left(\frac{\pi}{8}\right)-2\sin\left(\frac{\pi}{8}\right)\right)^2\right)$	0.0162432	Yes

Observe that $5/16$ is $0.\underbrace{010}_{=b}1$, which implies $b = 2$. The two nearest values $\ell = 2, 3$ to true θ have the highest probability.

3. By using $p(|m-b|>e) \leq \frac{1}{2(e-1)}$ compute the lower bound on the probability of the event that the mesurement outcome of θ is within 3/8 from the true value $\theta = 5/16$. How much difference exists between the lower bound and the true probability?
Answer: Since the required accuracy is 3/8, the measurement outcomes $0, 1, 2, 3, 4, 5$ have the desired accuracy. The true probability is roughly 0.968. In this case $b = 010 = 2$. We have to choose $e = 2$.

We have to choose $e = 2$, because (draw a figure on the black board)

- the acceptable measurement outcomes m are $0, 1, 2, 3, 4, 5$,
- $m = 6, 7$ should be included in the event $|m - b| > e$,
- $|m - b| > e$ is considered modulo 2^t,
- and e is an integer,

we have to choose $e = 2$. $p(|m - b| \leq e) \geq 1 - 1/2(e - 1) = 1 - 1/2 = 1/2$.
The difference between the true probability and its lower bound is $0.968 - 0.5 = 0.468$.

Factoring N

Suppose that we are given N. We assume that N is odd, and is NOT a prime power. It can be checked by seeing if $\sqrt[i]{N}$ is an integer for some $i \leq \log_3 N$. In order to break the RSA, we need this kind of computation.
Firstly randomly choose $2 \leq x \leq N-1$, and see if $\gcd(x, N) = 1$. If $\gcd > 1$, then we have gotten a nontrivial factor of N.
Otherwise, compute the order of x modulo N, that is

$$\mathrm{ord}(x, N) = \min\{i \geq 1 \mid x^i \bmod N = 1\}$$

If $\gcd(x, N) > 1$ then there is no i such that $x^i \bmod N = 1$. So we have to exclude this case first.

Overview of the factorization procedure

Factorization by the order finding given N:

1. Choose $1 \leq x \leq N-1$ randomly. If $\gcd(x, N) > 1$ then output gcd as a factor of N.
2. Compute $r = \mathrm{ord}(x, N)$ (order finding).
3. Check if r is even. If r is odd, then return to Step 1.
4. Compute $z = x^{r/2} \bmod N$.
5. Check if $z \equiv -1 \pmod{N}$. If true, then return to Step 1. By Theorem 1, Step 1 is repeated more than once with a probability at most 1/4.
6. As a factor of N output $\gcd(z+1, N)$ if $\gcd(z+1, N) \neq 1$, otherwise output $\gcd(z-1, N)(\neq 1)$. Theorem 2 ensures that the output is a factor.

Supporting theorems

Theorem 1 Choose an integer x uniformly at random such that $\gcd(x, N) = 1$ and $1 \leq x \leq N-1$, define $r = \mathrm{ord}(x, N)$. Then the probability of the event that r is even that and $x^{r/2} \bmod N \neq N-1$ is $\geq 3/4$.

Proof. Omitted. You can find a proof in "Quantum Computation and Quantum Information," ISBN: 0521635039.

Assume that r is even and $x^{r/2} \bmod N \neq N-1$. Otherwise choose x again until the above condition is satisfied.

Theorem 2 Let z be an integer such that $2 \leq z \leq N-2$ and $z^2 \bmod N = 1$. Then at least one of $\gcd(z+1, N)$ or $\gcd(z-1, N)$ is greater than 1 and divides N.

Proof. Omitted. You can find a proof in "Quantum Computation and Quantum Information," ISBN: 0521635039.

Thus, $\gcd(x^{r/2} + 1 \bmod N, N)$ or $\gcd(x^{r/2} - 1 \bmod N, N)$ is a factor of N.

Computing the order of x modulo N

There is no known fast algorithm for computing the order of x modulo N **by digital computers**. I will introduce a fast quantum algorithm.
Let $2^{L-1} \leq N \leq 2^L - 1$ and $0 \leq y \leq 2^L - 1$, define the unitary operator U such that

$$U|y\rangle = |xy \bmod N\rangle.$$

We define $xy \bmod N = y$ if $N \leq y \leq 2^L - 1$. The order of x modulo N is related to the phase of eigenvalues of U as follows.

Recall $r = \mathrm{ord}(x, N)$. For $0 \leq s \leq r-1$, define the L-qubit quantum state

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \bmod N\rangle.$$

Then we have

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) U|x^k \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^{k+1} \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \exp\left(\frac{-2\pi i s (k-1)}{r}\right) |x^k \bmod N\rangle \\ &= \exp\left(\frac{2\pi i s}{r}\right) \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \bmod N\rangle \end{aligned}$$

$$
\begin{aligned}
U|u_s\rangle &= \exp\left(\frac{2\pi i s}{r}\right)\frac{1}{\sqrt{r}}\sum_{k=1}^{r}\exp\left(\frac{-2\pi i s k}{r}\right)|x^k \bmod N\rangle \\
&= \exp\left(\frac{2\pi i s}{r}\right)\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(\frac{-2\pi i s k}{r}\right)|x^k \bmod N\rangle \\
&= \exp\left(\frac{2\pi i s}{r}\right)|u_s\rangle
\end{aligned}
$$

If we could estimate the phase of the eigenvalue of $|u_s\rangle$, we would know s/r. From which we could know r. The obstacle is that the preparation of $|u_s\rangle$ requires the knowledge of r. Let us see how we can bypass this difficulty.

Preparation for eigenvectors

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{s=0}^{r-1}\exp\left(\frac{-2\pi isk}{r}\right)\right)|x^k \bmod N\rangle \tag{1}$$

We can show that

$$\sum_{s=0}^{r-1}\exp\left(\frac{-2\pi isk}{r}\right) = r\delta_{k0}. \tag{2}$$

Its proof is given in the Appendix of handout.
Substitution of Eq. (2) into Eq. (1) gives

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |x^0 \bmod N\rangle = |1\rangle = |0\rangle\otimes|0\rangle\otimes\cdots\otimes|0\rangle\otimes|1\rangle.$$

Useful shape of probability distribution of measurement outcomes

If we use the phase estimation algorithm with $|1\rangle$, then we get outcomes near to s/r with probability $1/r$ for $s = 0, ..., r-1$ (Draw a figure here. You are requested to draw a similar figure in Question 6.).
In the next lecture, I will show that how to compute r from a binary fractional ditits $0.b_1 b_2 \ldots b_t$ that is close to s/r for some unknown $0 \leq s \leq r-1$.

Exercise

1. Let $N = 5 \times 7$ and $x = 8$. Compute $r = \mathrm{ord}(x, N)$.
2. Tell whether or not $x^{r/2} \bmod N \neq N - 1$.
3. Tell whether either $\gcd(N, x^{r/2} - 1 \bmod N)$ or $\gcd(N, x^{r/2} + 1 \bmod N)$ is a factor of N or not.
4. Compute $|u_s\rangle$ with above values and $s = 1$.
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?
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 $s = 0, ..., r - 1$ have higher probabilities than the rest.

The final report will be similar to Q4–6.

Hint for Q6

In order to find the probability distribution of outcomes of phase estimation, we need to calculate the quantum state immediately before the measurement in the phase estimation.
Let $|v_s\rangle$ be the quantum state before measurement when the input state to the phase estimation is $|u_s\rangle$ as visualized below:

$$\begin{matrix} (|0\rangle + |1\rangle)^{\otimes t} \\ \otimes \\ |u_s\rangle \end{matrix} \rightarrow \boxed{\text{unitary manipulation in phase estimation}} \rightarrow \begin{matrix} |v_s\rangle \\ \otimes \\ |u_s\rangle \end{matrix} \rightarrow \boxed{\text{measurement of } |v_s\rangle \text{ in phase estimation}}$$

Because the input state to the phase estimation is $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$, we have

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \begin{array}{c} (|0\rangle + |1\rangle)^{\otimes t} \\ \otimes \\ |u_s\rangle \end{array} \rightarrow \boxed{\text{unitary manipulation in phase estimation}} \rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \begin{array}{c} |v_s\rangle \\ \otimes \\ |u_s\rangle \end{array} \rightarrow \boxed{\text{measurement of } |v_s\rangle \text{ in phase estimation}}$$

For each $s = 0, ..., r-1$, we compute $|v_s\rangle$. Since we use $t = 4$ qubits for the phase estimation, We express $|v_s\rangle$ as a linear combination of $|0\rangle, ..., |15\rangle$. Let $\alpha_{s,\ell}$ be $|v_s\rangle$'s complex coefficient of $|\ell\rangle$, i.e.,

$$|v_s\rangle = \sum_{\ell=0}^{15} \alpha_{s,\ell} |\ell\rangle.$$

By Unit 9, recall that $\alpha_{s,\ell}$ is given by

$$\frac{1}{2^t}\sum_{k=0}^{2^t-1}[\exp\left(2\pi i(\theta-\ell/2^t)\right)]^k. \tag{3}$$

Warning: Some students assumed the input-output relation between $|u_s\rangle$ and $|v_s\rangle$ is **linear**. But it is not clear. $|u_s\rangle$ has $6=\lceil\log_2 35\rceil$ qubits while $|v_s\rangle$ has $4=t$ qubits. Their relation cannot be unitary, which suggests it is not linear either.

Thus, when the input is a linear combination of $|u_s\rangle$, the output cannot be assumed as a **linear combination of $|v_s\rangle$ without a justifying explanation.**

The phase estimation measures $|v_s\rangle$ and does not measure $|u_s\rangle$. To compute the probability distribution of the measurement outcomes, we need to compute the partial trace over the quantum system containing $|v_s\rangle$, and remove $|u_s\rangle$ from the quantum state. Firstly, the vector representation of output is

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

Its matrix representation is

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

whose partial trace is ...(please do the rest by yourself). Please verify whether the total of the probabilities is 1.

Appendix: Proof of Eq. (2)

Let $1 \le k \le r-1$. Consider the sequence $0k \bmod r$, $k \bmod r$, $2k \bmod r$, ... Define $d = \min\{j \ge 1 \mid jk \bmod r = 0\}$. d must divide r otherwise $rk \bmod r$ would not be zero. Moreover, $jk \bmod r = (j+d)k \bmod r$. Therefore,

$$\sum_{s=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) = \frac{r}{d} \sum_{s=0}^{d-1} \exp\left(\frac{-2\pi i s k}{r}\right)$$

On the other hand, if $0 \le j \ne j' \le d-1$ then $jk \bmod r \ne j'k \bmod r$, otherwise $(j-j')k \bmod r = 0$, which is a contradiction to the minimality of d. This means that

$$\exp\left(\frac{-2\pi i 0k}{r}\right), \exp\left(\frac{-2\pi i 1k}{r}\right), \ldots, \exp\left(\frac{-2\pi i (d-1)k}{r}\right)$$

are pairwise distinct roots of $X^d - 1 = 0$.

$$
\begin{aligned}
X^d - 1 &= \prod_{s=0}^{d-1}\left(X - \exp\left(\frac{-2\pi i s k}{r}\right)\right) \\
&= X^d + \sum_{s=0}^{d-1} \exp\left(\frac{-2\pi i s k}{r}\right) X^{d-1} + \cdots - 1.
\end{aligned}
$$

This means that

$$
\sum_{s=0}^{d-1} \exp\left(\frac{-2\pi i s k}{r}\right) = 0.
$$