QIP Course 9: Quantum Factorization Algorithm (Part 2)

Ryutaroh Matsumoto

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

September 2018
@ Tokyo Tech.

Acknowledgment and Copyright

Inverse QFT

Answers to the previous exercises will be given on the blackboard.

Let $|0\rangle, \ldots, |N-1\rangle$ be an orthonormal basis of an N-dimensional space. The QFT transforms

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi i jk/N)|k\rangle.$$

The inverse of QFT (IQFT) is given by

$$|k\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} \exp(-2\pi i k\ell/N)|\ell\rangle. \tag{1}$$

IQFT can be realized by applying R_k^{-1} and H^{-1} in the reverse order.
$\Rightarrow$ IQFT can also be realized with the same efficiency ($n(n+1)/2$ operations of R_k^{-1} and H^{-1}) as QFT.

Phase estimation 1

Suppose that we have a unitary matrix U and its eigenvector vector $|u\rangle$. Let $\exp(2\pi i\theta)$ be the eigenvalue to which $|u\rangle$ belongs to. We shall show how we can compute θ.
Assumption: We are able to do the controlled-U^{2^j} operation for any $j \geq 0$.
Suppose that we apply the controlled-U^{2^j} to $(|0\rangle + |1\rangle)|u\rangle$, with $|u\rangle$ being the target (we omit the normalizing factor $1/\sqrt{2}$). Then the result is

$$\begin{aligned} & |0\rangle|u\rangle + |1\rangle \otimes U^{2^j}|u\rangle \\ = \ & |0\rangle|u\rangle + |1\rangle \otimes \exp(2\pi i 2^j \theta)|u\rangle \\ = \ & (|0\rangle + \exp(2\pi i 2^j \theta)|1\rangle) \otimes |u\rangle \end{aligned}$$

Assume we have t qubits that are initialized to $(|0\rangle + |1\rangle)/\sqrt{2}$, and apply the controlled-U^{2^j} to the j-th qubit (the rightmost is the zero-th). The result is

$$\begin{aligned} & \frac{1}{2^{t/2}}(|0\rangle + \exp(2\pi i 2^{t-1}\theta)|1\rangle) \otimes \cdots \otimes (|0\rangle + \exp(2\pi i 2^{0}\theta)|1\rangle) \\ = \quad & \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} \exp(2\pi i k\theta)|k\rangle. \end{aligned} \tag{2}$$

Applying the IQFT (1) to (2) yields

$$\frac{1}{2^t} \sum_{\ell=0}^{2^t-1} \sum_{k=0}^{2^t-1} \exp\left(\frac{-2\pi i k\ell}{2^t}\right) \exp(2\pi i k\theta)|\ell\rangle.$$

Probability distribution of the measurement outcomes 1

$$\frac{1}{2^t}\sum_{\ell=0}^{2^t-1}\sum_{k=0}^{2^t-1}\exp\left(\frac{-2\pi ik\ell}{2^t}\right)\exp(2\pi ik\theta)|\ell\rangle.$$

We shall compute the probability distribution of the mesurement in the $\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^t - 1\rangle\}$ basis. (The observable is $\sum_{j=0}^{2^t-1} j|j\rangle\langle j|$.) Recall that $0 \le \theta < 1$, and we can write

$$\theta = 0.b_1 b_2 \cdots b_t b_{t+1} \cdots .$$

Let $b = b_1 b_2 \cdots b_t$. We have $0 \le b \le 2^t - 1$. b **is the nearest** t**-bit integer** $\le 2^t\theta$**. When** m **is the measurement outcome, we regard** $m/2^t$ **as our estimate of** θ**. I will explain that** $m \simeq 2^t\theta \simeq 2^t b$ **with large probability.**

$$\frac{1}{2^t}\sum_{\ell=0}^{2^t-1}\sum_{k=0}^{2^t-1}\exp\left(\frac{-2\pi i k\ell}{2^t}\right)\exp(2\pi i k\theta)|\ell\rangle.$$

Let α_c be the coefficient of $|(b+c) \bmod 2^t\rangle$ in the result of the IQFT (the above). We shall show that if c is large then $|\alpha_c|$ is small. Observe that the coefficient of $|\ell\rangle$ is

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

Substituting ℓ with $b+c$ we have

$$\alpha_c = \frac{1}{2^t}\sum_{k=0}^{2^t-1}[\exp\left(2\pi i(\theta-(b+c)/2^t)\right)]^k$$

$$\alpha_c = \frac{1}{2^t} \sum_{k=0}^{2^t-1} [\exp\left(2\pi i(\theta - (b+c)/2^t)\right)]^k$$

is the sum of a geometric series, so it is equal to

$$\alpha_c = \frac{1}{2^t} \cdot \frac{1 - \exp(2\pi i(2^t\theta - (b+c)))}{1 - \exp(2\pi i(\theta - (b+c)/2^t))}.$$

Define $\delta = \theta - b/2^t$, then

$$\alpha_c = \frac{1}{2^t} \cdot \frac{1 - \exp(2\pi i(2^t\delta - c))}{1 - \exp(2\pi i(\delta - c/2^t))}$$

We shall upper bound the probability of getting a measurement outcome m such that $|m - b| > e$. Observe $\Pr[m = b + c] = |\alpha_c|^2$.

We shall upper bound the probability of getting a measurement outcome m such that $|m-b|>e$. We have

$$p(|m-b|>e)=\sum_{-2^{t-1}<c\le -e-1,\, e+1\le c<2^{t-1}} |\alpha_c|^2.$$

Since $|1-\exp(ix)|\le 2$,

$$|\alpha_c|\le \frac{2}{2^t|1-\exp(2\pi i(\delta-c/2^t))|}.$$

We have $|1-\exp(ix)|\ge 2|x|/\pi$ for $-\pi\le x\le\pi$ and $-\pi\le 2\pi(\delta-c/2^t)\le\pi$, it follows

$$|\alpha_c|\le \frac{1}{2^{t+1}|\delta-c/2^t|}.$$

Therefore we have

$$\begin{aligned}
4p(|m-b|>e) &\leq \sum_{-2^{t-1}<c\leq -e-1} \frac{1}{(2^t\delta - c)^2} + \sum_{e+1\leq c<2^{t-1}} \frac{1}{(2^t\delta - c)^2} \\
&\leq \sum_{-2^{t-1}<c\leq -e-1} \frac{1}{c^2} + \sum_{e+1\leq c<2^{t-1}} \frac{1}{(c-1)^2} \\
&\leq 2\sum_{e\leq c<2^{t-1}-1} \frac{1}{c^2} \\
&\leq 2\int_{e-1}^{2^{t-1}-1} \frac{dc}{c^2} \\
&\leq 2\int_{e-1}^{\infty} \frac{dc}{c^2} \\
&= \frac{2}{(e-1)}.
\end{aligned}$$

Sufficiently many qubits ensure the accuracy with high probability

Suppose that we want an accuracy of 2^{-n}, that is, $|\theta - m/2^t| < 2^{-n}$.

$$\begin{aligned} & |\theta - m/2^t| < 2^{-n} \\ \Leftrightarrow \quad & |2^t\theta - m| < 2^{t-n} \\ \Leftarrow \quad & |b - m| < 2^{t-n} - 1. \end{aligned}$$

We can see that $e = 2^{t-n} - 1$ ensures the desired accuracy. The probability of the accuracy below 2^{-n} is $1/2(2^{t-n} - 2)$. In order for $1/2(2^{t-n} - 2) < \epsilon$, we need $t \geq n + \log_2(2 + 1/2\epsilon)$.

Exercise

1. Let

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

Find the all eigenvalues of U.
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 is eight possible measurement outcomes. Compute the probability distiribution of outcomes **and their corresponding estimates of θ.** I recommend you to use Mathematica, Matlab, Maple, and so on.
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?