QIP Course 8: Quantum Factorization Algorithm (Part 1)

Ryutaroh Matsumoto

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

September 2019
@ Tokyo Tech.

Acknowledgment and Copyright

Answers of prev. exercises

1. Prove Eq. (2).
Recall that
$\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$, and
$P^2 = P$ for a projection matrix P.

$$\mathrm{Tr}[P_i \rho P_i] = \mathrm{Tr}[P_i P_i \rho] = \mathrm{Tr}[P_i \rho].$$

2. Same.
Reason: After the measurement and obtaining the outcome i, the state vector is

$$\frac{P_i|\varphi\rangle}{||P_i|\varphi\rangle||}.$$

Its corresponding density matrix is

Its corresponding density matrix is

$$\frac{P_i|\varphi\rangle\langle\varphi|P_i^*}{||P_i|\varphi\rangle||^2} = \frac{P_i\rho P_i}{||P_i|\varphi\rangle||^2}$$

On the other hand,

$$\begin{aligned} ||P_i|\varphi\rangle||^2 &= \langle\varphi|P_i^* P_i|\varphi\rangle \\ &= \langle\varphi|P_i|\varphi\rangle \\ &= \mathrm{Tr}[P_i|\varphi\rangle\langle\varphi|] \\ &\quad \text{by an argument similar to Unit 6} \\ &= \mathrm{Tr}[P_i\rho]. \end{aligned}$$

Therefore, the state vector and the density matrix represent the same physical state.
4. Explain why Eq. (3) is not linear.
See `http://en.wikipedia.org/wiki/No_cloning_theorem`

5. Verify Eq. (**??**) is a density matrix.
6. Verify the claim at the bottom of p.**??**.
7. Compute a purification of the density matrix $\begin{pmatrix} 9/25 & 0 \\ 0 & 16/25 \end{pmatrix}$. Then compute the partial trace of your answer, and see if the original density matrix is restored.

Quantum Fourier transform

I will explain the quantum factoring algorithm that computes the pairs (p_i, e_i) from a given composit number $p_1^{e_1} \cdots p_m^{e_m}$, where p_i's are pairwise distinct prime numbers and e_i is a positive integer. An important ingredient of the quantum factoring is the quantum Fourier transform, on which I will concentrate in this unit.

Discrete Fourier transform (in Conventional Computing)

---

transforms $(x_0, ..., x_{N-1}) \in \mathbf{C}^N$ to $(y_0, ..., y_{N-1}) \in \mathbf{C}^N$, where

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp(2\pi i jk/N). \tag{1}$$

Quantum Fourier transform (QFT):

Let $\{|0\rangle, ..., |N-1\rangle\}$ be an orthonormal basis of $\mathbf{C}^N$. QFT transforms

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

This means that QFT transforms

$$x_0|0\rangle + x_1|1\rangle + \cdots + x_{N-1}|N-1\rangle$$

into

$$y_0|0\rangle + y_1|1\rangle + \cdots + y_{N-1}|N-1\rangle,$$

where y_k is the same as DFT (Eq. (1)).

How the efficiency of QFT is claimed

I will show that QFT can be realized by a combination of unitary operators acting on one or two qubits. Recall that we cannot assume that any unitary operator can be realized in quantum computation, otherwise we become unable to discuss the computational complexity of quantum algorithms.

Quantum Fourier transform 2

Hereafter we assume $N = 2^n$. Define $j_1 j_2 \ldots j_n . j_\ell j_{\ell+1} \ldots j_m$ to be

$$j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n + j_\ell/2 + j_{\ell+1}/4 + \cdots + j_m/2^{m-\ell+1},$$

where j_i is either 0 or 1. Fix $0 \le j < 2^n$. We introduce a useful representation of QFT.

$$\begin{aligned}
& |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle = |j\rangle && (3)\\
\mapsto\ & \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \exp(2\pi i jk/2^n)|k\rangle && (4)\\
=\ & \frac{1}{2^{n/2}} \sum_{k_1=0,1} \cdots \sum_{k_n=0,1} \exp\left(2\pi i j \sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right) |k_1 k_2 \ldots k_n\rangle && (5)\\
=\ & \frac{1}{2^{n/2}} \sum_{k_1=0,1} \cdots \sum_{k_n=0,1} \bigotimes_{\ell=1}^{n} \exp(2\pi i j k_\ell 2^{-\ell})|k_\ell\rangle && (6)
\end{aligned}$$

$$
\begin{aligned}
& \frac{1}{2^{n/2}} \sum_{k_1=0,1} \cdots \sum_{k_n=0,1} \bigotimes_{\ell=1}^{n} \exp(2\pi i j k_\ell 2^{-\ell}) |k_\ell\rangle & (7) \\
= \; & \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left(\sum_{k_\ell=0,1} \exp(2\pi i j k_\ell 2^{-\ell}) |k_\ell\rangle \right) & (8) \\
= \; & \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + \exp(2\pi i j 2^{-\ell}) |1\rangle \right) & (9) \\
= \; & \frac{1}{2^{n/2}} (|0\rangle + \exp(2\pi i 0.j_n)|1\rangle) \otimes (|0\rangle + \exp(2\pi i 0.j_{n-1} j_n)|1\rangle) \otimes \\
& \cdots \otimes (|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle) & (10)
\end{aligned}
$$

The last equality may needs further explanation.

$$
\begin{aligned}
\exp(2\pi i j 2^{-\ell}) &= \exp(2\pi i (j_1 j_2 \cdots j_n) 2^{-\ell}) & (11) \\
&= \exp(2\pi i (j_1 j_2 \cdots j_{n-\ell} . j_{n-\ell+1} \cdots j_n)) & (12) \\
&= \exp(2\pi i (j_1 j_2 \cdots j_{n-\ell})) \cdot \exp(2\pi i (0.j_{n-\ell+1} \cdots j_n)) & (13) \\
&= 1 \cdot \exp(2\pi i (0.j_{n-\ell+1} \cdots j_n)) & (14)
\end{aligned}
$$

Quantum Fourier transform 3

In summary, QFT transforms

$$|j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$$

into

$$2^{-n/2}(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle) \otimes \cdots \otimes (|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle). \quad (15)$$

This equivalent representation of the QFT allows us to find an efficient implementation of the QFT. Define the unitary operator R_k by

$$|0\rangle \mapsto |0\rangle, \quad |1\rangle \mapsto \exp(2\pi i/2^k)|1\rangle,$$

and the controlled-R_k by

$$|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |10\rangle, |11\rangle \mapsto \exp(2\pi i/2^k)|11\rangle.$$

The controlled-R_k applies R_k to the first qubit iff the second qubit is 1. Observe that the effect by R_k is symmetric on the first and the second qubits.

Quantum Fourier transform 3

$$|j_1\rangle|j_2\rangle\cdots|j_n\rangle \mapsto$$
$$2^{-n/2}(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle)\cdots(|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle).$$

We shall show that n operations can produce $|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle$ in the first qubit. Recall that $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

1-1. Apply H to the first qubit, which changes the first qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_1}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_1)|1\rangle),$$

while keeping other qubits unchanged.

1-2. Apply the controlled-R_2 to the first and the second qubit, which changes the first qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_1 j_2)|1\rangle),$$

while keeping other qubits unchanged.

1-3. Apply the controlled-R_3 to the first and the third qubit, which changes the first qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_1 j_2 j_3)|1\rangle),$$

while keeping other qubits unchanged.

$$\vdots$$

1-n. Apply the controlled-R_n to the first and the n-th qubit, which changes the first qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_1 j_2 \dots j_n)|1\rangle),$$

while keeping other qubits unchanged.

Quantum Fourier transform 4

$$|j_1\rangle|j_2\rangle\cdots|j_n\rangle \mapsto$$
$$(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle)\cdots(|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle).$$

We shall show that $n-1$ operations can produce $|0\rangle + \exp(2\pi i 0.j_2 \cdots j_n)|1\rangle$ in the second qubit. After finishing the operations in the previous page, the quantum state is

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_1 j_2 \ldots j_n)|1\rangle) \otimes |j_2 j_3 \ldots j_n\rangle.$$

2-1. Apply H to the second qubit, which changes the second qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_2}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_2)|1\rangle),$$

while keeping other qubits unchanged.
2-2. Apply the controlled-R_2 to the second and the third qubit, which changes the second qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_2 j_3)|1\rangle)$$

2-3. Apply the controlled-R_3 to the second and the forth qubit, which changes the second qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_2 j_3 j_4)|1\rangle),$$

while keeping other qubits unchanged.

$$\vdots$$

2-$(n-1)$. Apply the controlled-R_{n-1} to the second and the n-th qubit, which changes the first qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_2 j_3 \ldots j_n)|1\rangle),$$

while keeping other qubits unchanged.

Quantum Fourier transform 5

$$|j_1\rangle|j_2\rangle\cdots|j_n\rangle \mapsto$$
$$(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle)\cdots(|0\rangle + \exp(2\pi i 0.j_1 j_2 \cdots j_n)|1\rangle).$$

We shall show that single operation can produce $|0\rangle + \exp(2\pi i 0.j_n)|1\rangle$ in the n-th qubit. After finishing the operations in the previous pages on the first to the $(n-1)$-th qubits, the quantum state is
$\frac{1}{2^{(n-1)/2}}(|0\rangle + \exp(2\pi i 0.j_1 j_2 \dots j_n)|1\rangle)\,(|0\rangle + \exp(2\pi i 0.j_2 j_3 \dots j_n)|1\rangle)\cdots$
$(|0\rangle + \exp(2\pi i 0.j_{n-1} j_n)|1\rangle) \otimes |j_n\rangle$.
n-1. Apply H to the n-th qubit, which changes the n-th qubit to

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_n}) = \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle),$$

while keeping other qubits unchanged.

Now the quantum state of the whole n qubits is
$\frac{1}{2^{n/2}}\left(|0\rangle + \exp(2\pi i 0.j_1 j_2 \dots j_n)|1\rangle\right)\left(|0\rangle + \exp(2\pi i 0.j_2 j_3 \dots j_n)|1\rangle\right)\cdots$
$\left(|0\rangle + \exp(2\pi i 0.j_{n-1} j_n)|1\rangle\right)\left(|0\rangle + \exp(2\pi i 0.j_n)|1\rangle\right)$,
which is the result of QFT in the reverse order of qubits.
Observe that the number of operations is $n(n+1)/2$.

Universal quantum operations

Any classical computation can be realized by the AND, OR, NOT gates, and the computational complexity can be measured as the number of necessary gates.
QFT uses the n kinds of unitary operations instead of a fixed set of operations. This makes the couting of computational steps unfair.
It is known that any controlled-U operation can be approximated by about $[\log(1/\epsilon)]^2$ operations in some fixed set of operations, where ϵ is the accuracy of approximation V_1 with a given unitary matrix V_2 defined by

$$\max_{|\varphi\rangle} \| V_1 |\varphi\rangle - V_2 |\varphi\rangle \|.$$

Therefore, the degree of computational complexity of QFT on n qubits is roughly proportional to $n(n+1)/2$.

Exercise

Let $N = 8$ and $n = 3$.
1. Compute the QFT in Eq. (2) with $j = 3$.
2. Compute the QFT in Eq. (15) with $j_1 = 0$, $j_2 = 1$, $j_3 = 1$.
3. Compute the QFT by using H, the controlled-R_2 and the controlled-R_3 with $j_1 = 0$, $j_2 = 1$, $j_3 = 1$. (Optional: computation is too complicated).
4. Compare the above results.