## QIP Course 8: Quantum Factorization Algorithm (Part 1)

Ryutaroh Matsumoto

Nagoya University, Japan
Send your comments to ryutaroh.matsumoto@nagoya-u.jp
September 2017
@ Tokyo Tech.

## Acknowledgment and Copyright

Materials presented here can by reused under the Creative Commons Attribution 40 International License https://creativecommons.org/licenses/by/4.o

## Answers of prev. exercises

1. Prove Eq. (2).

Recall that
$\operatorname{Tr}[A B]=\operatorname{Tr}[B A]$, and
$P^{2}=P$ for a projection matrix $P$.

$$
\operatorname{Tr}\left[P_{i} \rho P_{i}\right]=\operatorname{Tr}\left[P_{i} P_{i} \rho\right]=\operatorname{Tr}\left[P_{i} \rho\right]
$$

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,

$$
\begin{aligned}
\| P_{i}|\varphi\rangle \|^{2} & =\langle\varphi| P_{i}^{*} P_{i}|\varphi\rangle \\
& =\langle\varphi| P_{i}|\varphi\rangle \\
= & \operatorname{Tr}\left[P_{i}|\varphi\rangle\langle\varphi|\right] \\
& \text { by an argument similar to Unit } 6 \\
& =\operatorname{Tr}\left[P_{i} \rho\right] .
\end{aligned}
$$

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/Noncioning theorem
5. Verify Eq.
6. Verify the claim at the bottom of p.??.
7. Compute a purification of the density matrix $\left(\begin{array}{cc}9 / 25 & 0 \\ 0 & 16 / 25\end{array}\right)$. 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 $\left(p_{i}, e_{i}\right)$ 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 inqredient of the quantum factoring is the quantum Fourier transform, on which I will concentrate in this unit.
Discrete Fourier transform (in Conventional Computing)
transforms $\left(x_{0}, \ldots, x_{N-1}\right) \in \mathbf{C}^{N}$ to $\left(y_{0}, \ldots, y_{N-1}\right) \in \mathbf{C}^{N}$, where

$$
\begin{equation*}
y_{k}=\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_{j} \exp (2 \pi i j k / N) \tag{1}
\end{equation*}
$$

Quantum Fourier transform (QFT):
Let $\{|0\rangle, \ldots,|N-1\rangle\}$ be an orthonormal basis of $\mathbf{C}^{N}$. QFT transforms

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

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.

## 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 $0 \leq j<2^{n}$. We introduce a useful representation of QFT.

$$
\begin{align*}
& \left|j_{1}\right\rangle \otimes\left|j_{2}\right\rangle \otimes \cdots \otimes\left|j_{n}\right\rangle=|j\rangle  \tag{3}\\
\mapsto & \frac{1}{2^{n / 2}} \sum_{k=0}^{2^{n}-1} \exp \left(2 \pi i j k / 2^{n}\right)|k\rangle  \tag{4}\\
= & \frac{1}{2^{n / 2}} \sum_{k_{1}=0,1} \cdots \sum_{k_{n}=0,1} \exp \left(2 \pi i j \sum_{\ell=1}^{n} k_{\ell} 2^{-\ell}\right)\left|k_{1} k_{2} \ldots k_{n}\right\rangle  \tag{5}\\
= & \frac{1}{2^{n / 2}} \sum_{k_{1}=0,1} \cdots \sum_{k_{n}=0,1} \bigotimes_{\ell=1}^{n} \exp \left(2 \pi i j k_{\ell} 2^{-\ell}\right)\left|k_{\ell}\right\rangle \tag{6}
\end{align*}
$$

$$
\begin{align*}
& \frac{1}{2^{n / 2}} \sum_{k_{1}=0,1} \cdots \sum_{k_{n}=0,1} \bigotimes_{\ell=1}^{n} \exp \left(2 \pi i j k_{\ell} 2^{-\ell}\right)\left|k_{\ell}\right\rangle  \tag{7}\\
= & \frac{1}{2^{n / 2}} \bigotimes_{\ell=1}^{n}\left(\sum_{k_{\ell}=0,1} \exp \left(2 \pi i j k_{\ell} 2^{-\ell}\right)\left|k_{\ell}\right\rangle\right)  \tag{8}\\
= & \frac{1}{2^{n / 2}} \bigotimes_{\ell=1}^{n}\left(|0\rangle+\exp \left(2 \pi i j 2^{-\ell}\right)|1\rangle\right)  \tag{9}\\
= & \frac{1}{2^{n / 2}}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{n}\right)|1\rangle\right) \otimes\left(|0\rangle+\exp \left(2 \pi i 0 . j_{n-1} j_{n}\right)|1\rangle\right) \otimes \\
& \cdots \otimes\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \cdots j_{n}\right)|1\rangle\right) \tag{10}
\end{align*}
$$

The last equality may needs further explanation.

$$
\begin{align*}
\exp \left(2 \pi i j 2^{-\ell}\right) & =\exp \left(2 \pi i\left(j_{1} j_{2} \cdots j_{n}\right) 2^{-\ell}\right)  \tag{11}\\
& =\exp \left(2 \pi i\left(j_{1} j_{2} \cdots j_{n-\ell} \cdot j_{n-\ell+1} \cdots j_{n}\right)\right)  \tag{12}\\
& =\exp \left(2 \pi i\left(j_{1} j_{2} \cdots j_{n-\ell}\right)\right) \cdot \exp \left(2 \pi i\left(0 . j_{n-\ell+1} \cdots j_{n}\right)\right)  \tag{13}\\
& =1 \cdot \exp \left(2 \pi i\left(0 . j_{n-\ell+1} \cdots j_{n}\right)\right) \tag{14}
\end{align*}
$$

## Quantum Fourier transform 3

In summary, QFT transforms

$$
\left|j_{1}\right\rangle \otimes\left|j_{2}\right\rangle \otimes \cdots \otimes\left|j_{n}\right\rangle
$$

into

$$
\begin{equation*}
2^{-n / 2}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{n}\right)|1\rangle\right) \otimes \cdots \otimes\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \cdots j_{n}\right)|1\rangle\right) \tag{15}
\end{equation*}
$$

This equivalent representation of the QFT allows us to find an efficient implementation of the QFT. Define the unitary operator $R_{k}$ by

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

and the controlled $-R_{k}$ by

$$
|00\rangle \mapsto|00\rangle,|01\rangle \mapsto|01\rangle,|10\rangle \mapsto|10\rangle,|11\rangle \mapsto \exp \left(2 \pi i / 2^{k}\right)|11\rangle
$$

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

$$
\begin{gathered}
\left|j_{1}\right\rangle\left|j_{2}\right\rangle \cdots\left|j_{n}\right\rangle \mapsto \\
2^{-n / 2}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{n}\right)|1\rangle\right) \cdots\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{1} j_{2} \cdots j_{n}\right)|1\rangle\right) .
\end{gathered}
$$

We shall show that $n$ operations can produce $|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \cdots j_{n}\right)|1\rangle$ 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

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{j_{1}}|1\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{1}\right)|1\rangle\right)
$$

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

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2}\right)|1\rangle\right)
$$

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

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} j_{3}\right)|1\rangle\right)
$$

while keeping other qubits unchanged.
$1-n$. Apply the controlled- $R_{n}$ to the first and the $n$-th qubit, which changes the first qubit to

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \ldots j_{n}\right)|1\rangle\right)
$$

while keeping other qubits unchanged.

## Quantum Fourier transform 4

$$
\begin{gathered}
\left|j_{1}\right\rangle\left|j_{2}\right\rangle \cdots\left|j_{n}\right\rangle \mapsto \\
\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{n}\right)|1\rangle\right) \cdots\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \cdots j_{n}\right)|1\rangle\right) .
\end{gathered}
$$

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

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{1} j_{2} \ldots j_{n}\right)|1\rangle\right) \otimes\left|j_{2} j_{3} \ldots j_{n}\right\rangle
$$

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

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

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

$$
\frac{1}{2}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{2} j_{3}\right)|1\rangle\right),
$$

$2-3$. Apply the controlled $-R_{3}$ to the second and the forth qubit, which changes the second qubit to

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{2} j_{3} j_{4}\right)|1\rangle\right)
$$

while keeping other qubits unchanged.

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

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{2} j_{3} \ldots j_{n}\right)|1\rangle\right)
$$

while keeping other qubits unchanged.

## Quantum Fourier transform 5

$$
\begin{gathered}
\left|j_{1}\right\rangle\left|j_{2}\right\rangle \cdots\left|j_{n}\right\rangle \mapsto \\
\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{n}\right)|1\rangle\right) \cdots\left(|0\rangle+\exp \left(2 \pi i 0 \cdot j_{1} j_{2} \cdots j_{n}\right)|1\rangle\right)
\end{gathered}
$$

We shall show that single operation can produce $|0\rangle+\exp \left(2 \pi i 0 . j_{n}\right)|1\rangle$ 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
$\frac{1}{2^{(n-1) / 2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \ldots j_{n}\right)|1\rangle\right)\left(|0\rangle+\exp \left(2 \pi i 0 . j_{2} j_{3} \ldots j_{n}\right)|1\rangle\right) \cdots$ $\left(|0\rangle+\exp \left(2 \pi i 0 . j_{n-1} j_{n}\right)|1\rangle\right) \otimes\left|j_{n}\right\rangle$.
$n$-1. Apply $H$ to the $n$-th qubit, which changes the $n$-th qubit to

$$
\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{j_{n}}\right)=\frac{1}{\sqrt{2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{n}\right)|1\rangle\right)
$$

while keeping other qubits unchanged.

Now the quantum state of the whole $n$ qubits is $\frac{1}{2^{n / 2}}\left(|0\rangle+\exp \left(2 \pi i 0 . j_{1} j_{2} \ldots j_{n}\right)|1\rangle\right)\left(|0\rangle+\exp \left(2 \pi i 0 . j_{2} j_{3} \ldots j_{n}\right)|1\rangle\right) \cdots$ $\left(|0\rangle+\exp \left(2 \pi i 0 . j_{n-1} j_{n}\right)|1\rangle\right)\left(|0\rangle+\exp \left(2 \pi i 0 . j_{n}\right)|1\rangle\right)$, 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 $\epsilon$ 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. 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.
