量子フーリエ変換のスペクトル分解

青木貴史*, 前阪裕介**, 中原幹夫*

Spectral Decomposition of Quantum Fourier Transform

Takashi AOKI*, Yusuke MAESAKA** and Mikio NAKAHARA*

The spectral decomposition of an n-qubit quantum Fourier transform (QFT_n) is derived exactly. It is then applied to find the logarithm of a QFT_n gate. Hamiltonian which generates QFT_n in a single step is suggested.
Key words: Quantum Fourier transform, Spectral decomposition

1. Introduction

In this article we present a concrete form of the spectral decomposition of the quantum Fourier transform (QFT). QFT is one of the most useful mathematical tools in applied mathematics and mathematical sciences such as signal processing and quantum computing[1]. For example, in the famous quantum algorithm of factorization of a large integer due to Shor[2], QFT plays an essential rôle. Thus studying QFT is an important subject in various fields of applied mathematics. Spectral decomposition of QFT provides us with a very convenient way of theoretical treatment of QFT. As an application, we compute the logarithm of QFT.

2. Quantum Fourier Transform (QFT)

Let $n \geq 3$ be an integer and $N = 2^n$. Then the n-qubit quantum Fourier transform F_n is defined as follows.

$$F_n = \begin{pmatrix} F_{0,0} & \cdots & F_{N-1,0} \\ \vdots & & \vdots \\ F_{0,N-1} & \cdots & F_{N-1,N-1} \end{pmatrix}, \quad (1)$$

where

$$F_{j,k} = (-i)^{\frac{1}{N}} \frac{1}{\sqrt{N}} \exp\left(\frac{2\pi i}{N} jk\right), \quad (j,k = 0,1,\cdots,N). \quad (2)$$

The phase $(-i)^{1/N}$ has been introduced to make F_n unimodular; $|F_n| = 1$. Therefore F_n is an element of SU(N). We may equally work with the gate without the phase since the overall phase has no physical effects. It will turn out to be convenient to introduce an auxiliary matrix $\tilde{F}$ defined as

$$\tilde{F} = \begin{pmatrix} \tilde{F}_{0,0} & \cdots & \tilde{F}_{N-1,0} \\ \vdots & & \vdots \\ \tilde{F}_{0,N-1} & \cdots & \tilde{F}_{N-1,N-1} \end{pmatrix}, \quad (3)$$

$$\tilde{F}_{j,k} = \frac{1}{\sqrt{N}} \exp\left(\frac{2\pi i}{N} jk\right).$$

3. Spectral decomposition of QFT

Our main result is

Theorem 1. *The matrix $\tilde{F}_n$ has four eigenvalues $\lambda_1 = 1$, $\lambda_2 = -1$, $\lambda_3 = i$ and $\lambda_4 = -i$, with the multiplicity $g_1 = 2^{n-2}+1$, $g_2 = 2^{n-2}$, $g_3 = 2^{n-2}$ and $g_4 = 2^{n-2}-1$, respectively. Therefore the spectral decomposition of $\tilde{F}$ is given by*

$$\tilde{F}_n = P_1 - P_2 + iP_3 - iP_4, \quad (4)$$

where P_j is the projection operator to the eigenspace corresponding to an eigenvalue λ_j;

$$P_j = \prod_{k\neq j} \frac{(\tilde{F} - \lambda_k I)}{(\lambda_j - \lambda_k)}, \quad (1 \leq j \leq 4). \quad (5)$$

Their explicit forms are

$$(P_1)_{jk} = \frac{1}{4}\Big[\delta_{j-k,0} + \delta_{j+k,0} + \delta_{j+k,N} + \frac{2}{\sqrt{N}} \cos\left(\frac{2\pi}{N} jk\right)\Big], \quad (6)$$

$$(P_2)_{jk} = \frac{1}{4}\Big[\delta_{j-k,0} + \delta_{j+k,0} + \delta_{j+k,N} - \frac{2}{\sqrt{N}} \cos\left(\frac{2\pi}{N} jk\right)\Big], \quad (7)$$

$$(P_3)_{jk} = \frac{1}{4}\Big[\delta_{j-k,0} - \delta_{j+k,0} - \delta_{j+k,N} + \frac{2}{\sqrt{N}} \sin\left(\frac{2\pi}{N} jk\right)\Big], \quad (8)$$

$$(P_4)_{jk} = \frac{1}{4}\Big[\delta_{j-k,0} - \delta_{j+k,0} - \delta_{j+k,N} - \frac{2}{\sqrt{N}} \sin\left(\frac{2\pi}{N} jk\right)\Big]. \quad (9)$$

平成18年6月24日受理
* 理学科
** 大学院総合理工学研究科理学専攻
現在 株式会社経営情報センター

This result is readily translated into that for F_n as

$$F_n = \varepsilon(P_1 - P_2 + iP_3 - iP_4), \qquad (10)$$

where $\varepsilon = (-i)^{1/N}$.

The proof of the theorem is divided into several steps. Let char(λ) be the characteristic polynomial of $\tilde{F}$:

$$\mathrm{char}(\lambda) = |\lambda I - \tilde{F}|. \qquad (11)$$

Obviously $\tilde{F}^4 = I$ holds and hence it should have the form:

$$\begin{aligned} \mathrm{char}(\lambda) &= (\lambda-1)^a(\lambda+1)^b \\ &\quad \times(\lambda-i)^c(\lambda+i)^d, \end{aligned} \qquad (12)$$

where $a = g_1,\ b = g_2,\ c = g_3$ and $d = g_4$ are the multiplicities of the eigenvalues. It follows from Eq. (12) that

$$\begin{aligned} &\mathrm{char}(\lambda)\cdot\mathrm{char}(-\lambda) \\ &\quad = (\lambda-1)^{a+b}(\lambda+1)^{a+b} \\ &\qquad \times(\lambda-i)^{c+d}(\lambda+i)^{c+d}. \end{aligned} \qquad (13)$$

Now let us consider the square of $\tilde{F}$

$$\tilde{F}^2 = \left(\begin{array}{c|cccc} 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & 1 \\ \vdots & & \iddots & \\ 0 & 1 & \cdots & 0 \end{array}\right). \qquad (14)$$

Since $N = 2^n$ is even, we have $\mathrm{char}(\lambda)\cdot\mathrm{char}(-\lambda) = |\lambda I - \tilde{F}|\cdot|-\lambda I - \tilde{F}| = |\lambda^2 I - \tilde{F}^2|$, from which we obtain

$$\begin{aligned} &\mathrm{char}(\lambda)\cdot\mathrm{char}(-\lambda) \\ &= |\lambda^2 I - \tilde{F}^2| \\ &= \underbrace{\left|\begin{array}{c|cccccc} \lambda^2-1 & 0 & & \cdots & & & 0 \\ \hline 0 & \lambda^2 & & & & & -1 \\ & & \ddots & & & \iddots & \\ & & & \lambda^2 & & -1 & \\ \vdots & & & & \lambda^2-1 & & \\ & & & -1 & & \lambda^2 & \\ & & \iddots & & & & \ddots \\ 0 & -1 & & & & & \lambda^2 \end{array}\right|}_{2^n} \\ &= (\lambda^2-1)^2 \underbrace{\left|\begin{array}{cccccc} \lambda^2 & & & & & -1 \\ & \ddots & & & \iddots & \\ & & \lambda^2 & -1 & & \\ & & -1 & \lambda^2 & & \\ & \iddots & & & \ddots & \\ -1 & & & & & \lambda^2 \end{array}\right|}_{2^n-2} \\ &= (\lambda^2-1)^2 \left|\begin{array}{cccccc} 0 & & & & & \lambda^4-1 \\ & \ddots & & & \iddots & \\ & & 0 & \lambda^4-1 & & \\ & & -1 & \lambda^2 & & \\ & \iddots & & & \ddots & \\ -1 & & & & & \lambda^2 \end{array}\right| \\ &= (\lambda^2-1)^2 \left|\begin{array}{cccccc} 1 & & & & & -\lambda^2 \\ & \ddots & & & \iddots & \\ & & 1 & -\lambda^2 & & \\ & & 0 & \lambda^4-1 & & \\ & \iddots & & & \ddots & \\ 0 & & & & & \lambda^4-1 \end{array}\right| \\ &= (\lambda^2-1)^2 \underbrace{\left|\begin{array}{ccc} \lambda^4-1 & & \\ & \ddots & \\ & & \lambda^4-1 \end{array}\right|}_{2^{n-1}-1} \\ &= (\lambda^2-1)^2(\lambda^4-1)^{2^{n-1}-1} \\ &= (\lambda-1)^{2^{n-1}+1}(\lambda+1)^{2^{n-1}+1} \\ &\quad \times(\lambda-i)^{2^{n-1}-1}(\lambda+i)^{2^{n-1}-1}. \end{aligned} \qquad (15)$$

It follows from Eqs. (13) and (15) that

$$a+b = 2^{n-1}+1\ ,\ c+d = 2^{n-1}-1. \qquad (16)$$

Two more equations necessary to find a, b, c and d are obtained by evaluating the trace of $\tilde{F}_n$. We obtain

$$\mathrm{tr}\tilde{F}_n = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(\frac{2\pi i}{N}j^2\right) = 1+i, \qquad (17)$$

by using the following identities[3)]

$$\begin{aligned} \sum_{j=0}^{M-1}\cos\left(\frac{2j^2\pi}{M}\right) &= \sqrt{M}, \\ \sum_{j=0}^{M-1}\sin\left(\frac{2j^2\pi}{M}\right) &= \sqrt{M}, \end{aligned} \qquad (18)$$

which are applicable when $M \equiv 0 \pmod 4$. Trace of $\tilde{F}_n$ is also evaluated by noting that $\mathrm{tr}P_j = g_j$ and found to be

$$\mathrm{tr}\tilde{F}_n = a - b + ci - di. \qquad (19)$$

Comparing this with Eq. (17), we find two equations

$$a-b=1, \quad c-d=1. \qquad (20)$$

Finally Eqs. (16) and (20) are solved to yield

$$a = 2^{n-2}+1,\ b = 2^{n-2},\ c = 2^{n-2},\ d = 2^{n-2}-1 \quad (21)$$

and Theorem 1 has been proved.

These results are also summarized in the form of the characteristic polynomial of $\tilde{F}_n$ as

$$\begin{aligned} \mathrm{char}(\lambda) &= (\lambda-1)^{2^{n-2}+1}(\lambda+1)^{2^{n-2}} \\ &\quad \times(\lambda-i)^{2^{n-2}}(\lambda+i)^{2^{n-2}-1}. \quad (22) \end{aligned}$$

We note *en passant* that the minimal polynomial of $\tilde{F}_n$ is

$$\min(\lambda) = \lambda^4 - 1. \quad (23)$$

Next we evaluate the projection operators. We first note that $\tilde{F}_n^3 = \tilde{F}_n^\dagger = F_n^*$, $*$ being the complex conjugation, and

$$\left(\tilde{F}_n^2\right)_{jk} = \delta_{j+k,0} + \delta_{j+k,N}.$$

Then

$$\begin{aligned} (P_1)_{jk} &= \frac{1}{4}\left[(\tilde{F}_n+I)(\tilde{F}_n-iI)(\tilde{F}_n+iI)\right]_{jk} \\ &= \frac{1}{4}(\tilde{F}_n^3+\tilde{F}_n^2+\tilde{F}_n+I)_{jk} \\ &= \frac{1}{4}\Big[\delta_{j-k,0}+\delta_{j+k,0}+\delta_{j+k,N} \\ &\quad +\frac{2}{\sqrt{N}}\cos\left(\frac{2\pi}{N}jk\right)\Big]. \quad (24) \end{aligned}$$

Other projction operators are obtained similarly.

4. Logarithm of F_n

Now that we have obtained the spectral decomposition of F_n, it is easy to construct its logarithm. Note that the logarithm of a unitary gate corresponds to the Hamiltonian (times time, to be precise) which implements the unitary gate, assuming all the generators of the Lie algebra are available.

The spectral decomposition (10) gives

$$\begin{aligned} \log F_n &= \{\log(\varepsilon)\}P_1 + \{\log(-\varepsilon)\}P_2 \\ &\quad + \{\log(i\varepsilon)\}P_3 + \{\log(-i\varepsilon)\}P_4 \\ &= \left(\frac{3}{2^{n+1}}\pi i + 2\pi n_1 i\right)P_1 \\ &\quad + \left(\frac{3}{2^{n+1}}\pi i + \pi i + 2\pi n_2 i\right)P_2 \\ &\quad + \left(\frac{3}{2^{n+1}}\pi i + \frac{\pi}{2}i + 2\pi n_3 i\right)P_3 \\ &\quad + \left(\frac{3}{2^{n+1}}\pi i + \frac{3\pi}{2}i + 2\pi n_4 i\right)P_4, \end{aligned} \quad (25)$$

where n_j is an integer specifying the branch of $\log(\lambda_j)$ function. We will fix $\{n_j\}$ such that the resulting matrix has vanishing trace. In other words, $\{n_j\}$ are chosen in such a way that $\log F_n$ be an element of the Lie algebra $\mathfrak{su}(N)$.

It follows from Eq. (21) that

$$\begin{aligned} \mathrm{tr}F_n &= 2\pi i\left(n_1+n_2+n_3+n_4+\frac{3}{2}\right)2^{n-2} \\ &\quad +2\pi i(n_1-n_4) = 0. \quad (26) \end{aligned}$$

An example of n_j which satisfies the above constraint is

$$\begin{aligned} n_1 &= -2^{n-2},\ n_2 = 2^{n-2}, \quad (27) \\ n_3 &= -2^{n-3},\ n_4 = 2^{n-3}. \end{aligned}$$

Now we have proved the following Corollary.

Corollary 1. *Let H_n be a matrix defined by*

$$\begin{aligned} H_n &= \frac{\pi i}{2^{n+1}}[(3-4^n)P_1 + (3+4^n+2^{n+1})P_2 \\ &\quad +(3-2^{2n-1}+2^n)P_3 \\ &\quad +(3+2^{2n-1}+3\cdot 2^n)P_4]. \quad (28) \end{aligned}$$

Then $H_n \in \mathfrak{su}(2^n)$ and $F_n = \exp H_n$.

In fact, there are infinitely different ways to make $\log F_n \in \mathfrak{su}(N)$. For instance Eq. (26) is satisfied if we take

$$\left(\begin{array}{lcl} \alpha+\beta+\gamma+\delta &=& 0, \\ \alpha-\delta+3\cdot 2^{n-3} &=& 0, \end{array}\right.$$

which are solved to yield two parameter family of solutions

$$\begin{aligned} n_1 &= n_4 - 3\cdot 2^{n-3}, \\ n_2 &= 3\cdot 2^{n-3} - n_3 - 2\delta. \end{aligned} \quad (29)$$

For each choice of the set $\{n_k\}$ there corresponds a Hamiltonian of different matrix elements. Which choice is best fitted depends on actual physical realization of the algorithm.

5. Summary and Discussion

We have obtained in this paper the explicit form of the spectral decomposition of the qauntum Fourier transform for an arbitaray n-qubit system with $n \geq 3$. We used this decomposition to find a Hamiltonian which implements the quantum Fourier transform in a single step. A Hamiltonian, looked upon as an element of the Lie algebra $\mathfrak{su}(2^n)$, has only a limited number of generators and further ingenuity must be required in actual implementation.

After completing this work, we were informed of the previous works[4, 5], where spectral decomposition of QFT were carried out. In both works, eigenvectors were explicitly obtained to evaulate the projection operators. We believe our work is superior to the previous works in that projection operators were evaluaed directly without employing the eigenvectors. This makes our analysis considerablly simpler. We would like to thank Yumi Nakajima for drawing our attention to references 4) and 5).

References

1) M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
2) P. W. Shor, in: *Proceeding of 35th IEEE FOCS*, Santa Fe, NM, (1994) 124.
3) P. G. L. Dirichlet and J. W. R. Dedekind, §111-112 in *Vorlesungen über Zahlentheorie*, Friedrich Vieweg und Sohn, (1894).
4) J. H. Maclellan and T. W. Parks, *IEEE Transaction on Audio and Electroacoustics*, **AU-20** (1972) 66.
5) M. L. Mehta, *J. Math. Phys.* **28** (1987) 781.