The Planck Constant and Quantum Fourier Transformation

Zhengjun Cao[1],   Zhenfu Cao[2]

Abstract. Quantum Fourier Transformation (QFT) plays a key role in quantum computation theory. But its transform size has never been discussed. In practice, the Xilinx LogiCORE IP Fast Fourier Transform core has the maximum transform size $N = 2^{16}$. Taking into account the Planck constant $\hbar = 6.62607015 \times 10^{-34}$ and the difficulty to physically implement basic operator $\begin{bmatrix} 1 & 0 \\ 0 & \exp(-2\pi\, i/N) \end{bmatrix}$ on a qubit, we think $N = 2^{120}$ could be an upper bound for the transform size of QFT.

Keywords: Quantum Fourier Transformation, transform size, depleted operator, Shor algorithm, Planck constant.

1 Introduction

Quantum computer is viewed as the biggest threat to public key cryptography, due to Shor algorithms [1]. Thirty years later, however, we are now facing the embarrassing situation. On the one hand, there were many announcements of success in manufacturing quantum computers, including IBM 133 qubits on the Heron chip. On the other hand, there is no guarantee of success in running these devices to solve an actual numerical computation problem. There must be some reasons for this fact. The misunderstandings about quantum algorithms (Shor algorithms, Grover algorithm [2], etc.), could be the main reason for the conflict between ideal and reality. The quantum Fourier transformation plays a pivotal role in modern quantum computation theory. But we find its transform size has never been mentioned and discussed. In this note, we argue that $N = 2^{120}$ could be a proper upper bound for the transform size of QFT. To the best of our knowledge, it is the first time to get such a result.

2 Preliminaries

The state of a qubit is described by a 2-dimensional vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. The basic two quantum states corresponding to the two states of a classical bit are defined by

$$\text{bit } 0 \leftrightarrow |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{bit } 1 \leftrightarrow |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

[1] Department of Mathematics, Shanghai University, Shanghai, 200444, China. Email: caozhj@shu.edu.cn

[2] Software Engineering Institute, East China Normal University, Shanghai, 200062, China.

The basic single-qubit operations include

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

where H is called Hadamard gate. Clearly,

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Given two separate qubits, the corresponding two-qubit state is given by the tensor product of vectors. For example,

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \\ \beta \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix}.$$

The basis for two-qubit states consists of

$$\text{string } 00 \leftrightarrow |00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \text{string } 01 \leftrightarrow |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$\text{string } 10 \leftrightarrow |10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad \text{string } 11 \leftrightarrow |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

A unitary transformation on n qubits is a matrix U of size $2^n \times 2^n$. The CNOT (controlled-NOT) gate is a commonly used two-qubit gate

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Sometimes, two-qubit gates can be described by the tensor product of some single-qubit gates. Not all two-qubit gates can be written as the tensor product of single-qubit gates. Such a gate is called an *entangling gate*, for example, the CNOT gate. The gates H, T and CNOT form a universal gate set because any general unitary transformation can be broken into a series of two qubit rotations.

The only way to change qubits without measuring is to apply a unitary operation. Quantum computations can be created by designing unitary operations in sequence, each of which is composed of smaller operations.

3 Quantum Fourier Transformation

Let n be the number of qubits used for QFT, $N = 2^n$, and $\omega = \exp(-2\pi\, i/N)$. The QFT for n-qubits is described by the matrix

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

Define $R_n := \begin{bmatrix} 1 & 0 \\ 0 & \exp(\frac{-2\pi\, i}{2^n}) \end{bmatrix}$. The QFT_N circuit is depicted as follows (see Fig.1, Ref.[3])

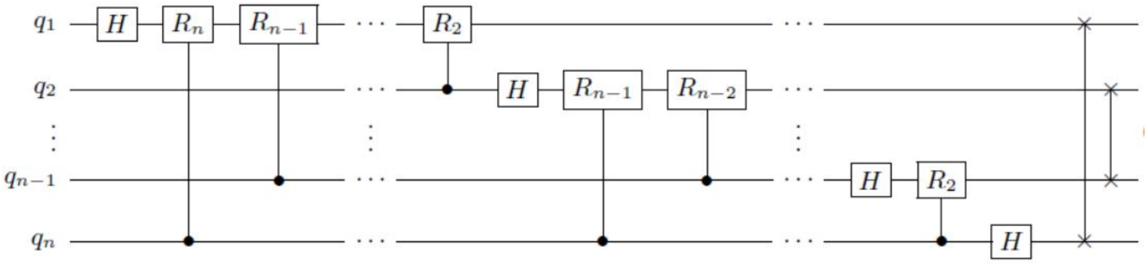

Figure 1: The QFT circuit for n qubits

4 The depleted operators

As we know, the Xilinx LogiCORE IP Fast Fourier Transform core designed for implementing the Cooley-Tukey algorithm, has only the maximum transform size $N = 2^{16}$. When using scaling, a schedule is used to divide by a factor of 1, 2, 4, or 8 in each stage. If scaling is insufficient, a butterfly output might grow beyond the dynamic range and cause an overflow. As a result of the scaling applied in the FFT implementation, the transform computed is a scaled transform [4]. The scale factor s is defined as

$$s = 2^{\sum_{i=0}^{\log(N-1)} b_i}$$

where b_i is the scaling applied in stage i. The scaling results in the final output sequence being modified by the factor $1/s$.

In contrast, the QFT needs a very huge transform size $N = 2^{1024}$ if Shor algorithm is used to fact RSA-1024. Is it possible to run QFT with such a transform size? The answer could be discouraging due to the difficulty to physically implement the basic operators. Actually, the Planck constant is $\hbar = 6.62607015 \times 10^{-34}$ joule second. The Planck length is 1.62×10^{-35} meters, the smallest possible length. The Planck time is 5.391247×10^{-44} seconds, an incredibly small interval of time. But now, we have

$$R_{1024} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(\frac{-2\pi\, i}{2^{1024}}) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \cos(\pi/2^{1023}) - i\sin(\pi/2^{1023}) \end{bmatrix},$$

where

$$\sin(\pi/2^{1023}) \approx 3.495137844 \times 10^{-308},$$

is an extremely tiny number. For convenience, we call such a transformation involving some extremely tiny quantities *depleted operator*. Apparently, the depleted operator acting on a qubit cannot generate any physical quantity change, such as energy, frequency, etc. In view of this fact, we think $N = 2^{120}$ could be an upper bound for the transform size of QFT, due to that

$$\hbar = 6.62607015 \times 10^{-34} \approx 880.756 \times 2^{-120}$$

This means only the operators $R_2, R_4, R_8, \cdots, R_{2^{120}}$, could be physically managed.

Can we adopt some schedule to scale the operators $R_{1024}, R_{1023}, \cdots, R_{121}$? In a classical algorithm, each intermediate machine state is explicit and can be measured, recorded, and scaled. But in a quantum algorithm, each intermediate quantum state is ambiguous and cannot be definitely measured and recorded. The common scaling schedule makes no sense for QFT. Keep in mind, we are now facing the depleted operators, instead of overflowed numbers. It is thorough erratic.

5 Conclusion

We investigate the transform size of Quantum Fourier Transformation, and remark that any depleted operator cannot be physically applied to a qubit. The finding in this note could be a good explanation for the conflict between ideal and reality of quantum computer manufacture.

References

[1] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5), 1484-1509, 1997.

[2] L. Grover. A fast quantum mechanical algorithm for database search. Proceedings 28th Annual Symposium on the Theory of Computing (STOC) 1996, pp. 212-219.

[3] D. Camps, R. Beeumen, C. Yang. Quantum Fourier transform revisited, arXiv:2003.03011v2, 2020.

[4] Fast Fourier Transform v9.1, LogiCORE IP Product Guide, May 4, 2022.