The Planck constant and Quantum Fourier Transformation

Zhengjun Cao and Zhenfu Cao

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 Fast Fourier Transform core has the maximum transform size $N = 2^{16}$. Taking into account the Planck constant $h = 6.626 \times 10^{-34}$ 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 the biggest threat to public key cryptography, due to Shor algorithm [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 1,000-qubit quantum chip [2]. On the other hand, there is no guarantee of success in running these devices to solve an actual numerical computing problem. There must be some reasons for this fact. The misunderstandings about quantum algorithms 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. M. Dyakonov [**?**] ever asked a crucial question what precision was required (for manipulating a quantum gate). In this note, we argue that $N = 2^{120}$ could be an upper bound for the transform size of QFT. We also argue that the precision for a qubit operation is no less than 4.72694×10^{-36}. To the best of our knowledge, it is the first time to get such a result of energy dependency of quantum computing.

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 bit $0 \leftrightarrow |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, bit $1 \leftrightarrow |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The basic single-qubit

Z.J. Cao is with Department of Mathematics, Shanghai University, Shanghai, China. caozhj@shu.edu.cn
Z.F. Cao is with Software Engineering Institute, East China Normal University, China. zfcao@sei.ecnu.edu.cn

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])

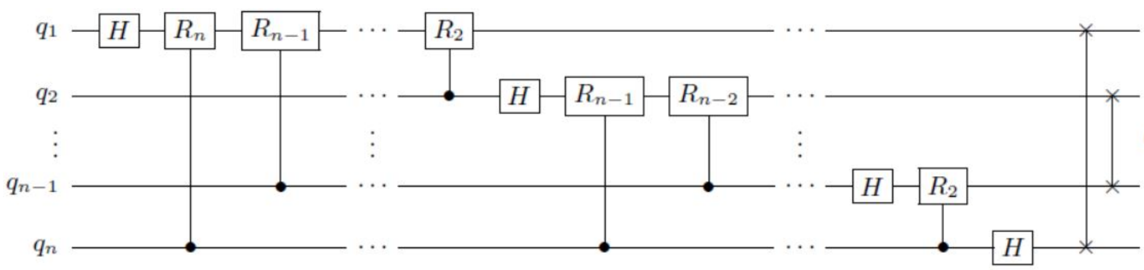

Figure 1: The QFT circuit for n qubits

4 The depleted operators

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

$$h = 6.626 \times 10^{-34} \ \text{ joule second.}$$

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 an extremely tiny number *depleted operator*. Apparently, the depleted operator acting on a qubit cannot generate any physical quantity change, such as energy and frequency.

5 An upper bound for QFT

Notice that the energy of a free particle with wave function Ae^{ikx} is

$$E = \frac{h^2 k^2}{8\pi^2 m}$$

where m is the mass of this particle, x is the distance between an observer and this particle, and k is the wave number. In the considered scenario, $k = \frac{2\pi}{2^n x}$, the approximate value of its energy is $\frac{h^2}{2^{2n+1}x^2 m}$. The rest mass of an electron is $m \approx 9.109 \times 10^{-31}$ kg. Hence, the energy of this electron is about $\frac{7.457\times10^{-654}}{x^2}$, if $n = 1024$. Since the Planck length is 1.62×10^{-35} meters, the smallest possible length. We have the approximation

$$\frac{7.457 \times 10^{-654}}{2.6244 \times 10^{-70}} \approx 2.84 \times 10^{-584} \text{ (joule)}$$

which is an extremely tiny number. Clearly, the operator R_{1024} acted on an electron (or other quantum particle) cannot generate any physical quantity change, such as energy and frequency.

Practically, the lowest frequency of radio waves is only 3 Hertz, with the energy 1.9878×10^{-33} joule. In view of this fact and taking into account the roundoff and truncation errors, we think, 2^{120} could be an upper bound to the transform size of QFT, corresponding to the extreme energy value 5.19724×10^{-40} joule. This means only the operators $R_2, R_3, \cdots, R_{120}$, could be manipulated by the current quantum technology.

M. Dyakonov [4] ever commented: "The notion of ENERGY, of primordial importance in physics, both classical and quantum, has absolutely no role in QC (quantum computing) theory!" The above argument shows the energy dependency of QFT, and the precision for a qubit operation is no less than $\sin(\pi/2^{119}) \approx 4.72694 \times 10^{-36}$.

6 The failure of scaling

The Xilinx Fast Fourier Transform (FFT) core has 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 [5]. The scale factor is $s = 2^{\sum_{i=0}^{\log(N-1)} b_i}$, 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 a classical algorithm, each intermediate machine state can be measured, recorded, and scaled. In a quantum algorithm, however, each intermediate quantum state cannot be definitely measured and recorded. So, the common scaling schedule makes no sense for QFT.

7 Conclusion

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

Acknowledgements

We thank the Key Programs of National Natural Science Foundation of China, Grant 2020YFA0712304, and Grant 62132005. We are grateful to prof. Mikhail Dyakonov for his valuable comments on this manuscript.

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] D. Castelvecchi, IBM releases first-ever 1,000-qubit quantum chip, Nature 624 (238), 2023.

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

[4] M. Dyakonov. The case against quantum computing. IEEE Spectrum 3, 2019.

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