Realization of quantum Fourier transform over Z_N*

Fu Xiang-Qun(付向群), Bao Wan-Su(鲍皖苏)†, Li Fa-Da(李发达), and Zhang Yu-Chao(张宇超)

Information Engineering University, Zhengzhou 450004, *China*

(Received 21 April 2013; revised manuscript received 4 July 2013; published online 10 December 2013)

Since the difficulty in preparing the equal superposition state of amplitude is $1/\sqrt{N}$, we construct a quantile transform of quantum Fourier transform (QFT) over Z_N based on the elementary transforms, such as Hadamard transform and Pauli transform. The QFT over Z_N can then be realized by the quantile transform, and used to further design its quantum circuit and analyze the requirements for the quantum register and quantum gates. However, the transform needs considerable quantum computational resources and it is difficult to construct a high-dimensional quantum register. Hence, we investigate the design of t-bit quantile transform, and introduce the definition of t-bit semiclassical QFT over Z_N. According to probability amplitude, we prove that the transform can be used to realize QFT over Z_N and further design its quantum circuit. For this transform, the requirements for the quantum register, the one-qubit gate, and two-qubit gate reduce obviously when compared with those for the QFT over Z_N.

Keywords: quantum Fourier transform, semiclassical quantum Fourier transform, quantum algorithm

PACS: 03.67.Lx, 03.65.Sq, 03.65.Ta, 03.67.–a **DOI:** 10.1088/1674-1056/23/2/020306

1. Introduction

Quantum computers have a strong ability to perform parallel computing with multi-input data processed in one operation, whereas a classical computer has no such ability. In 1994, Shor[1] presented a polynomial-time quantum algorithm for factorization and discrete logarithm problems. This algorithm can break public-key cryptography, such as RSA and Diffie–Hellman protocol. In 1996, Grover[2] presented a quantum searching algorithm, reducing the computational complexity of current exhaustive search attacks from $O(2^n)$ to $O(2^{n/2})$. Apparently, the emergence of these two algorithms greatly threatens current cryptography, especially public-key cryptography, whose security is based on factorization and discrete logarithm. Great attention has since been paid to research on quantum computation.[3–6]

Quantum Fourier transform (QFT) is the core of the existing quantum algorithm and can be used for preparing the equal superposition state. Parallel computing can then be implemented on the quantum computer. Meanwhile, the success probability of the quantum algorithm can be increased by the QFT. In Shor's quantum algorithm, since the Oracle function has the nature of existing order, the probability amplitude can be collected after the QFT over Z_{2^n} in the quantum state. Consequently, the target state can be observed with high probability. In 2003, Proos and Zalka[7] presented a quantum algorithm for the elliptic curve discrete logarithm over F_p (p is a prime), which makes the amplitude of non-target state, except the state $|0\rangle$, be 0 under the QFT over Z_p in the quantum states. So, the success probability is close to 1. If the QFT is not over Z_p, then the amplitude of non-target state, except the state $|0\rangle$, will not be 0. In 2012, Li *et al.*[8] presented a polynomial-time quantum algorithm for factorization, whose success probability is close to 1. It needs the QFT over Z_N, as does Zalka's algorithm, otherwise the success probability is not close to 1, where N is the factoring integer. It is obvious that the QFT over different rings has a great influence on the success probability of a quantum algorithm.

The different implementations of QFT have an influence on quantum computational resources and speeds. Generally speaking, when implementing the QFT over Z_{2^n}, an n-bit quantum state is one time inputted, its circuit needs $n^2/2$ two-bit quantum gates and n one-bit quantum gates in total.[9] Up to date, to the best of our knowledge, there has been no implementation method for the n-dimensional QFT within existing technology for larger n. In 1996, Griffiths and Niu[10] presented the single-bit semiclassical QFT over Z_{2^n}. Since the transform input comes from bit flipping, the transform only needs one-dimensional (1D) quantum register and a one-bit quantum gate and, therefore, the QFT can be implemented without a two-bit quantum gate. Thus, the single-bit semiclassical QFT provides a solution for implementing a high-dimensional QFT under the condition of limited computational resources. In 2005, Chiaverini *et al.*[11] implemented the single-bit semiclassical QFT in a system of three beryllium ion qubits (two-level quantum systems) confined in a segmented multizone trap, which verifies the feasibility of the semiclassical QFT. In 2012, we presented a t-bit semiclassical QFT over Z_{2^n},[12] which needs low-dimensional QFT. The requirements for the two-bit and one-bit quantum gates are, respectively, reduced to $1/l^2$ and $2/l$ times those of the QFT over Z_{2^n} (where n denotes the dimension of the QFT; if t divides n exactly, $l = [n/t] - 1$, otherwise $l = [n/t]$), and clarify that the speed of the t-bit semiclassical QFT over Z_{2^n} in-

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2014 Chinese Physical Society and IOP Publishing Ltd

creases to t times that of the single-bit case. Thus, the transform admits a resource/time-tradeoff in the implementation of the QFT. However, there is no quantum circuit of the QFT over Z_N, which should be used for the quantum algorithm. How to design the implementation of the QFT and t-bit semiclassical QFT over Z_N is worth further investigating.

Quantile transform, as defined below, is an important link of the QFT over Z_{2^n}. Up to now, it has been available to be realized based on Hadamard transform. The n quantile transforms are easily used for preparing the equal superposition state, with amplitude being $1/\sqrt{2^n}$, but it is difficult when the amplitude is $1/\sqrt{N}$. If the quantile transform of the QFT over Z_N can be designed, then the implementation of the QFT over Z_N can be given.

In this paper, we construct the quantile transform of QFT over Z_N based on the elementary transforms, such as Hadamard transform and Pauli transform. According to the probability amplitude, we prove that the QFT over Z_N can be realized by the quantile transform and used to further design its quantum circuit, which requires $(2n+1)$-dimensional quantum register, $2n$ one-bit quantum gates, and n^2 two-bit quantum gates. However, the transform needs considerable quantum computational resources and it is difficult to build a high-dimensional quantum register. We investigate the design of t-bit quantile transform based on the elementary transform, such as Hadamard transform and Pauli transform and, thus, introduce the definition of t-bit semiclassical QFT over Z_N. According to the probability amplitude, we prove that the transform can be used to realize QFT over Z_N and can also be used to further design its quantum circuit. The dimension of the quantum register, two-bit, and one-bit quantum gates required are, respectively, reduced to $1/l$, $1/l$, and $1/l^2$ times those of the QFT over Z_N (where $n = \lceil \log N \rceil$; if t divides n exactly, $l = [n/t]-1$, otherwise $l = [n/t]$).

2. t-bit semiclassical QFT over Z_{2^n}

Definition 1 (Quantum Fourier transform)[9] The QFT over Z_N on an orthonormal basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ is defined as a linear operator $U_{\rm F}$ with an action on the basis states described by

$$U_{\rm F} : |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle.$$

Therefore, the action on an arbitrary state may be written as

$$U_{\rm F} : \sum_{j=0}^{N-1} x_j |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j \omega_N^{jk} |k\rangle,$$

where the symbol "$\mapsto$" denotes an invertible transform and $\omega_N = {\rm e}^{2\pi {\rm i}/N}$.

If $N = 2^n$, then the QFT $U_{\rm F}$ acting on the state $|a\rangle$ can be written as

$$U_{\rm F} |a\rangle = \prod_{j=0}^{n-1} \otimes \left| p(\phi_j) \right\rangle_j.$$

It is called the n-dimensional QFT, where $a = \sum_{j=0}^{n-1} a_j 2^j$ is the binary representation of a, with a_j being 0 or 1; $\phi_j = \sum_{k=0}^{n-j} a_k 2^{j+k-n-1}$ for $j = 0, 1, \ldots, n-1$; $|p(\phi)\rangle = (|0\rangle + {\rm e}^{2\pi {\rm i}\phi} |1\rangle)/\sqrt{2}$. In this paper, we call $|p(\phi)\rangle$ the quantile transform.

It has been pointed out[9] that the circuit of the QFT requires a $(\lceil \log N \rceil)$-dimensional quantum register. In 2012, the t-bit semiclassical QFT over Z_{2^n} was presented.[12] It carries $|a\rangle = |a_{n-1}, a_{n-2}, \ldots, a_0\rangle$ into $|c\rangle = |c_{n-1}, c_{n-2}, \ldots, c_0\rangle$, whose amplitude is equal to that for the QFT. Thus, the t-bit semiclassical QFT over Z_{2^n} can realize the QFT, which can carry out the parallel computing of 2^n inputs within $l+1$ steps (if t divides n exactly, $l = [n/t]-1$, otherwise $l = [n/t]$). Measurements made after transforming each bit block show that the t-bit semiclassical QFT over Z_{2^n} requires less quantum computational resources than the QFT, where the first bit block has $n - lt$ bits and all of the others have t bits.

3. t-bit semiclassical QFT over Z_N

3.1. Circuit of the QFT over Z_N

Up to now, there has been no circuit of the QFT over Z_N, which the quantum algorithm requires. Thus, it is imperative to design the circuit. Its specific transform method is as follows.

Theorem 1 Suppose that N is a positive integer, the binary representation of $N-1$ is $(N_n, N_{n-1}, \ldots, N_1)$, and $|a\rangle = |a_n, a_{n-1}, \ldots, a_1\rangle$ is an arbitrary orthonormal state with orthonormal basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$. $U_{\rm d}$ transforms $|a\rangle$ from the most significant bit to the least bit, as follows.

(i) If $j_k = 1$, d_k on $|a_k\rangle$ under the two situations:

(i)-a $N_k = 0$

$$|j_k\rangle |a_k\rangle \mapsto |j_k\rangle |0\rangle \mapsto |j_{k-1} = 1\rangle |0\rangle;$$

(i)-b $N_k = 1$

$$\begin{aligned} |j_k\rangle |a_k\rangle \;&\mapsto\; |j_k\rangle \left(\frac{\sqrt{2^{k-1}}}{\sqrt{N-\lambda_k}} |0\rangle + \frac{\sqrt{N-\lambda_k-2^{k-1}}}{\sqrt{N-\lambda_k}} |1\rangle \right) \\ &\mapsto\; \frac{2^{k-2}}{\sqrt{N-\lambda_k}} |j_{k-1} = 0\rangle |0\rangle \\ &\quad + {\rm e}^{2^k \pi {\rm i} (\varphi_k + 2^{k-2} a_{k-1} + \cdots + a_1)/N} \\ &\quad \times \frac{\sqrt{N-\lambda_k-2^{k-1}}}{\sqrt{N-\lambda_k}} |j_{k-1} = j_k\rangle |1\rangle, \end{aligned}$$

(ii) If $j_k = 0$, d_k on $|a_k\rangle$ is that

$$\begin{aligned} &|j_k\rangle |a_k\rangle \\ \mapsto\; &\frac{1}{\sqrt{2}} |j_k\rangle (|0\rangle + |1\rangle) \\ \mapsto\; &\frac{1}{\sqrt{2}} |j_{k-1} = 0\rangle (|0\rangle + |1\rangle) \end{aligned}$$

$$\mapsto |j_{k-1}=0\rangle \otimes \left(|0\rangle + \mathrm{e}^{2^k\pi \mathrm{i}(\varphi_k+2^{k-1}a_k+2^{k-2}a_{k-1}+\cdots+a_1)/N}|1\rangle\right)/\sqrt{2},$$

where $k=1,2,\ldots,n$, $\varphi_{k-1}=\varphi_k+2^{k-1}a_k$, $\varphi_n=0$, $\lambda'_k=\lambda_{k'+1}+2^{k'-1}N'_k$, $\lambda_n=2^{n-1}N_n$, $k'=1,2,\ldots,n-1$, and $j_n=1$. U_{d} is equal to the QFT over Z_N and d_k is called quantile transform of QFT over Z_N.

Proof d_k carries $|a_k\rangle$ into $|c_k\rangle$, whose amplitude is different depending on the value of j_k.

1) If $j_k=0$

$$\begin{aligned} A_k &= \mathrm{e}^{2^k\pi \mathrm{i}(\varphi_k+2^{k-1}a_k+2^{k-2}a_{k-1}+\cdots+a_1)}/\sqrt{2} \\ &= \mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}/\sqrt{2}; \end{aligned}$$

2) If $j_k=1$, there are two situations.

2)-a $N_k=1$

$$A_k = \begin{cases} \dfrac{\sqrt{2^{k-1}}}{\sqrt{N-\lambda_k}}, & c_k=0, \\ \dfrac{\sqrt{N-\lambda_k-2^{k-1}}}{\sqrt{N-\lambda_k}}\,\mathrm{e}^{2^k\pi \mathrm{i}(\varphi_k+2^{k-1}a_k+\cdots+a_1)c_k/N}, & c_k=1, \end{cases}$$

$$= \begin{cases} \dfrac{\sqrt{2^{k-1}}}{\sqrt{N-\lambda_k}}, & c_k=0, \\ \dfrac{\sqrt{N-\lambda_k-2^{k-1}}}{\sqrt{N-\lambda_k}}\,\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}, & c_k=1, \end{cases}$$

2)-b $N_k=0$

$$A_k=1.$$

Then, the amplitude of $|c\rangle=|c_n,c_{n-1},\ldots,c_1\rangle$ can be obtained.

2)-b1 If $c_n=0$, then $j_{n-1}=0$ and $A_n=\sqrt{2^{n-1}}/\sqrt{N}$. The amplitude of c_k is $A_k=\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}/\sqrt{2}$, so the amplitude of $|c\rangle=|0,c_{n-1},\ldots,c_1\rangle$ is

$$\begin{aligned} A &= A_nA_{n-1}\bullet\cdots\bullet A_1 \\ &= \frac{\sqrt{2^{n-1}}}{\sqrt{N}}\prod_{k=1}^{n-1}\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}/\sqrt{2} \\ &= \frac{1}{\sqrt{N}}\prod_{k=1}^{n-1}\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N} \\ &= \frac{1}{\sqrt{N}}\mathrm{e}^{2\pi \mathrm{i}ac/N}, \end{aligned}$$

2)-b2 If $c_n=1$ and $N_{n-1}=0$, then

$$A_n=\frac{\sqrt{N-2^{n-1}}}{\sqrt{N}}\,\mathrm{e}^{2^{nk}\pi \mathrm{i}ac_n/N},$$

$j_{n-1}=1$ and $A_{n-1}=1$. So the quantum state $|c\rangle$ has a unique form $|1,0,c_{n-2},\ldots,c_1\rangle$, whose amplitude is

$$\frac{\sqrt{N-2^{n-1}}}{\sqrt{N}}\,\mathrm{e}^{2^{nk}\pi \mathrm{i}ac_n/N}\bullet A_{n-2}\bullet\cdots\bullet A_1.$$

2)-b3 If $c_n=1$ and $N_{n-1}=1$, then $j_{n-1}=1$ and $A_n=\sqrt{N-2^{n-1}}/\sqrt{N}$. When $c_{n-1}=0$, then

$$A_{n-1}=\sqrt{2^{n-2}}/\sqrt{N-2^{n-1}}$$

and the amplitude of c_k is $A_k=\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}/\sqrt{2}$. Thus, the amplitude of $|c\rangle=|1,0,c_{n-2},\ldots,c_1\rangle$ is

$$\begin{aligned} A &= A_nA_{n-1}\bullet\cdots\bullet A_1 \\ &= \frac{\sqrt{N-2^{n-1}}}{\sqrt{N}}\bullet\frac{\sqrt{2^{n-2}}}{\sqrt{N-2^{n-1}}}\prod_{k=1}^{n-2}\mathrm{e}^{2^k\pi \mathrm{i}ac_k/N}/\sqrt{2} \\ &= \frac{1}{\sqrt{N}}\mathrm{e}^{2\pi \mathrm{i}ac/N}. \end{aligned}$$

When $c_{n-1}=1$, then

$$A_{n-1}=\frac{\sqrt{N-2^{n-1}-2^{n-2}}}{\sqrt{N-2^{n-1}}}\,\mathrm{e}^{2^{n-1}\pi \mathrm{i}ac_{n-1}/N}$$

and $j_{n-2}=1$. According to the case 2)-b1, the amplitude of $|c\rangle=|1,1,0,c_{n-3},\ldots,c_1\rangle$ is $(1/\sqrt{N})\,\mathrm{e}^{2^k\pi \mathrm{i}ac/N}$ and that of $|c\rangle=|1,1,1,c_{n-3},\ldots,c_1\rangle$ is

$$\frac{\sqrt{N-2^{n-1}-2^{n-2}}}{\sqrt{N}}\,\mathrm{e}^{2^k\pi \mathrm{i}a(c_n+c_{n-1})/N}\bullet A_{n-2}\bullet\cdots\bullet A_1.$$

If $N_{n-2}=0$, then $c_{n-3}=0$ and $A_{n-2}=1$, otherwise

$$A_{n-2}=\frac{\sqrt{N-2^{n-1}-2^{n-2}-2^{n-3}}}{\sqrt{N-2^{n-1}-2^{n-2}}}\,\mathrm{e}^{2^{n-1}\pi \mathrm{i}ac_{n-2}/N}$$

and $j_{n-3}=1$. According to the case 2)-b1, the amplitude of $|c\rangle=|1,1,1,0,c_{n-4},\ldots,c_1\rangle$ is $(1/\sqrt{N})\,\mathrm{e}^{2\pi \mathrm{i}ac/N}$ and that of $|c\rangle=|1,1,1,1,c_{n-4},\ldots,c_1\rangle$ is

$$\frac{\sqrt{N-2^{n-1}-2^{n-2}-2^{n-3}}}{\sqrt{N}}\,\mathrm{e}^{2^k\pi \mathrm{i}a(c_n+c_{n-1}+c_{n-2})/N}\bullet A_{n-3}\bullet\cdots\bullet A_1.$$

Similarly, by combining cases 2)-b2 and 2)-b3, we can obtain that the amplitude of $|c\rangle=|1,c_{n-1},\ldots,c_1\rangle$ is $(1/\sqrt{N})\,\mathrm{e}^{2\pi \mathrm{i}ac/N}$, and $\sum_{j=1}^{n}2^{j-1}c_j<N$.

We thus obtain Theorem 1.

In Theorem 1, the QFT over Z_N on $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$ is divided into the transform d_k on each $|a_k\rangle$. Based on this, its circuit can be designed as shown in Fig. 1.

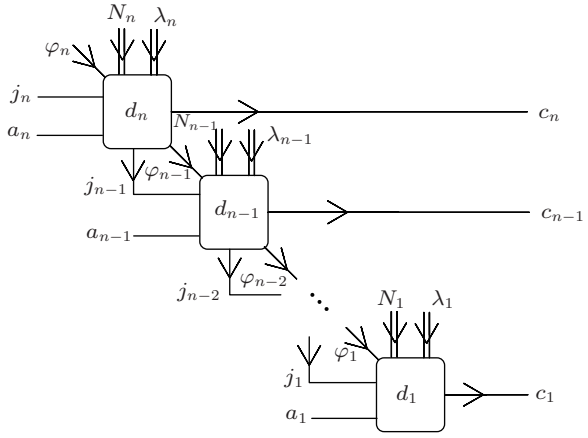


Fig. 1. Circuit of the QFT over Z_N.

Figure 1 is explained as follows.

i) Each symbol is the same as defined in Theorem 1.

ii) A single line represents a quantum signal and a double line represents a classical signal.

iii) The final measurement result is $c=\sum_{k=1}^{n}2^{k-1}c_k$.

Figure 1 shows that the circuit needs to store $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$, φ_k, and $|j_k\rangle$, hence, it requires $(2n+1)$-dimensional quantum register. d_k contains Hadamard transform H,

$$U(q,Q)=\frac{1}{\sqrt{Q}}\begin{bmatrix}\sqrt{q} & \sqrt{Q-q}\\ \sqrt{Q-q} & -\sqrt{q}\end{bmatrix}$$

and phase transform. H and U are all one-bit gate and only used once in d_k. The phase transform is a two-bit gate, which is used n times in d_k. Since the circuit contains $d_1, d_2, \ldots, d_n$, it needs $2n$ one-bit gates and n^2 two-bit gates.

3.2. Circuit of the t-bit semiclassical QFT over Z_N

The t-bit semiclassical QFT over Z_{2^n} needs less quantum computational resource than the QFT over Z_{2^n}, and has higher implementation speed than the single-bit semiclassical QFT over Z_{2^n}.[10] Thus, the transform can balance the tradeoff between the quantum computational resource and speed in the implementation of the QFT. Therefore, we will give the t-bit semiclassical QFT over Z_N.

Definition 2 Suppose that N and t are both positive integers, the binary representation of $N-1$ is $(N_n,N_{n-1},\ldots,N_1)$, $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$ is an arbitrary orthonormal state with orthonormal basis $|0\rangle,|1\rangle,\ldots,|N-1\rangle$,

$$l=\begin{cases}[n/t], t\not|n,\\ l=[n/t]-1, t|n,\end{cases}$$

and $n=\lceil\log N\rceil$. $U_{Z_N^t}$ transforms a block of bits of $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$ entering on the left into one leaving on the right through

$$\begin{aligned}&D_{Z_N^t}^{l+1}:|a_n,a_{n-1},\ldots,a_{lt+1}\rangle|j_{l+1}\rangle\mapsto A_{l+1},\\ &D_{Z_N^t}^{l}:\left|a_{lt},a_{lt-1},\ldots,a_{(l-1)t+1}\right\rangle|j_l\rangle\mapsto A_l,\\ &\cdots,\\ &D_{Z_N^t}^{1}:|a_t,a_{t-2},\ldots,a_1\rangle|j_1\rangle\mapsto A_1,\end{aligned}$$

where

$$\begin{aligned}A_{l+1}=&\frac{\sqrt{N-\lambda_{l+1}}}{\sqrt{N}}\omega_N^{a\sum_{i=lt+1}^{n}2^{i-1}N_i}\\ &\times|N_n,N_{n-1},\ldots,N_{lt+1}\rangle|j_l=j_{l+1}\rangle\\ &+\frac{\sqrt{2^{lt}N_{lt+1}}}{\sqrt{N}}\omega_N^{a\sum_{i=lt+2}^{n}2^{i-1}N_i}\\ &\times|N_n,N_{n-1},\ldots,N_{lt+2},0\rangle|j_l=j_{l+1}-1\rangle+\cdots\\ &+\frac{\sqrt{2^{n-2}N_n}}{\sqrt{N}}\sum_{c'_{n-1},\ldots,c'_{lt+2},c'_{lt+1}}\omega_N^{a\sum_{i=lt+1}^{n-1}c'_i2^{i-1}}\\ &\times\left|0,c'_{n-1},\ldots,c'_{lt+2},c'_{lt+1}\right\rangle|j_l=j_{l+1}-1\rangle.\end{aligned}$$

If $j_i=0$, then

$$A_i=\frac{1}{2^{t/2}}\sum_{c'_{it},c'_{it-1},\ldots,c'_{(i-1)t+1}}\omega_{2^t}^{ac''_i}\left|c'_{it},c'_{it-1},\ldots,c'_{(i-1)t+1}\right\rangle,$$

otherwise

$$\begin{aligned}A_i=&\frac{\sqrt{N-\lambda_{i-1}}}{\sqrt{N-\lambda_i}}\omega_N^{a\sum_{i=(i-1)t+1}^{it}2^{i-1}N_i}\\ &\times\left|N_{it},N_{it-1},\ldots,N_{(i-1)t+1}\right\rangle|j_l=j_{l+1}\rangle\\ &+\frac{\sqrt{2^{(i-1)t}N_{lt+1}}}{\sqrt{N-\lambda_i}}\sum_{c'_{(i-1)t+1}}\omega_N^{a(2^{(i-1)t}c'_{(i-1)t+1}+\sum_{i=(i-1)t+2}^{it}2^{i-1}N_i)}\\ &\times\left|N_{it},N_{it-1},\ldots,N_{(i-1)t+2},c'_{(i-1)t+1}\right\rangle|j_l=j_{l+1}-1\rangle+\cdots\\ &+\frac{\sqrt{2^{it-2}N_n}}{\sqrt{N-\lambda_i}}\sum_{c'_{it-1},\ldots,c'_{(i-1)t+1}}\omega_N^{a\sum_{i=(i-1)t+1}^{it-1}c'_i2^{i-1}}\\ &\times\left|0,c'_{it-1},\ldots,c'_{(i-1)t+1}\right\rangle|j_l=j_{l+1}-1\rangle,\end{aligned}$$

where c'_i is 0 or 1,

$$\begin{aligned}&\lambda_i=\lambda_{i+1}+\sum_{j=(i-1)t+1}^{it}2^{j-1}N_j,\\ &\lambda_{l+1}=\sum_{i=lt+1}^{n}2^{i-1}N_i,\quad i=1,2,\ldots,l,\end{aligned}$$

$j_{l+1}=1$, and $\omega_N=\mathrm{e}^{2\pi\mathrm{i}/N}$. Therefore $U_{Z_N^t}$ is called the t-bit semiclassical QFT over Z_N, and $D_{Z_N^t}^{j}$ is called the t-bit quantile transform.

Theorem 2 Suppose that $|0\rangle,|1\rangle,\ldots,|N-1\rangle$ is an orthonormal basis, U_{F} is the QFT over Z_N, $U_{Z_N^t}$ is t-bit semiclassical QFT over Z_N, then the probability of $|c\rangle=|c_n,c_{n-1},\ldots,c_1\rangle$ obtained by U_{F} on $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$ will be equal to that by $U_{Z_N^t}$.

Proof To prove the theorem, we only need to prove that the amplitude of $|c\rangle=|c_n,c_{n-1},\ldots,c_1\rangle$ obtained by U_{F} on $|a\rangle=|a_n,a_{n-1},\ldots,a_1\rangle$ is equal to that by $U_{Z_N^t}$.

$U_{Z_N^t}$ carries $|a\rangle$ into $|c\rangle$, whose amplitude is as follows.

(I) If $(c_n,c_{n-1},\ldots,c_{lt+1})\neq(N_n,N_{n-1},\ldots,N_{lt+1})$, A_{l+1} contains the state $|c_n,c_{n-1},\ldots,c_{lt+1}\rangle=|N_n,N_{n-1},\ldots,N_{lt+2},0\rangle$. When $N_{lt+1}=1$, the amplitude of $|c_n,c_{n-1},\ldots,c_{lt+1}\rangle$ is

$$\frac{\sqrt{2^{lt}N_{lt+1}}}{\sqrt{N}}\omega_N^{a(2^{lt}c_{lt+1}+\sum_{i=lt+2}^{n}2^{i-1})}$$

and $j_{l-1}=0$. Furthermore, according to the form of $A_l,\ldots,A_1$, we can obtain that the amplitude of $|c\rangle$ is

$$\begin{aligned}&\frac{\sqrt{2^{lt}N_{lt+1}}}{\sqrt{N}}\omega_N^{a(2^{lt}c_{lt+1}+\sum_{i=lt+2}^{n}2^{i-1})}\prod_{i=1}^{l}\frac{1}{2^{t/2}}\omega_{2^t}^{ac''_i}\\ &=\frac{1}{\sqrt{N}}\omega_N^{ac}.\end{aligned}$$

When $N_{lt+1}=0$,

$$|c_n,c_{n-1},\ldots,c_{lt+1}\rangle=|N_n,N_{n-1},\ldots,N_{lt+2},1\rangle.$$

But the state is not contained in A_{l+1}.

So, only when $N_{lt+1}=1$, is

$$(c_n,c_{n-1},\ldots,c_{lt+1})\neq(N_n,N_{n-1},\ldots,N_{lt+1})$$

contained in A_{l+1}.

Similarly, if $(c_n,c_{n-1},\ldots,c_{lt+1})$ is in other form and

$$\sum_{i=lt+1}^{n}2^{i-1}c_i<\sum_{i=lt+1}^{n}2^{i-1}N_i,$$

then the amplitude of $|c\rangle$ is

$$\frac{1}{\sqrt{N}}\omega_N^{ac}.$$

(II) If $(c_n,c_{n-1},\ldots,c_{lt+1})=(N_n,N_{n-1},\ldots,N_{lt+1})$, then the amplitude of $|c_n,c_{n-1},\ldots,c_{lt+1}\rangle$ is

$$\frac{\sqrt{N-\lambda_{l+1}}}{\sqrt{N}}\omega_N^{a\sum_{i=lt+1}^{n}2^{i-1}N_i}.$$

(II)-a When

$$\left|c_{lt},c_{lt-1},\ldots,c_{(l-1)t+1}\right\rangle\neq\left|N_{lt},N_{lt-1},\ldots,N_{(l-1)t+1}\right\rangle$$

and

$$\sum_{i=(l-1)t+1}^{lt}2^{i-1}c_i<\sum_{i=(l-1)t+1}^{lt}2^{i-1}N_i,$$

according to case (I), the amplitude of $|c\rangle$ is

$$\frac{1}{\sqrt{N}}\omega_N^{ac}.$$

(II)-b When

$$\left|c_{lt},c_{lt-1},\ldots,c_{(l-1)t+1}\right\rangle=\left|N_{lt},N_{lt-1},\ldots,N_{(l-1)t+1}\right\rangle,$$

the amplitude of $\left|c_n,c_{n-1},\ldots,c_{(l-1)t+1}\right\rangle$ is

$$\frac{\sqrt{N-\lambda_l}}{\sqrt{N-\lambda_{l+1}}}\omega_N^{a\sum_{i=(l-1)t+1}^{it}2^{i-1}N_i}.$$

If

$$\left|c_{(l-1)t},c_{(l-1)t-1},\ldots,c_{(l-1)t+1}\right\rangle\neq\left|N_{(l-1)t},N_{(l-1)t-1},\ldots,N_{(l-2)t+1}\right\rangle,$$

according to case (I), the amplitude of $|c\rangle$ is

$$\frac{1}{\sqrt{N}}\omega_N^{ac}.$$

If

$$\left|c_{(l-1)t},c_{(l-1)t-1},\ldots,c_{(l-1)t+1}\right\rangle=\left|N_{(l-1)t},N_{(l-1)t-1},\ldots,N_{(l-2)t+1}\right\rangle,$$

then the amplitude of

$$\left|\left|c_n,c_{n-1},\ldots,c_{(l-1)t+1}\right\rangle=\left|N_n,N_{n-1},\ldots,N_{(l-2)t+1}\right\rangle\right\rangle$$

is

$$\frac{\sqrt{N-\lambda_l}}{\sqrt{N-\lambda_{l+1}}}\omega_N^{a\sum_{i=(l-1)t+1}^{n}2^{i-1}N_i}.$$

Similarly, by combining cases (I) and (II), we can obtain that the amplitude of $|c\rangle$ is

$$\frac{1}{\sqrt{N}}\omega_N^{ac}$$

and $\sum_{j=1}^{n}2^{j-1}c_j<N$.

From Definition 1, we obtain

$$U_{\mathrm{F}}|a\rangle=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{ak}|k\rangle.$$

Then, after U_{F} acts on $|a\rangle$, the amplitude of $|c\rangle=|c_n,c_{n-1},\ldots,c_1\rangle$ is

$$\frac{1}{\sqrt{N}}\mathrm{e}^{2\pi\mathrm{i}ac/N}.$$

We thus obtain Theorem 2.

Then, we can conclude that the t-bit semiclassical QFT over Z_N can actually realize the QFT over Z_N. Its circuit is illustrated in Fig. 2.

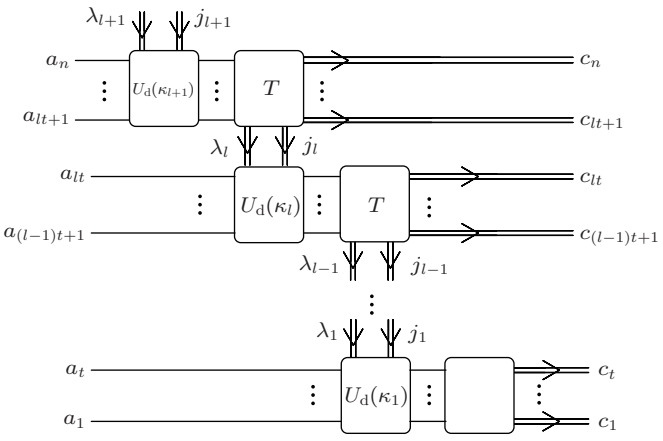


Fig. 2. Circuit of the t-bit semiclassical QFT over Z_N.

Figure 2 is explained as follows.

I)

$$\kappa_{l+1}=\frac{1}{2^{lt+1}}\sum_{j=lt+1}^{n}2^{j-1}N_j$$

and

$$\kappa_i=\frac{1}{2^{(i-1)t+1}}\sum_{j=(i-1)t+1}^{it}2^{j-1}N_j,$$

where $i=1,\ldots,l$.

II) $U_{\mathrm{d}}(\kappa_{l+1})$ is the QFT over $Z_{\kappa_{l+1}}$, in which $\sum_{j=lt+1}^{n}2^{j-1}N_j$ and 2^{x+lt+1} respectively replace κ_{l+1} and 2^x.

III) If $j_i = 1$, then $U_{\rm d}(\kappa_i)$ is the QFT over Z_{κ_i} in which $\sum_{j=(i-1)t+1}^{it} 2^{j-1}N_j$ and $2^{x+(i-1)t+1}$ respectively replace κ_i and 2^x, otherwise it is the QFT over Z_{2^t}, where $i = 1,\ldots,l$.

IV) T is the detector.

V) The final measurement result is $c = \sum_{k=1}^{n} 2^{k-1}c_k$.

Figure 2 shows that $U_{\rm d}(\kappa_i)$ is the QFT over Z_{κ_i}, which requires a $(2t+1)$-dimensional quantum register. Since the other value is a classical value and the quantum register can be recycled, the t-bit semiclassical QFT over Z_N only needs $(2t+1)$-dimensional quantum register. $U_{\rm d}(\kappa_i)$ requires $2t$ one-bit gates and t^2 two-bit gates, and these gates can be recycled, so the t-bit semiclassical QFT over Z_N needs $2t$ one-bit gates and t^2 two-bit gates.

In conclusion, the quantum register, one-bit gate and two-bit gate for the t-bit semiclassical QFT over Z_N are, respectively, $1/l$, $1/l$, and $1/l^2$ times as large as those of the QFT over Z_N. Like the t-bit semiclassical QFT over Z_{2^n}, the t-bit semiclassical QFT over Z_N can also balance the tradeoff between the quantum computational resource and speed in the implementation of the QFT over Z_N, and the requirements for the two-bit gate is reduced obviously, which can reduce the difficulty in realizing the QFT over Z_N. Meanwhile, low-dimensional quantum register is required, which can provide a solution for implementing the QFT over Z_N when N is large.

So far, realizing that the quantum algorithms are all based on the QFT over Z_{2^m}, where $m = \lceil \log N \rceil$,[7] but not on the QFT over Z_N, the former is easier to implement than the latter. However, when both of these QFTs are used for implementing quantum algorithms, like Zalka's algorithm, the success probability of the latter is highly accurate, even much more sp than that of the former. Now we will give an example to explain the result.

Example Zalka's algorithm requires three quantum registers. It can obtain superposition state

$$\frac{1}{q\sqrt{q}} \sum_{x',y'=0}^{q-1} \sum_{y=0}^{q-1} \omega_q^{(x_0-dy)x'} \omega_q^{yy'} \left|x'\right\rangle \left|y'\right\rangle$$

in double QFT over Z_q, where $\omega_q = {\rm e}^{2\pi {\rm i}/q}$ and q is a prime. Since

$$\sum_{y=0}^{q-1} \omega_q^{(x_0-dy)x'} \omega_q^{yy'} = \begin{cases} q, & y' = dx' \bmod q, \\ 0, & y' \neq dx' \bmod q, \end{cases}$$

we obtain

$$\frac{1}{\sqrt{q}} \sum_{x'=0}^{q-1} \omega_q^{x_0x'} \left|x'\right\rangle \left|y' = dx' \bmod q\right\rangle.$$

By measuring, we obtain a pair x', y' from which we can calculate $d = (x')^{-1}y' \bmod q$ as long as $x' \neq 0$. Thus, the success probability is close to 1. If we replace each of the two QFTs over Z_q with QFT over Z_{2^m}, we will obtain

$$\frac{1}{2^m\sqrt{2^m}} \sum_{x',y'=0}^{2^m-1} \sum_{y=0}^{2^m-1} \omega_{2^m}^{(x_0-dy)x'} \omega_{2^m}^{yy'} \left|x'\right\rangle \left|y'\right\rangle,$$

where $m = \lceil \log q \rceil$. By measuring, we obtain a pair x', y', which may not satisfy $y' = dx' \bmod q$, and the success probability is less than 1.

4. Conclusions

In this paper, we gave the circuit of the QFT over Z_N. Because of the difficulty in building a high-dimensional quantum register, in this paper we presented the t-bit semiclassical QFT over Z_N, which admits a tradeoff between the quantum computational resource and speed in the implementation of the QFT over Z_N. We have further designed its circuit, which leads to the implementation of quantum algorithms, like Zalka's algorithm, whose success probability is highly accurate, even much more so than that of the QFT over Z_{2^m} ($m = \lceil \log N \rceil$).

References

[1] Shor P W 1997 *SIAM Journal on Computing* **26** 1484
[2] Grover L K 1996 *Proceeding of the* 28*th ACM Symposium on Theory of Computation*, 2002, May 22–24, New York, USA
[3] Zheng S B 2005 *Chin. Phys.* **14** 11
[4] Zhong P C and Bao W S 2008 *Chin. Phys. Lett.* **25** 8
[5] Zhou N R and Zeng G H 2005 *Chin. Phys.* **14** 11
[6] Hallgren S 2002 *Proceedings of the* 34*th Annual ACM Symposium on Theory of Computing*, 2002, May 19–21, Montreal, Canada
[7] Proos J and Zalka C 2003 *Quantum Information & Computation* **3** 4
[8] Li J, Peng X, Du J and Suter D 2012 *Nature Sci. Rep.* **2** 260
[9] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (London: Cambridge University Press) Chap. 5, p. 216
[10] Griffiths R B and Niu C S 1996 *Phys. Rev. Lett.* **76** 3228
[11] Chiaverini J, Britton J, Leibfried D, Knill E, Barrett M D, Blakestad R B, Itano W M, Jost J D, Langer C, Ozeri R, Schaetz T and Wineland D J 2005 *Science* **308** 997
[12] Fu X Q, Bao W S, Zhou C and Song Z 2012 *Chin. Sci. Bull.* **57** 1