Comment on Demonstrations of Shor's Algorithm in the Past Decades

Zhengjun Cao[1,*], Zhenfu Cao,[2] Lihua Liu[3]

Abstract. We remark that the experimental demonstrations of Shor's algorithm in the past decades are falsely claimed and flawed, because they had used too less qubits in the first quantum register to accomplish the step of Continued Fraction Expansion in Shor's algorithm. More worse, the amount of qubits used in some experiments are too less to represent all residues modulo n, which means that the number n cannot be truly involved in the related computations.

Keywords. Shor's algorithm; continued fraction expansion; quantum Fourier transformation; quantum modular exponentiation

1 Introduction

It is well known that factoring an integer n can be reduced to finding the order of some integer x modulo n, i.e., $\mathrm{ord}_n(x)$. So far, there is not a polynomial time algorithm run on classical computers which can be used to compute the order. But in 1994, Shor [1] claimed that his algorithm can be used to compute $\mathrm{ord}_n(x)$ on a quantum computer.

Since 2001, some teams have reported that they had successfully factored 15 into 3×5 using Shor's algorithm. We shall have a close look at those experimental demonstrations and argue that all these demonstrations are falsely claimed because they violate the necessary condition that the selected number q must satisfy $n^2 \le q < 2n^2$. Essentially, these demonstrations have no relation to the Shor's algorithm.

2 Preliminaries

A quantum analogue of a classical computer operates with quantum bits involving quantum states. The state of a quantum computer is described as a basis vector in a Hilbert space. A qubit is a quantum state $|\Psi\rangle$ of the form $|\Psi\rangle = a|0\rangle + b|1\rangle$, where the amplitudes $a, b \in \mathbb{C}$ such that

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

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

[3] Department of Mathematics, Shanghai Maritime University, Shanghai, China.

$|a|^2 + |b|^2 = 1$, $|0\rangle$ and $|1\rangle$ are basis vectors of the Hilbert space. Here, the *ket* notation $|x\rangle$ means that x is a quantum state. The state of a quantum system having n qubits is a point in a 2^n-dimensional vector space. Given a state $\sum_{i=0}^{2^n-1} a_i|\chi_i\rangle$, where the amplitudes are complex numbers such that $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$ and each $|\chi_i\rangle$ is a basis vector of the Hilbert space, if the machine is measured with respect to this basis, the probability of seeing basis state $|\chi_i\rangle$ is $|a_i|^2$.

Two quantum mechanical systems are combined using the tensor product. For example, a system of two qubits $|\Psi\rangle = a_1|0\rangle + a_2|1\rangle$ and $|\Phi\rangle = b_1|0\rangle + b_2|1\rangle$ can be written as

$$|\Psi\rangle|\Phi\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1b_1 \\ a_1b_2 \\ a_2b_1 \\ a_2b_2 \end{pmatrix}$$

We shall also use the shorthand notations $|\Psi, \Phi\rangle$. We call a quantum state having two or more components *entangled* state, if it is not a product state. According to the Copenhagen interpretation of quantum mechanics, measurement causes an instantaneous collapse of the wave function describing the quantum system into an eigenstate of the observable state that was measured. If entangled, one object cannot be fully described without considering the other(s).

Operations on a qubit are described by 2×2 unitary matrices. Of these, some of the most important are

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

where H denotes the Hadamard gate. Clearly, $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Operations on two qubits are described by 4×4 unitary matrices. Of these, the most important operation is the controlled-NOT, denoted by CNOT. The action of CNOT is given by $|c\rangle|t\rangle \to |c\rangle|c \oplus t\rangle$, where $\oplus$ denotes addition modulo 2. The matrix representation of CNOT is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Likewise, operations on ℓ qubits are described by $2^\ell \times 2^\ell$ unitary matrices.

There is another method to describe linear operators performed on *multiple qubits.* Suppose that V and W are vector spaces of dimension 2^μ and 2^ν (they describe quantum systems corresponding to μ and ν qubits, respectively). Suppose $|v\rangle$ and $|w\rangle$ are vectors in V and W, and A and B are linear operators on V and W, respectively. Then we can define a linear operator $A \otimes B$ on $V \otimes W$ by the equation

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle.$$

3 Description of Shor's algorithm

The Shor's algorithm requires two quantum registers. At the beginning of the algorithm, one has to find $q = 2^s$ for some integer s such that $n^2 \leq q < 2n^2$, where n is to be factored. It then proceeds as follows.

- *Initialization.* Put register-1 in the uniform superposition
$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0\rangle.$$
- *Computation.* Keep a in register-1 and compute x^a in register-2 for some randomly chosen integer x. It gives the state
$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|x^a\rangle.$$
- *Fourier Transformation.* Performing Fourier transform on register-1, we obtain the state
$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle|x^a\rangle.$$
- *Observation.* It suffices to observe register-1. The probability p that the machine reaches the state $|c, x^k\rangle$ is
$$\left|\frac{1}{q}\sum_{a:\, x^a \equiv x^k}\exp(2\pi iac/q)\right|^2,$$
where $0 \leq k < r = \text{ord}_n(x)$, the sum is over all $a\,(0 \leq a < q)$ such that $x^a \equiv x^k$.
- *Continued Fraction Expansion.* If there is a d such that
$$\frac{-r}{2} \leq dq - rc \leq \frac{r}{2},$$
then the probability of seeing $|c, x^k\rangle$ is greater than $1/3r^2$. Since $q \geq n^2$, we have $\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q} \leq \frac{1}{2n^2} < \frac{1}{2r^2}$. Then d/r can be obtained by rounding c/q.

4 The complexity argument of Shor's algorithm

At the end of the Shor's factoring algorithm, one should observe the first register and denote the measured result as an integer c. Its complexity argument comprises:

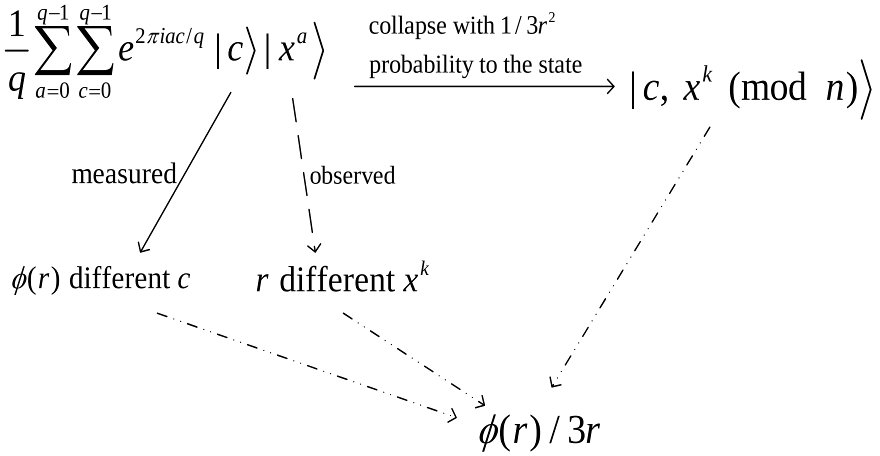
(1) The probability p of seeing a quantum state $|c, x^k\,(\text{mod}\, n)\rangle$ such that $r/2 \geq \{rc\}_q$ is greater than $1/3r^2$, where n is the integer to be factored, q is a power of 2 satisfying $n^2 \leq q < 2n^2$ and $r = \text{ord}_n(x)$.

(2) There are $\phi(r)$ possible c which can be used to compute the order r.

(3) The measured number in the second register, i.e., x^k, takes r possible values $1, x, x^2, \cdots, x^{r-1}$.

(4) The success probability of running the algorithm once is greater than $r \cdot \phi(r) \cdot \frac{1}{3r^2}$. By $\phi(r)/r > \xi/\log\log r$ for some constant ξ, it concludes that the algorithm runs in polynomial time.

The Shor's complexity argument can be depicted by the following Graph-1.



Graph-1: Shor's complexity argument

5 Demonstrations of Shor's algorithm

In 2001, it was reported that Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3 × 5, using a quantum computer with 7 qubits, 3 qubits in register-1 and 4 qubits in register-2 (see Figure-1) [2].

In 2007, a group at University of Queensland reported an experimental demonstration of a compiled version of Shor's algorithm. They factored 15 into 3 × 5, using 7 qubits either, 3 qubits in register-1 and 4 qubits in register-2 (see Figure-2) [3].

In 2007, a group at University of Science and Technology of China reported another experimental demonstration of a complied version of Shor's algorithm. They factored 15 into 3 × 5 using 6 qubits only, 2 qubits in register-1 and 4 qubits in register-2 (see Figure-3) [4].

In 2012, a group at University of California, Santa Barbara, reported a new experimental demonstration of a compiled version of Shor's algorithm. They factored 15 into 3 × 5 using 3 qubits either, 1 qubits in register-1 and 2 qubits in register-2 (see Figure-4) [5].

In 2015, Monz, et al. [6] have reported a new demonstration of factoring 15 using a scalable Shor algorithm with an ion-trap quantum computer.

Demonstrations	qubits in register-1	qubits in register-2
Figure 1, Ref.[2]	3	4
Figure 2, Ref.[3]	3	4
Figure 3, Ref.[4]	2	4
Figure 4, Ref.[5]	1	2
Figure 5, Ref.[6]	1	4

Table 1: The number of qubits used in some demonstrations.

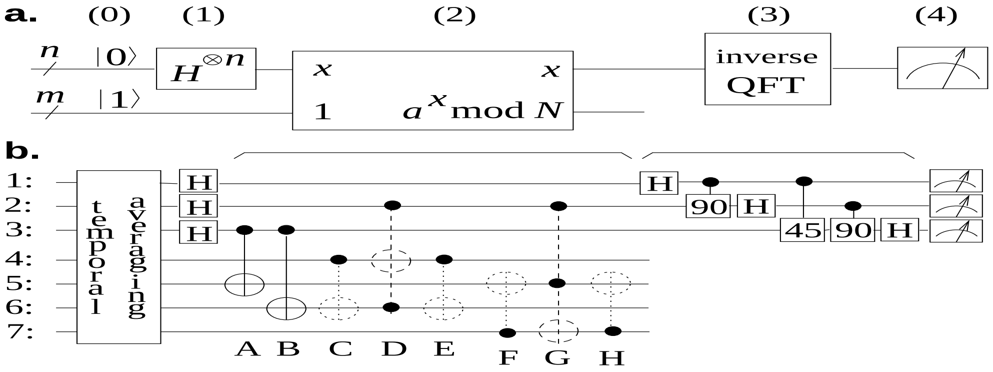


Figure 1: Demonstration (IBM, $N = 15, a = 7$)

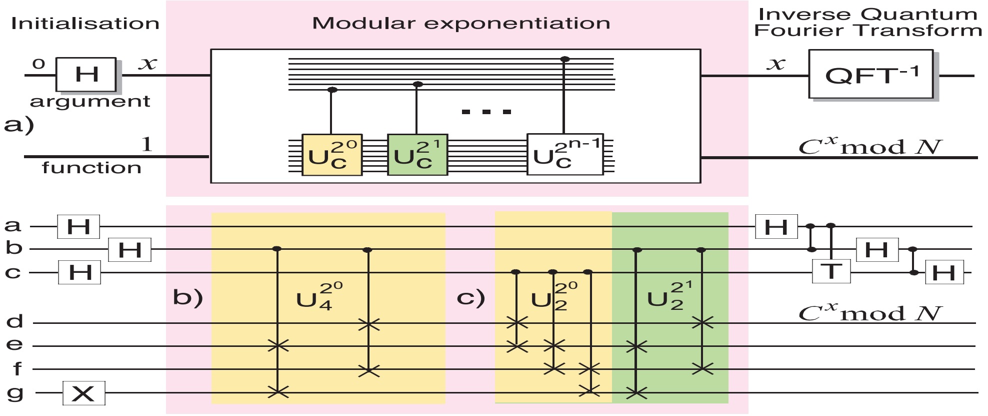


Figure 2: Demonstration (University of Queensland, $N = 15, C = 4$)

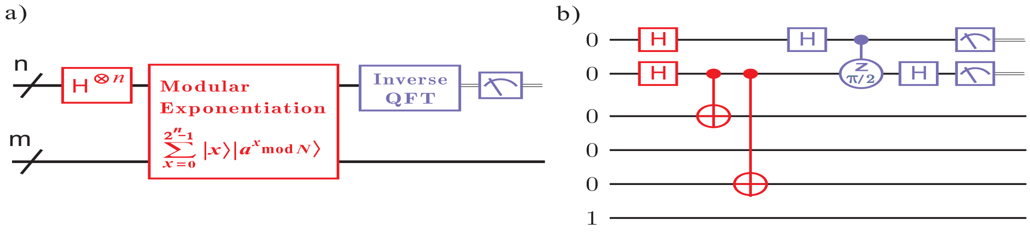


Figure 3: Demonstration (University of Science and Technology of China, $N = 15, a = 11$)

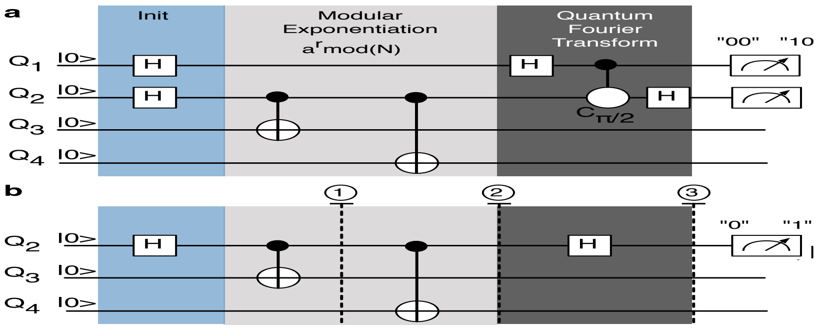


Figure 4: Demonstration (University of California, Santa Barbara, $N = 15$)

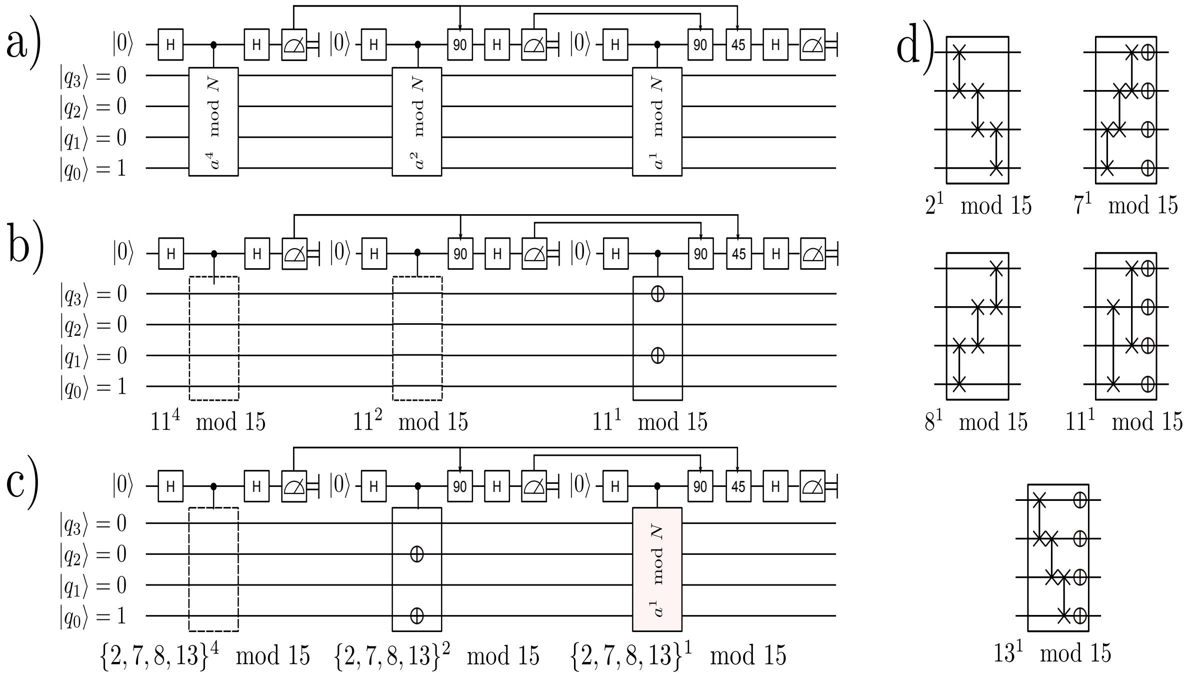


Figure 5: Demonstration (Universität Innsbruck, Technikerstr, $N = 15$)

6 The demonstrations are falsely claimed and flawed

6.1 8 qubits should be used in the first register

All these demonstrations are falsely claimed because they do not meet the necessary condition that $15^2 < 2^8 < 2 \times 15^2$, which means 8 qubits should be used in the first register. Obviously, the last step of Continued Fraction Expansion in Shor's algorithm can not be accomplished if less qubits are used in the first register.

6.2 The Shor's complexity argument does not apply to these demonstrations

The Shor's complexity argument does not apply to these demonstrations because less qubits are used in the register-1. In such case, the probability p of seeing a quantum state $|c, x^k \,(\mathrm{mod}\, n)\rangle$ such that $r/2 \geq \{rc\}_q$ is greater than $1/3r^2$ can not be properly estimated using the original Shor argument.

Here is a brief description of the original Shor argument for the estimation of the probability p. Setting $a = br + k$ for some integer b and the order $r = \mathrm{ord}_n(x)$, the probability p is

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} e^{2\pi i (br+k)c/q} \right|^2 .$$

Then it argues that the probability p equals to

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} e^{2\pi i b \{rc\}_q/q} \right|^2 .$$

Writing the above sum into an integral, we obtain

$$\frac{1}{q} \int_{b=0}^{\lfloor \frac{(q-k-1)}{r} \rfloor} e^{2\pi i b \{rc\}_q/q} \mathrm{d}b + O\left(\frac{\lfloor (q-k-1)/r \rfloor}{q} (e^{2\pi i \{rc\}_q/q} - 1) \right).$$

Taking $u = rb/q$, we have

$$\frac{1}{r} \int_0^{\frac{r}{q} \lfloor \frac{q-k-1}{r} \rfloor} \exp\left(2\pi i u \frac{\{rc\}_q}{r} \right) \mathrm{d}u$$

Taking into account that $k < r$, we can obtain the approximation

$$\frac{1}{r} \int_0^1 \exp\left(2\pi i u \frac{\{rc\}_q}{r} \right) \mathrm{d}u.$$

Hence, we have

$$\left| \frac{1}{r} \int_0^1 \exp\left(2\pi i u \frac{\{rc\}_q}{r} \right) \mathrm{d}u \right| \geq 2/(\pi r)$$

Therefore,

$$p \geq \frac{4}{\pi^2 r^2} > 1/3r^2.$$

6.3 The high dimension unitary operator for quantum modular exponentiation is falsely specified

In math, the operators performed in the process of Shor's algorithm can be described as follows.

$$
\begin{array}{lcl}
|0\rangle|0\rangle & \xrightarrow{H^{\otimes s}} & \dfrac{1}{\sqrt{q}}\displaystyle\sum_{a=0}^{q-1}|a\rangle|0\rangle \\
 & & \text{(Hadamard gate } H \text{ performed on each qubit in Register-1)} \\
 & \xrightarrow{\mathcal{U}} & \dfrac{1}{\sqrt{q}}\displaystyle\sum_{a=0}^{q-1}|a\rangle|x^a\rangle \\
 & & \text{(Unitary operator } \mathcal{U} \text{ performed on all qubits in Register-2)} \\
 & \xrightarrow{\text{QFT}} & \dfrac{1}{q}\displaystyle\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle|x^a\rangle \\
 & & \text{(Quantum Fourier Transformation performed on all qubits in Register-1)} \\
 & \overset{\text{measurement}}{\dashrightarrow} & |c, x^k\rangle
\end{array}
$$

We know the wanted superposition in the first register is modulated by the following procedure. First, a Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is performed on each qubit to obtain the s intermediate states of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Second, combine all these states using the tensor product.

$$
\begin{array}{cl}
 & \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \dfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
 & \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 = & \dfrac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\
 & \vdots \\
 & \underbrace{\dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{s \text{ qubits}} = \dfrac{1}{\sqrt{q}}\displaystyle\sum_{a=0}^{q-1}|a\rangle
\end{array}
$$

Note that the procedure works well because all those involved pure states are in binary form.

We would like to stress that if two pure states are in decimal representations $|x\rangle, |x^2\rangle$, then we can not directly combine them to obtain $|x^3\rangle$. Suppose that the binary strings for integers x, x^2 are $b_k \cdots b_0$, $b'_i \cdots b'_0$. We have $|x\rangle \otimes |x^2\rangle = |b_k \cdots b_0 b'_i \cdots b'_0\rangle = |2^{i+1}x + x^2\rangle$. Thus,

$$
\frac{1}{\sqrt{2}}(|1\rangle + |x\rangle) \otimes \frac{1}{\sqrt{2}}(|1\rangle + |x^2(\mathrm{mod}\, n)\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|1\rangle + |x^{2^{s-1}}(\mathrm{mod}\, n)\rangle\right) \neq \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|x^a(\mathrm{mod}\, n)\rangle,
$$

where $q = 2^s$. Some people are misled by the conventional equation

$$(1+x)(1+x^2)(1+x^{2^2})\cdots(1+x^{2^{s-1}}) = \sum_{a=0}^{q-1} x^a,$$

which can be computed by fast squaring algorithm, and simply take for granted that quantum modular exponentiation is in polynomial time.

We remark that the specified quantum unitary operations used on each qubit or each group of qubits in the second quantum register in these demonstrations are flawed. In fact, these low dimension operators can not be composed to a high dimension unitary operator $\mathcal{U}$ such that

$$\mathcal{U}: \ \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0\rangle \ \longrightarrow \ \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|x^a\rangle.$$

In other words, these demonstrations failed to specify the procedure of quantum modular exponentiation. In short, nobody has successfully described the structure of the high dimension unitary operator $\mathcal{U}$.

6.4 Further remarks

We remark that the principles behind these demonstrations have not been explained properly, including their correctness and complexity.

In Figure 2, it directly denotes the output of the second register by $C^x \mod N$. Clearly, the authors confused the number $C^x \mod N$ with the state $|C^x \mod N\rangle$. By the way, the state in the second register is the superposition $\frac{1}{\sqrt{8}}\sum_{x=0}^{7}|C^x \mod N\rangle$ instead of the pure state $|C^x \mod N\rangle$.

In Figure 4, only 3 qubits are used in the compiled version. Clearly, the residues $0, 1, 2, \cdots, 14$ of module 15 can not be represented by 3 qubits. In such case, how to ensure that the modular 15 is really involved in the computation? It is certain that the demonstration is unbelievable.

In Figure 5, to modulate the wanted quantum state in the register-2, one has to find an efficient and universal quantum modular exponentiation method, which does not depend on any special bases. But the proposed circuit diagram shows that the method does depend on the different bases. It is not universal. Concretely, for base 11 one has to use the circuit b). For bases 2, 7, 8, 13, the circuit c) should be used. But even worse, both two circuits cannot generate the wanted quantum state in the register-2 in the original Shor's algorithm. It claims [6] that the scalable Shor algorithm is based on the Kitaev's result [7]. In the page 2 (left column) of [6], it writes:

> In Ref.[7] Kitaev notes that, if only the classical information of the QFT (such as the period r) is of interest, $2n$ qubits subject to a QFT can be replaced by a single qubit. This approach, however, requires qubit-recycling (specifically: in-sequence single-qubit readout and state reinitialization) paired with feed-forward to compensate for the reduced system size.

But we find the claim is wrong. In fact, Kitaev only claimed that factoring can be reduced to the Abelian Stabilizer Problem (ASP). Throughout the paper [7], He did not claim that 2ℓ qubits subject to a Quantum Fourier Transformation (QFT) can be replaced by a single qubit if only the classical information of the QFT (such as the period r) is of interest. We here want to stress that the authors [6] misunderstand the purpose of using QFT in Shor algorithm. The aim of applying QFT to the register-1 is to accumulate the wanted state $|c, x^k \,(\bmod\, n)\rangle$ such that it is possibly observed with significant probability. QFT has no direct relation to the order r. In fact, r is deduced by rounding $\frac{c}{q}$.

7 Conclusion

We point out that the experimental demonstrations of Shor's algorithm in the past decades are falsely claimed and flawed. These demonstrations have misled researches who studying quantum computing and modern cryptography. Taking into account the development of quantum computer, especially the awful performance of D-Wave Two which was advertised as a 512-qubit quantum computer [8], and some unsolved questions about the Shor's algorithm [9, 10], we do not think that Shor's algorithm will become a real threat to modern public key cryptosystems, such as RSA and ElGamal.

Acknowledgements. This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001), and the Shanghai Leading Academic Discipline Project (S30104).

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. Vandersypen, et al.: Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance, Nature 414 (6866): 883-887, arXiv:quant-ph/0112176 (2001)

[3] B. Lanyon, et al.: Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement", Physical Review Letters 99 (25): 250505. arXiv:0705.1398 (2007)

[4] C.Y. Lu, et al.: Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits, Physical Review Letters 99 (25): 250504, arXiv:0705.1684 (2007)

[5] E. Lucero, et al.: Computing Prime Fctors with a Josephson Phase Qubit Quantum Processor. Nature Physics 8, 719-723, 2012. arXiv:1202.5707 (2012)

[6] T. Monz, et al.: Realization of a scalable Shor algorithm. http://arxiv.org/abs/1507.08852 (2015)

[7] A. Kitaev: Quantum measurements and the Abelian Stabilizer Problem. http://arxiv.org/abs/quant-ph/9511026 (1995)

[8] http://en.wikipedia.org/wiki/D-Wave_Systems

[9] Z.J. Cao and Z.F. Cao: On Shor's Factoring Algorithm with More Registers and the Problem to Certify Quantum Computers, http://arxiv.org/abs/1409.7352 (2014)

[10] Z.J. Cao, Z.F. Cao and L.H. Liu: Remarks on Quantum Modular Exponentiation and Some Experimental Demonstrations of Shor's Algorithm, http://arxiv.org/abs/1408.6252 (2014)