Fundamental Journal of Modern Physics
ISSN: 2249-9768
Volume 18, Issue 1, 2022, Pages 27-44
This paper is available online at http://www.frdint.com/
Published online October 25, 2022

THE PROOF THAT THE NON-CLONING THEOREM OF QUANTUM STATES DOES NOT HOLD

(The physical basis for the absolute secrecy of quantum communication does not exist)

XIAOCHUN MEI

Institute of Innovative Physics
Fuzhou, Fujian
China
e-mail: ycwlyjs@yeah.net

Abstract

W. K. Wootters and W. H. Zurek proposed "the non-cloning theorem of quantum superposition states" in 1982. H. P. Yuen proved that single quantum states satisfying orthogonal condition $\langle \varphi_i | \varphi_j \rangle = 0$ can be cloned in 1986, which should actually be called as "the cloning theorem of orthogonal quantum states". This paper proves that the proofs of these two theorems are not correct. The reasons are below. 1. Both theorems assumed that the quantum clone operator $\hat{U}$ does not change the form of arbitrary wave function $|\varphi_i\rangle$, but can change a fixed initial state wave function $|S\rangle$ into $|\varphi_i\rangle$. Such an operator can not exist in mathematics and is impossible in physics unless it is a unit operator.

Keywords and phrases: quantum mechanics, non-cloning theorem of quantum states, cloning operator, single quantum orthogonal state, quantum superposition state, laser, quantum communication.

Received September 17, 2022; Accepted September 29, 2022

2. For example, for the ground state and some excited states of hydrogen atom, the orthogonal condition $\langle \varphi_k | \varphi_i \rangle = 0$ holds, so they are clonable according to the proof method of Yuen. However, due to some forbidden transition rules, they can not be cloned. 3. For the quantum superposition state $|\varphi\rangle$ with the eigenstate's number $N > 2$, infinite numbers of orthogonal wave functions $|\psi\rangle \neq |\varphi\rangle$ can always be found to satisfy the clonable condition $\langle \psi | \varphi \rangle = 0$ or $\langle \psi | \varphi \rangle = 1$. So the proofs of Yuen and Wootters are contradictory. 4. A large number of experiments have proved that single quantum states of microscopic particles can be cloned, such as the generation of laser. But these processes involve complex interactions between electrons and photons that can not be described by quantum cloning operators. 5. In the actual operation process of quantum communication, what sent and received are quantum keys composed of single polarization states of photons, all of them can be cloned. Therefore, the conclusion of this paper is that the non-cloning theorem of quantum states is an ambiguous, contradictory and wrong proposition and meaningless. The so-called unconditional secrecy of quantum communication has not any physical foundation and can not be achieved.

1. Introduction

This paper comprehensively and carefully analyzes the so-called non-cloning theorem of quantum states and proves that the theorem can not hold. More specifically, it is meaningless. The key problem is that the definition of quantum cloning operator can not exist in mathematics and is impossible in physics. Based on the non-cloning theorem of quantum states, the absolute confidentiality of quantum communication has not any physical foundation and is possible to realize.

In 1982, W. K. Wootters and W. H. Zurek published a paper proposing this famous theorem [1]. The proof of Wootters and Zurek was only for quantum superposition states and concluded that quantum superposition states could not be cloned. For single quantum polarization states, Wootters and Zurek believed that they were possible to be cloned. In their paper, there was a literal statement of the idea, but had no rigorous proof.

In 1986, H. P. Yuen published a paper to prove that the single quantum states which satisfied the orthogonality condition $\langle \psi_i | \varphi_i \rangle = 0$ could be cloned [2]. This proof actually should be called as "The cloning theorem of orthogonal quantum states". So for the single orthogonal quantum states, Yuen and Wootters agreed that they could be cloned. As for the quantum superposition states, Yuen thought that they were non-cloning [2].

It is pointed out in this paper that there are serious problems in the definition of quantum cloning operator. In quantum mechanics, any operator needs to have its concrete form. However, quantum cloning operator is only an abstract symbol, has not any concrete form. According to the definition, when a quantum clone operator is applied to any wave function $|\varphi_i\rangle$, it does not change the form of $|\varphi_i\rangle$. But if it is applied to a mixing initial state wave function $|S\rangle$, it can change $|S\rangle$ into $|\varphi_i\rangle$. Such an operator can not exist in mathematics unless $|\varphi_i\rangle = |S\rangle$. In this case, quantum clone operator becomes a unit operator, does not change any wave function.

In addition, quantum cloning operators are generally impossible in physics. According to Yuen's proof, orthogonal states satisfying $\langle \varphi_i | \varphi_j \rangle = 0$ can be cloned. However, there are some forbid rules in physics which make single orthogonal states non-cloning. For example, taking the ground state $\varphi_0 = R_{10}Y_{00}$ of a hydrogen atom as an initial state, and the orthogonal excited states are $\varphi_3 = R_{30}Y_{00}$ and $\varphi_4 = R_{32}Y_{21}$. The transitions from φ_0 to φ_3 or φ_4 are physically impossible. It means that φ_3 and φ_4 are non-clonable. However, according to the proof of Yuen, they can be cloned.

In fact, the transition from the ground state to the excited state need to absorb a photon, but the quantum cloning operator does not consider the existence of photons at all. Therefore, it can not correctly describe the practical physics process. Bedsides, the proof of Yuen has a logic mistake.

It is also proved that if $|\psi\rangle$ and $|\varphi\rangle$ are superposition states, assuming that $|\psi\rangle$ is known and $|\varphi\rangle$ is unknown, when the number $N > 2$ of superposition states, we can always find infinite number of $|\varphi\rangle$ to make them satisfying $\langle\psi|\varphi\rangle = 0.$ So according to the proof method of Yuen, $|\psi\rangle$ and $|\varphi\rangle$ are still clonable. But according to the proof of Wootters, the superposition states $|\psi\rangle$ and $|\varphi\rangle$ can not be cloned. The proofs of Yuen and Wootters are contradictory to each other.

For the case of $\langle\psi|\varphi\rangle = 1,$ the present theory considered that it was a trivial solution with $|\psi\rangle = |\varphi\rangle$ and has no value for discussion. It is indicated in this paper that when $|\psi\rangle \neq |\varphi\rangle$ and $N > 2,$ we can also find infinite numbers of $|\varphi\rangle$ to make them satisfying $\langle\psi|\varphi\rangle = 1,$ so that they are still clonable according to the proof method of Yuen, which still contradicts with the proof of Wootters.

In the practical experiments, the non-cloning theorem of quantum states is clearly inconsistent with the facts. A large number of experiments have proved that single quantum states of microscopic particles can be cloned. Lasers can clone not only a single photon, but also a large number of photons. Continuous spectrum lasers can clone not only same particular photons, but also a variety of photons by adjusting the parameters. In physics, the preparations of quantum states have long been a quite mature discipline.

In the actual operation process of quantum communication, the input and output are polarization states of photons. All of them are clonable. Even according to Wootters and Zurek, they are clones. However, the general impression given by the non-cloning theorem of quantum states is that all quantum states are non-cloning. This is not true.

The cloning processes of actual quantum states involve interactions and are very complex ones that can not be represented by such a simple quantum cloning operator. The non-cloning theorem of quantum states is an ambiguous, contradictory and completely wrong proposition, which not only has no meaning, but also seriously misleads the development of quantum theory and technology.

Therefore, the conclusion of this paper is that the non-cloning theorem of quantum states does not hold. Established on this theorem, the so-called unconditional confidentiality of quantum communication has not any physical foundation and can not be achieved.

2. The Proof of the Non-Cloning Theorem of Quantum States

The proof of Wootters and Zurek on the non-cloning theorem of quantum states was quite simple. The title of Wootters and Zurek's paper was "A single quantum can not be cloned". However, the paper actually discussed the superposition states and proved that quantum superposition states could not be cloned. For a single polarization quantum state, Wootters and Zurek thought that they were still clonable, but no concrete proof was provided [1].

Yuen used another method to prove that single quantum states satisfying the orthogonality condition can be cloned. The title of Yuen's paper was "Amplification of quantum states and noiseless photon amplifiers". For quantum superposition states, Yuen thought that they were clonable, but had not used the method he proposed to prove that the quantum superposition states can not be cloned.

We at first introduce the proof of Yuen and then introduce the proof of Wootters and Zure below.

2.1. The proof of Yuen

Yuen at first defined a so-called "the fixed initial state of the device including any relevant environment" $|S\rangle$, meanwhile assumed that the cloned particle was in an arbitrary single quantum state $|\varphi_i\rangle$. Then Yuen used a unitary operator $\hat{U}$ of quantum cloning. Its effects on a direct product wave function $|\varphi_i\rangle|S\rangle$ was defined as

$$\hat{U}|\varphi_i\rangle|S\rangle = |\varphi_i\rangle|\varphi_i\rangle. \tag{1}$$

In many literatures and textbooks on quantum cloning problems, single quantum states $|\varphi_i\rangle$ and quantum superposition states $|\varphi\rangle$ are often not distinguished, and Eq. (2) was written in a more general form

$$\hat{U}|\varphi\rangle|S\rangle = |\varphi\rangle|\varphi\rangle. \tag{2}$$

As for what is the concrete form of the fixed initial state of the device including any relevant environment $|S\rangle$, there were no any further explanation in the paper of Yuen. Compared to the process of photocopying, the operator $\hat{U}$ can be equivalent to a photocopier, $|\varphi_i\rangle$ can be equivalent to the picture to be copied and $|S\rangle$ can be equivalent to blank paper.

Using the same pure state $|S\rangle$, the clone operator is applied to another single quantum state $|\varphi_k\rangle$. According to Eq. (2), the result is

$$\hat{U}|\varphi_k\rangle|S\rangle = |\varphi_k\rangle|\varphi_k\rangle. \tag{3}$$

Taking the inner product of both sides of Eqs. (2) and (3), the result is

$$\langle S|\langle\varphi_k|\hat{U}^{+}\hat{U}|\varphi_i\rangle|S\rangle = \langle\varphi_k|\langle\varphi_k|\varphi_i\rangle|\varphi_i\rangle. \tag{4}$$

Due to $\hat{U}^{+}\hat{U} = 1$ and $\langle S|S\rangle = 1$, it can get from two sides of Eq. (4)

$$\langle\varphi_k|\varphi_i\rangle = \langle\varphi_k|\varphi_i\rangle^2. \tag{5}$$

Eq. (5) has two solutions

$$\langle \varphi_k \mid \varphi_i \rangle = 0 \quad \text{and} \quad \langle \varphi_k \mid \varphi_i \rangle = 1. \tag{6}$$

If these two conditions are satisfied, $|\varphi_i\rangle$ and $|\varphi_k\rangle$ can be cloned. Otherwise, they can not be cloned. The present theory only discusses the case of $\langle \varphi_k \mid \varphi_i \rangle = 0$, does not discuss the case of $\langle \varphi_k \mid \varphi_i \rangle = 1$.

Therefore, according to Yuen's proof, some orthogonal quantum states can be cloned, rather than any quantum state can not be cloned. To make this point clear, the abstract of Yuen's paper is cited as follows:

"It is shown that in principle a device exists which would duplicate a quantum system within a class of quantum states if and only if those quantum states are mutually orthogonal. The possible existence of a related noiseless photon amplifier is also established."

In this sense, we should call the result proved by Yuen as "the cloning theorem of single quantum orthogonal state".

2.2. The proof of Wootters and Zurek

The paper of Wootters and Zurek discussed quantum superposition states without using cloning operator. We use cloning operator below to make the discussions more simple and clear. The superposition states composed of two single quantum states is written as

$$|\varphi\rangle = a|\varphi_1\rangle + b|\varphi_2\rangle, \tag{7}$$

where $a^2 + b^2 = 1$. Applying the cloning operator on it, there are two results. The first is to act the operator on single states $\langle \varphi_1 |$ and $\langle \varphi_2 |$ and obtains

$$\begin{aligned}\hat{U}|\varphi\rangle|S\rangle &= (a\hat{U}|\varphi_1\rangle + b\hat{U}|\varphi_2\rangle)|S\rangle \\ &= a\hat{U}|\varphi_1\rangle|S\rangle + b\hat{U}|\varphi_2\rangle|S\rangle \\ &= a|\varphi_1\rangle|\varphi_1\rangle + b|\varphi_2\rangle|\varphi_2\rangle. \end{aligned} \tag{8}$$

The second is to act the operator on whole superposition state $|\varphi\rangle$. According to Eq. (2), the result is

$$\hat{U}|\varphi\rangle|S\rangle = |\varphi\rangle|\varphi\rangle = (a|\varphi_1\rangle + b|\varphi_2\rangle)(a|\varphi_1\rangle + b|\varphi_2\rangle)$$

$$= a^2|\varphi_1\rangle|\varphi_1\rangle + 2ab|\varphi_1\rangle|\varphi_2\rangle + b^2|\varphi_2\rangle|\varphi_2\rangle. \tag{9}$$

Because Eqs. (8) and (9) are contradictory, Wootters and Zurek concluded that the quantum superposition states can not be cloned. As for single polarization quantum states, Wootters and Zurek thought that they were still clonable.

The following passages are cited from the paper of Wootters and Zurek, making this point clearly.

"Thus no apparatus exists which will amplify an arbitrary polarization. The above argument does not rule out the possibility of a device which can amplify two special polarizations such as vertical and horizontal. Indeed, any measuring device which distinguishes between these two polarizations, a Nicol prism for example, would be used to trigger such an amplification.

The same argument can be applied to any other kind of quantum system. As in the case of photons, linearity does not forbid the amplification of any given state by a device designed especially for that state, but it does rule out the existence of a device capable of amplifying an arbitrary state" [1].

3. The Proof that the Non-Cloning Theorem of Quantum States does not hold

3.1. The quantum clone operator can not exist in mathematics

In Yuen's proof, the definition of the initial state $|S\rangle$ of the cloning device was unclear. Considering that the cloning device is also made up of microscopic particles, we can think of it as a quantum superposition system made up of a huge number of microscopic particles.

On the other hand, we know that quantum mechanics uses operators to represent mechanical quantities, so the definition of operators is very strict. For example, momentum operators, energy operators, angular momentum operators, etc., all of them have definite mathematical expression formulas. However, the quantum cloning operator is only a formal symbol, which has not been expressed in any specific mathematical form.

According to the definition of Eq. (2), the clone operator does not change arbitrary wave function $|\varphi_i\rangle$, but changes the initial state wave function $|S\rangle$ into $|\varphi_i\rangle$. We take a concrete example to show that this kind of operator is impossible to exist in mathematics.

Suppose that we want to clone the first excited state φ_1 of a hydrogen atom. Then, what is "the fixed initial state of the device including any relevant environment"? A most reasonable and simplified method is to treat the ground state wave function φ_0 as the initial wave function, i.e., let $S = \varphi_0$. It is hard to think of any other atomic state more suitable to be used as a initial wave function. The specific forms of these two wave functions are

$$\varphi_0 = \frac{1}{\sqrt{4\pi}a_0^{3/2}} e^{-r/a_0}, \qquad \varphi_1 = \frac{r}{2\sqrt{3\pi}a_0^{3/2}} e^{-r/2a_0} \cos\theta, \tag{10}$$

φ_0 and φ_1 are orthogonal. According to the definition of Eq. (1), we have

$$\hat{U}(\varphi_1\varphi_0) = (\hat{U}\varphi_1)\varphi_0 + \varphi_1(\hat{U}\varphi_0) = \varphi_1\hat{U}\varphi_0 = \varphi_1\varphi_1. \tag{11}$$

Eq. (11) means $\hat{U}\varphi_1 = 0$ and $\hat{U}\varphi_0 = \varphi_1$. However, in order to satisfy $\hat{U}\varphi_0 = \varphi_1$, it should have $\hat{U} \sim \varphi_1/\varphi_0$. Therefore, we have $\hat{U}\varphi_1 \sim \varphi_1^2/\varphi_0 \neq 0$

which is contradictory to $\hat{U}\varphi_1 = 0.$ That is to say, it is impossible for us to find an operator which can satisfy $\hat{U}\varphi_1 = 0$ and $\hat{U}\varphi_0 = \varphi_1$ simultaneously, so the definition of Eq. (1) can not hold. Since there is no clear mathematical expression form, using quantum cloning operator to describe the quantum cloning process is actually magic, having nothing to do with quantitative physical calculation.

For general situations, considering that $|\varphi\rangle|S\rangle$ is a direct product, we use matrix to represent cloning operator and quantum state

$$\hat{U} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi/S \end{pmatrix}, \qquad |\varphi\rangle|S\rangle = \begin{pmatrix} \varphi \\ S \end{pmatrix}. \tag{12}$$

Then write the cloning process of Eq. (2) as

$$\hat{U}|\varphi\rangle|S\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \varphi/S \end{pmatrix}\begin{pmatrix} \varphi \\ S \end{pmatrix} = \begin{pmatrix} \varphi \\ \varphi \end{pmatrix} = |\varphi\rangle|\varphi\rangle. \tag{13}$$

Because $\hat{U}$ is a unitary operator, we have

$$\hat{U}^{+}\hat{U} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi^{*}/S^{*} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \varphi/S \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi^{*}\varphi/S^{*}\,S \end{pmatrix} = I. \tag{14}$$

So we have $\varphi^{*}\varphi\big/S^{*}S = 1,$ then get $\varphi = S$ and

$$\hat{U} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi/\varphi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{15}$$

We can only obtain a unit operator, which can not describe the real cloning process.

In fact, the mathematical forms of quantum mechanical wave functions are quite complicated. To change an initial state wave function $|S\rangle$ into an arbitrary wave function $|\varphi_i\rangle$, the form of the operator would be very complicated. We can not find a mathematical transformation form, which can make an arbitrary wave function $|\varphi_i\rangle$ unchanged, and can change an initial wave function $|S\rangle$ into $|\varphi_i\rangle$.

3.2. The proof of Yuen does not hold in logic

The argument of Eq. (5) has a problem in logic. According to the definition of Eq. (2), the cloning operator changes $|S\rangle$ in to $|\varphi_i\rangle$, so the clonable condition should be $\langle S|\varphi_i\rangle = 0$. According to this definition, the cloning operator can also change $|S\rangle$ in to another function $|\psi_i\rangle$, and $|\psi_i\rangle$ and $|\varphi_i\rangle$ are independent of each other.

However, according to Eq. (6), the clonable condition becomes $\langle\psi_k|\varphi_i\rangle = 0$. The problem is what we discuss is the cloning between $|S\rangle$ and $|\varphi_i\rangle$ which has noting to do with $|\psi_k\rangle$. That $|\psi_k\rangle$ and $|\varphi_i\rangle$ are orthogonal does not mean that $|S\rangle$ and $|\varphi_i\rangle$ are also orthogonal. It does not make sense in logic that the clonable condition between $|S\rangle$ and $|\varphi_i\rangle$ is replaced by the orthogonal condition between $|\psi_k\rangle$ and $|\varphi_i\rangle$.

3.3. The examples that quantum state cloning operators do not hold in physics

We provide an example to show that Eq. (1) can not hold in physics in general. The transition process of hydrogen atom should obey a certain restraint rules, such as that angular quantum number l and magnetic quantum number m must satisfy $\Delta l = \pm 1$, $\Delta m = 0, \pm 1$. Thus a transition from the ground state $|\varphi_0\rangle = R_{10}Y_{00}$ to excited states $|\varphi_3\rangle = R_{30}Y_{00}$ and $|\varphi_4\rangle = R_{32}Y_{21}$ are impossible.

On the other hand, the states $|\varphi_0\rangle$, $|\varphi_3\rangle$ and $|\varphi_4\rangle$ are orthogonal each other, so we have $\langle\varphi_3|\varphi_4\rangle = 0$. If let $|S\rangle = |\varphi_0\rangle$ be the initial state, according to Eq. (5), $|\varphi_3\rangle$ and $|\varphi_4\rangle$ can be cloned. But we can not actually do that. We can not convert initial state $|\varphi_0\rangle$ into $|\varphi_3\rangle$ and $|\varphi_4\rangle$, so $|\varphi_3\rangle$

and $|\varphi_4\rangle$ are impossible to be cloned.

In fact, the cloning processes of quantum states are very complex because interactions are involved. For example, to transform a hydrogen atom from the ground state to the first excited state, an incident photon is required. The electron must absorb a photon before it transits to the first excited state. However, in the cloning formula (1), there is no place for the wave function of photon at all!

It is clear that we can not complete a cloning process by using a simple operator such as that defined in Eqs. (1) and (2), and can not judge whether a quantum state can be cloned by the simple formula of Eq. (6). The so-called quantum cloning operator is just an abstract concept and a formal symbol. It is impossible in mathematics, and there are a lot of problems in physics. Based on such operator and concept, the so-called non-cloning theorem of quantum states makes no sense.

3.4. The problems in the proof of Wootters and Zurek

Since the definition of quantum cloning operator is itself wrong, it is impossible to get the correct result by applying such operator to the superposition state wave function. Because both Eqs. (8) and (9) are wrong, and it is not surprise that there is a contradiction between them.

Some documents called the theory of Wootters and Zurek as the non-cloning theorem of unknown quantum states, but there is no clear explanation what an unknown quantum state is [5]. In fact, the claim that unknown quantum states can not be cloned is literally problematic. If a quantum state is unknown, without knowing the prototype or template, how can it be cloned?

For example, for the superposition state $|\varphi\rangle = a|\varphi_1\rangle + b|\varphi_2\rangle + c|\varphi_3\rangle$, if a, b and c are known, it is a known state. If a, b and c are arbitrary, the state is unknown. It is a prerequisite to know a, b and c before we clone this state. The claim of the non-cloning theorem of unknown quantum states is completely meaningless.

3.5. The proofs of Wootters and Yuen are contradictory

Wootters' proof is for the quantum superposition states. If the wave function is a single state, according to Wootters, it is still clonable. Yuen's proof is also for orthogonal single states. There is no contradiction between the proofs of Wootters and Yuen for single quantum states.

It is proved below that for quantum superposition states, when $|\psi\rangle \neq |\varphi\rangle$, we can still have $\langle\psi|\varphi\rangle = 0$ or $\langle\psi|\varphi\rangle = 1$. That is to say, according to the method of Yuen's proof, any quantum superposition state can still be cloned. Therefore, for quantum superposition states, the proofs of Wootters and Yuen are contradiction and incompatible.

In quantum mechanics, Hermitian operator $\hat{F}$ represents the mechanical quantities. Acting it on a stationary state wave function φ_n, we get

$$\hat{F}\varphi_n = \lambda_n \varphi_n. \tag{16}$$

Constant λ_n is called the eigenvalue. Hermitian operators have following two basic properties [3]:

1. The eigen functions of Hermitian operators with definite eigenvalues have orthogonality. If the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of $\varphi_1, \varphi_2, \ldots, \varphi_n$ are not equal to each other, then $\langle\varphi_m|\varphi_n\rangle = \delta_{mn}$.

2. The eigen function of Hermitian operator is complete. It can be strictly proved that any steady-state wave function can be expressed as a superposition of eigen wave functions of Hermitian operators with

$$|\varphi\rangle = \sum_{n=1}^{N} b_n |\varphi_n\rangle. \tag{17}$$

According to above two properties, we reconsider the proof of the non-cloning theorem of quantum superposition states. Write two pure state's superposition wave functions of a quantum ensemble with different expansion coefficients as

$$|\psi\rangle = \sum_{m=1}^{N} a_m |\varphi_m\rangle, \qquad |\varphi\rangle = \sum_{n=1}^{N} b_n |\varphi_n\rangle. \tag{18}$$

Considering the normalization formulas $\langle\psi|\psi\rangle = \langle\varphi|\varphi\rangle = 1$ of the wave functions, the expansion coefficient satisfies following formulas:

$$\sum_{m=1}^{N} a_m^2 = 1, \qquad \sum_{n=1}^{N} b_n^2 = 1. \tag{19}$$

Substituting Eq. (19) in $\langle\psi|\varphi\rangle = 0$ and considering $\langle\varphi_m|\varphi_n\rangle = \delta_{mn}$, we get

$$\sum_{n=1}^{N}\sum_{m=1}^{N} a_m^* b_n \langle\varphi_m|\varphi_n\rangle = \sum_{n=1}^{N} a_n^* b_n = 0. \tag{20}$$

For the case with $N = 2$, considering that the expansion parameters may be complex numbers, Eqs. (19) and (20) can be written as

$$|a_1|^2 + |a_2|^2 = 1, \quad |b_1|^2 + |b_2|^2 = 1, \quad a_1^* b_1 + a_2^* b_2 = 0. \tag{21}$$

Assume that $|\psi\rangle$ is known, so a_1 and a_2 are known. According to Eq. (21), there are two independent equations and two unknown complex numbers b_1 and b_2. So b_1 and b_2 can be uniquely determined. By solving the equations, we get $b_1 = a_2$ and $b_2 = a_1$. In the case of $N = 2$, we can always find another wave function $|\varphi\rangle$ to make them orthogonal. According the proof of Yuen, they are clonable.

For the case of $N = 3$, we have

$$|a_1|^2 + |a_2|^2 + |a_3|^2 = 1, \qquad |b_1|^2 + |b_2|^2 + |b_3|^2 = 1,$$

$$a_1^* b_1 + a_2^* b_2 + a_3^* b_3 = 0. \tag{22}$$

Assume that $|\psi\rangle$ is known, so a_1, a_2 and a_3 are known. There are two independent equations but three unknown complex numbers b_1, b_2 and b_3, so there are infinite forms to determine b_1, b_2 and b_3. For example, taking $a_1 = 1/2$ and $a_2 = 1/4$, from the first formula of Eq. (22), we get $a_3 = \sqrt{11}/4$. Choosing $b_1 = 1/3$ and calculating b_2 and b_3 according Eq. (22), we get following wave function:

$$|\psi\rangle = \frac{1}{2}|\varphi_1\rangle + \frac{1}{4}|\varphi_2\rangle + \frac{\sqrt{11}}{4}|\varphi_3\rangle, \tag{23}$$

$$|\varphi\rangle = \frac{1}{3}|\varphi_1\rangle + \frac{5\left(\sqrt{275} + i11\right)}{18\sqrt{275}}|\varphi_2\rangle + \frac{5\sqrt{11}\left(\sqrt{275} - i\right)}{18\sqrt{275}}|\varphi_3\rangle. \tag{24}$$

By choosing different b_1, we can get different expansion formulas for $|\varphi\rangle$ which are orthogonal with $|\psi\rangle$. Hence according to the proof of Yuen, the non-cloning theorem of quantum superposition states still hold. This result contradicts with the proof of Wootters and Zurek. Both are incompatible.

3.6. The discussion on the case of $\langle\psi|\varphi\rangle = 1$

It is now generally thought that $\langle\psi|\varphi\rangle = 1$ means $|\psi\rangle = |\varphi\rangle$, which is a trivial case and has no sense to talk about the cloning and non-cloning of quantum states. However, this is not the case. For the case $|\psi\rangle \neq |\varphi\rangle$ but $\langle\psi|\varphi\rangle = 1$, Eqs. (18) and (18) still hold, we only need to replace Eq. (20) with

$$\sum_{n=1}^{N} a_n^* b_n = 1. \tag{25}$$

When $N = 3$, we have

$$|a_1|^2 + |a_2|^2 + |a_3|^2 = 1, \qquad |b_1|^2 + |b_2|^2 + |b_3|^2 = 1,$$

$$a_1^* b_1 + a_2^* b_2 + a_3^* b_3 = 1. \tag{26}$$

Assume that $|\psi\rangle$ is known, so a_1, a_2 and a_3 are known. There are two independent equations but three unknown complex numbers, so there are infinite forms to determine b_1, b_2 and b_3.

Therefore, in the general case with $|\psi\rangle \neq |\varphi\rangle$, as long as the appropriate expansion coefficients are chosen, it is always possible to make $\langle\psi|\varphi\rangle = 1$. According to Yuen's proof, $|\varphi\rangle$ and $|\psi\rangle$ are still clonable. The contradiction still exists between the proofs of Wootters and Yuen.

4. Conclusions

The non-cloning theorem of quantum states is an ambiguous proposition full of contradictions and errors. It is proved in this paper that the definition of quantum clone operator is wrong. When a clone operator is applied to any wave function $|\varphi_i\rangle$, the wave function is unchanged. But when the operator is applied to an initial state wave function $|S\rangle$, it turns $|S\rangle$ into $|\varphi_i\rangle$. This kind of operator can not exist in mathematics, and is generally impossible in physics.

The proof of Wootters and Zurek was for quantum superposition states. The result should be called the non-cloning theorem of quantum superposition states. Due to the mistake of definition of quantum cloning operator, the proof of Wootters and Zurek was meanless. For orthogonal single quantum states, Wootters and Zurek thought that they were still clonable, but had not provided concrete proof.

The proof of Yuen was for single quantum states. The result is that the single quantum states satisfying the orthogonal condition $\langle \varphi_k | \varphi_i \rangle = 0$ were clonable. So the proof of Yuen should be called "the cloning theorem of single quantum orthogonal states". Due to the same mistake of the definition of cloning operator, the proof of Yuen is also incorrect. Besides, Yuen's proof had some problems in logic.

By considering the completeness of quantum mechanical wave functions, any wave function can be written as the superposition forms of eigenstate wave functions. It is proved in this paper, for a known superposition wave function with the eigenstate's number $N > 2$, we can always find infinite numbers of different superposition wave functions to make them satisfying the orthogonal conditions $\langle \psi | \varphi \rangle = 0$ and normalization condition $\langle \psi | \varphi \rangle = 1$. It means that according to the proof of Yuen, any quantum superposition state with $N > 2$ can be cloned. So the proofs of Yuen and Wootters are contradictory to quantum superposition states, though they are consistent to think that single quantum polarization states can be cloned.

A large number of experiments have shown that single quantum state of microscopic particle can be cloned. Laser is a typical example. In fact, the preparation of quantum states has long been a quite mature discipline in physics. The cloning processes of actual quantum states involve the interactions of multi-particles and are very complex [4] that can not be described by such a simple quantum cloning operators. The non-cloning theorem of quantum states is not only meaningless, but also seriously misleading the development of physical theory and technology.

In the actual operation of quantum communication, the input and output are the single polarization and orthogonal photons. All of them are clonable even according to the non-cloning theorem of quantum superposition states. Based on the so-called non-cloning theorem of quantum states, the so-called unconditional security of quantum communication has no any physical foundation and is impossible to realize.

References

[1] W. K. Wootters and W. H. Zurek, A single quantum can not be cloned, Nature 299 (1982), 802-803.

[2] H. P. Yuen, Amplification of quantum states and noiseless photon amplifiers, Phys. Lett. A 113 (1986), 405.

[3] Yin Hao and Han Yang, Quantum Communication Principle and Technology, Publishing House of Electronics Industry, 2013, p. 54.

[4] Zhou Shixun, Quantum Mechanics, Fudan University Press, 1961, p. 337.

[5] Zhang Yongde, Physics Principles of Quantum Information, Science Press, 2006, p. 187.