Novel cloning machine with supplementary information

2006 J. Phys. A: Math. Gen. 39 5135

(http://iopscience.iop.org/0305-4470/39/18/026)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 5135–5150 doi:10.1088/0305-4470/39/18/026

Novel cloning machine with supplementary information

Daowen Qiu

Department of Computer Science, Zhongshan University, Guangzhou 510275, People's Republic of China

E-mail: issqdw@mail.sysu.edu.cn

Received 7 November 2005, in final form 13 February 2006
Published 19 April 2006
Online at stacks.iop.org/JPhysA/39/5135

Abstract

Probabilistic cloning was first proposed by Duan and Guo. Then Pati established a *novel cloning machine* (NCM) for copying superposition of multiple clones simultaneously. In this paper, we deal with the *novel cloning machine with supplementary information* (NCMSI). For the case of cloning two states, we demonstrate that the optimal efficiency of the NCMSI in which the original party and the supplementary party can perform quantum communication equals that achieved by a two-step cloning protocol wherein classical communication is only allowed between the original and the supplementary parties. From this equivalence, it follows that NCMSI may increase the success probabilities for copying. Also, an upper bound on the unambiguous discrimination of two nonorthogonal pure product states is derived. Our investigation generalizes and completes the results in the literature.

PACS numbers: 03.67.−a, 03.65.Ud

1. Introduction

Over the past decade, quantum computation and quantum information has been given extensively attention due to the more power in essence than classical computation [1]. While the characteristics of quantum principles such as quantum superposition and entanglement essentially enhance the power of quantum information processing, the unitarity and linearity of quantum physics also lead to some impossibilities—the *no-cloning theorem* [2–4] and the *no-deleting principle* [5]. The linearity of quantum theory makes an unknown quantum state unable to be perfectly copied [2, 3] and deleted [5], and two nonorthogonal states are not allowed to be precisely cloned and deleted as a result of the unitarity [4, 6, 7], that is, for nonorthogonal pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, no physical operation in quantum mechanics can exactly achieve the transformation $|\psi_i\rangle \rightarrow |\psi_i\rangle|\psi_i\rangle (i = 1, 2)$. This has been

generalized to mixed states and entangled states [8, 9]. Remarkably, these restrictions provide a valuable resource in quantum cryptography [10], because they forbid an eavesdropper to gain information on the distributed secret key without producing errors.

Recently Jozsa [11] and Horodecki *et al* [12] further clarified the no-cloning theorem and the no-deleting principle from the viewpoint of conservation of quantum information, and in light of this point of view two copies of any quantum state contain more information than one copy; in contrast, two classical states have only the same information as any one of the two states. Specifically, Jozsa [11] verified that if supplementary information, say a mixed state ρ_i is supplemented, then there is a physical operation

$$|\psi_i\rangle \otimes \rho_i \to |\psi_i\rangle|\psi_i\rangle \tag{1}$$

if and only if there exists physical operation

$$\rho_i \to |\psi_i\rangle, \tag{2}$$

where by physical operation we mean a completely positive trace-preserving map, and $\{|\psi_i\rangle\}$ is any given finite set of pure states containing no orthogonal pairs of states. This result implies that the supplementary information must be provided as the copy $|\psi_i\rangle$ itself, since the second copy can always be generated from the supplementary information, independently of the original copy. Therefore, this result may show the 'permanence' of quantum information; that is, to get a copy of quantum state, the state must already exist somewhere. Notwithstanding, cloning quantum states with a limited degree of success has been proved always possibly. A natural issue is that if the supplementary information is added in a *novel cloning machine* (NCM) by Pati [13], then whether the optimal efficiency of the machine may be increased. This problem will be positively addressed in this paper.

Let us briefly recall the pioneers' works regarding quantum cloning, and the more detailed references may be referred to Fiurášek [14] therein. In general, there are two kinds of cloners. One is the *universal quantum-copying machine* (UQCM) firstly introduced by Bužek and Hillery [15], and this kind of machines is deterministic and does not need any information about the states to be cloned, so it is *state independent*. To be more precise, the UQCM obtained by Bužek and Hillery [15] is described by the following unitary transformation U:

$$|0\rangle_a|Q\rangle_x \to \sqrt{\tfrac{2}{3}}|00\rangle_{ab}|\uparrow\rangle + \sqrt{\tfrac{1}{3}}|+\rangle_{ab}|\downarrow\rangle, \tag{3}$$

$$|1\rangle_a|Q\rangle_x \to \sqrt{\tfrac{2}{3}}|11\rangle_{ab}|\downarrow\rangle + \sqrt{\tfrac{1}{3}}|+\rangle_{ab}|\uparrow\rangle, \tag{4}$$

where $|Q\rangle_x$ is the state of the copying device (auxiliary state), $|\uparrow\rangle$ and $|\downarrow\rangle$ are an orthonormal basis states and $|+\rangle_{ab} = \frac{1}{\sqrt{2}}(|10\rangle_{ab} + |01\rangle_{ab})$. The 'universal' means that for any pure state $|s\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$ to be cloned, the distances $D_a = \mathrm{Tr}\big[\rho_a^{(\mathrm{out})} - \rho_a^{(\mathrm{id})}\big]^2$ and $D_{ab} = \mathrm{Tr}\big[\rho_{ab}^{(\mathrm{out})} - \rho_{ab}^{(\mathrm{id})}\big]^2$ are independent of α, that is to say, the efficiency of cloning under these measures does not rely on the original state $|s\rangle_a$, where by denoting $|\Psi\rangle_{abx}^{(\mathrm{out})} = U(|s\rangle_a|Q\rangle_x)$, then the density operator $\rho_{abx}^{(\mathrm{out})} = |\Psi\rangle_{abx}^{(\mathrm{out})}{}_{abx}^{(\mathrm{out})}\langle\Psi|$, the real output in the system ab is $\rho_{ab}^{(\mathrm{out})} = \mathrm{Tr}_x\big[\rho_{abx}^{(\mathrm{out})}\big]$, the real output in the system a is $\rho_a^{(\mathrm{out})} = \mathrm{Tr}_b\big[\rho_{ab}^{(\mathrm{out})}\big]$; by contrast, the ideal output in the system ab is $\rho_{ab}^{(\mathrm{id})} = \rho_a^{(\mathrm{id})} \bigotimes \rho_b^{(\mathrm{id})}$, where $\rho_a^{(\mathrm{id})} = |s\rangle_a\,{}_a\langle s|$, $\rho_b^{(\mathrm{id})} = |s\rangle_b\,{}_b\langle s|$, in which $|s\rangle_b = \alpha|0\rangle_b + \beta|1\rangle_b$. (A direct calculation shows that $D_a = \frac{1}{18}$ for the above UQCM.) To date many authors have deeply dealt with this kind of cloning devices (for example, [16–26]). By the way, recently the universal quantum deleting machines have also been considered [27, 28].

The other kind of cloners is *state dependent*, since it needs some information from the states to be cloned. Furthermore, this kind of cloning machines may be divided into three fashions of cloning: first is probabilistic cloning machines proposed firstly by Duan and Guo [29, 30], and then by Chefles and Barnett [31] and Pati [13], and Han *et al* [32], that can clone linearly independent states with nonzero probabilities. Duan and Guo's machine can be stated as follows: for states secretly chosen from the set $S = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$, there is a unitary operator U such that

$$U(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{r_i}|\psi_i\rangle|\psi_i\rangle|P_0\rangle + \sum_{j=1}^{n} c_{ij}\left|\Phi_{AB}^{(j)}\right\rangle|P_j\rangle, \quad (i = 1, 2, \ldots, n), \tag{5}$$

if and only if states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ are linearly independent, where r_i is the probability of success for copying $|\psi_i\rangle$, $|\Sigma\rangle$ is a blank state, $|P_0\rangle, |P_1\rangle, \ldots, |P_n\rangle$ are probe states and orthonormal, and $\left|\Phi_{AB}^{(j)}\right\rangle$ are n normalized states of the composite system AB. Therefore, a general unitary evolution together with a post-selection by measurement results yields faithful copies of the input states with certain probabilities. Indeed, a more general unitary evolution of the system ABP can be decomposed as the form

$$U(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{r_i}|\psi_i\rangle|\psi_i\rangle|P^{(i)}\rangle + \sqrt{1 - r_i}\left|\Phi_{ABP}^{(i)}\right\rangle, \quad (i = 1, 2, \ldots, n), \tag{6}$$

that can be stated as: the states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ can be probabilistically cloned with efficiencies r_i if and only if the matrix $X^{(1)} - \sqrt{\Gamma}X_P^{(2)}\sqrt{\Gamma^+}$ is positive semidefinite, where matrices $X^{(1)} = [\langle\psi_i|\psi_j\rangle]$, $\sqrt{\Gamma} = \mathrm{diag}(r_1, r_2, \ldots, r_n)$, $X_P^{(2)} = [\langle\psi_i|\psi_j\rangle^2\langle P^{(i)}|P^{(j)}\rangle]$; $|P_0\rangle, |P^{(i)}\rangle$ are normalized states of the probe P (not generally orthogonal) and $\left|\Phi_{ABP}^{(i)}\right\rangle$ are n normalized states of the composite system ABP (not generally orthogonal, but it is required that $\left\langle P^{(i)}\middle|\Phi_{ABP}^{(j)}\right\rangle = 0$ for any $i, j = 1, 2, \ldots, n$). The success probabilities r_i and r_j satisfy that

$$\frac{r_i + r_j}{2} \leqslant \frac{1}{1 + |\langle\psi_i|\psi_j\rangle|}, \tag{7}$$

where $|\langle\psi_i|\psi_j\rangle| \neq 1$ is assumed.

Second is deterministic cloners first investigated by Bruß *et al* [33] and then by Chefles and Barnett [34]. Such a deterministic cloning machine is described by the unitary operator U

$$U(|\psi_i\rangle^{\otimes M}|\Sigma\rangle^{\otimes(N-M)}) = |\alpha_i\rangle, \quad (i = 1, 2, \ldots, n), \tag{8}$$

where $|\Sigma\rangle$ is a blank state and $|\alpha_i\rangle$ are the output states cloned. According to [33] the global fidelity F of this cloning device can be expressed as

$$F = \sum_{i=1}^{n} p_i|\langle\alpha_i|\psi_i\rangle^{\otimes N}|^2, \tag{9}$$

where p_i is the *a priori* probability of the state $|\psi_i\rangle^{\otimes M}$ chosen. From [33, 34] it follows that the optimal output state $|\alpha_i\rangle$ must lie in the subspace spanned by the exact clones $|\psi_1\rangle^{\otimes N}, |\psi_2\rangle^{\otimes N}, \ldots, |\psi_n\rangle^{\otimes N}$.

Third is hybrid cloner studied by Chefles and Barnett [32], that combines deterministic cloner with probabilistic one. The basic process of cloning is that firstly the initial states, say $\left|\psi_1^1\right\rangle$ and $\left|\psi_2^1\right\rangle$, are separated with certain probability P_S, i.e. a non-unitary transformation makes with certain probability P_S the states $\left|\psi_1^1\right\rangle$ and $\left|\psi_2^1\right\rangle$ become states $|\phi_1\rangle$ and $|\phi_2\rangle$ [31], such that

$$|\langle\phi_1|\phi_2\rangle| \leqslant \left|\left\langle\psi_1^1\middle|\psi_2^1\right\rangle\right|. \tag{10}$$

Such a transformation is implemented by some linear operators A_{Sk} and A_{Fk} satisfying

$$\sum_k \left(A_{Sk}^\dagger A_{Sk} + A_{Fk}^\dagger A_{Fk}\right) = \hat{\mathbf{1}}, \tag{11}$$

where $\hat{\mathbf{1}}$ is the identity operator, and

$$A_{Sk}\left|\psi_i^1\right\rangle = s_{ki}|\phi_i\rangle, \qquad A_{Fk}\left|\psi_i^1\right\rangle = f_{ki}|\phi_i\rangle,$$

for $i = 1, 2$, where

$$P_S = \sum_{i=1}^{2} \frac{1}{2} \sum_k |s_{ki}|^2 \leqslant \frac{1 - \left|\left\langle\psi_1^1\middle|\psi_2^1\right\rangle\right|}{1 - |\langle\phi_1|\phi_2\rangle|}. \tag{12}$$

Whereafter, by utilizing deterministic cloner for copying the states $|\phi_1\rangle$ and $|\phi_2\rangle$, the states $\left|\psi_1^2\right\rangle$ and $\left|\psi_2^2\right\rangle$ are determinately obtained. Therefore, such a cloning scheme obtain the appropriate states $\left|\psi_i^2\right\rangle$ for copying $\left|\psi_i^1\right\rangle$ $(i = 1, 2)$. (Notably, these quantum cloning machines stated above have been applied to many quantum cryptographic protocols [35–37].)

The probabilistic machine by Duan and Guo [29, 30] can be thought of as $|\psi\rangle \to |\psi\rangle^{\otimes 2}$ cloning. A question addressed by many authors is that given a quantum state, whether it is possible for a device to produce $|\psi\rangle \to |\psi\rangle^{\otimes 2}, |\psi\rangle \to |\psi\rangle^{\otimes 3}, \ldots, |\psi\rangle \to |\psi\rangle^{\otimes(m+1)}$, in a deterministic or probabilistic way. Motivated by this proposal and the idea of probabilistic cloning, Pati [13] established a NCM that could produce $|\psi\rangle \to |\psi\rangle^{\otimes(m+1)}(m = 1, 2, \ldots, k)$ clones simultaneously, which appear in a linear superposition of all possible multiple copies with respective probabilities. Therefore, Pati's NCM [13] generalizes Duan and Guo's cloning machine [29, 30]. For avoiding repetition, we will describe the NCM in sections 2 and 3 in detail, and differentiate between our results and the previous those related. In this paper, we deal with the *NCM with supplementary information* (NCMSI), and present an equivalent characterization of such a quantum cloning device in terms of a two-step cloning protocol in which the original and the supplementary parties are only allowed to communicate with classical channel.

The remainder of the paper is organized as follows. In section 2, we first introduce the existing results regarding probabilistic cloning with supplementary information, and then present our main contributions concerning NCMSI. Section 3 is the detailed demonstration of our major outcomes. In this section, we first provide a number of related unitary transformations describing cloning machines, and the corresponding inequalities characterizing the existence of these unitary transformations are then given; afterwards, we prove the main results expressed by theorems 1 and 2. Also we derive an upper bound for unambiguous discrimination of the set $\{|\psi_1\rangle|\phi_1\rangle, |\psi_2\rangle|\phi_2\rangle\}$ (remark 1). Finally, in section 4 we summarize our results obtained, mention some potential of applications, and address a number related issues for further consideration.

In addition, though some transformations describing cloning machines have been introduced in section 1, in the interest of readability, we would like to present partially them again with somewhat different forms in sections 2 and 3 to lead to our results.

2. Preliminaries and main results

In this section, we first give the existing results by Azuma *et al* [38], and then present our main results.

As pointed out above, Jozsa [11] and Horodecki *et al* [12] verified the no-cloning theorem and the no-deleting principle by utilizing supplementary information and conservation of quantum information, respectively. Then we may naturally address that if supplementary

information is added in the NCM, then whether the success probability for copying will be increased. Recently, Azuma *et al* [38] suggested probabilistic cloning with supplementary information by combining probabilistic cloning and supplementary information. Specifically, for any two nonorthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, and supplementary states $|\phi_1\rangle$ and $|\phi_2\rangle$, Azuma *et al* [38] showed the following implication: if there exists the unitary operator U

$$U(|\psi_i\rangle|\phi_i\rangle|P_0\rangle) = \sqrt{r_i}|\psi_i\rangle^{\otimes(m+1)}|P^{(i)}\rangle + \sqrt{1-r_i}\left|\Phi^{(i)}_{abp}\right\rangle, \quad (i=1,2), \tag{13}$$

then there are corresponding unitary operators U_B and U_A

$$U_B(|\phi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{r_i^B}|\psi_i\rangle^{\otimes m}\left|P_B^{(i)}\right\rangle + \sqrt{1-r_i^B}\left|\Phi^{(i)}_{abp_B}\right\rangle, \quad (i=1,2), \tag{14}$$

$$U_A(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{r_i^A}|\psi_i\rangle^{\otimes(m+1)}\left|P_A^{(i)}\right\rangle + \sqrt{1-r_i^B}\left|\Phi^{(i)}_{abp_A}\right\rangle, \quad (i=1,2), \tag{15}$$

such that $r_i^B + (1-r_i^B)r_i^A \geqslant r_i$ $(i=1,2)$, where r_i, r_i^B and r_i^A denote the success probabilities in the three machines, respectively, and $\left\langle P^{(i)}\middle|\Phi^{(j)}_{abp}\right\rangle = \left\langle P_B^{(i)}\middle|\Phi^{(j)}_{abp_B}\right\rangle = \left\langle P_A^{(i)}\middle|\Phi^{(j)}_{abp_A}\right\rangle = 0$ for any $i, j \in \{1,2\}$. The above implication means that when the state chosen from two nonorthogonal states, the best efficiency of producing $m+1$ copies is always achieved by a two-step cloning protocol in which the auxiliary party first tries to produce m copies from the supplementary state, and if it fails, then the original state is used to produce $m+1$ copies by means of the probabilistic cloning device proposed by Duan and Guo [29, 30]. For the sake of simplicity, we may represent the cloning devices described by equations (13), (14), (15) as

$$|\psi_i\rangle|\phi_i\rangle \xrightarrow{r_i} |\psi_i\rangle^{m+1}, \quad (i=1,2), \tag{16}$$

$$\Longrightarrow \quad |\phi_i\rangle \xrightarrow{r_i^B} |\psi_i\rangle^m \qquad \text{and} \qquad |\psi_i\rangle \xrightarrow{r_i^A} |\psi_i\rangle^{m+1}, \quad (i=1,2). \tag{17}$$

However, when the state chosen from n states, with $n > 2$ and without orthogonal pairs of states, the above implication described by equations (16), (17) may not hold again, i.e. the best efficiency is not always reached by such a two-step cloning protocol [38].

In this paper, we will show the following equivalent relation: for any two nonorthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, and supplementary states $|\phi_1\rangle$ and $|\phi_2\rangle$, there exists the unitary operator U:

$$U(|\psi_i\rangle|\phi_i\rangle|P_0\rangle) = \sum_{k=1}^{m}\sqrt{r_k^{(i)}}|\psi_i\rangle^{\otimes(k+1)}|0\rangle^{\otimes(m-k)}\left|P_k^{(i)}\right\rangle + \sum_{l=m+1}^{N}\sqrt{f_l^{(i)}}|\Psi_l\rangle_{AB}|P_l\rangle, \quad (i=1,2), \tag{18}$$

where $\left|P_1^{(i)}\right\rangle, \left|P_2^{(i)}\right\rangle, \ldots, \left|P_m^{(i)}\right\rangle, |P_{m+1}\rangle, |P_{m+2}\rangle, \ldots, |P_N\rangle$ are orthonormal for any $i \in \{1,2\}$, if and only if there are unitary operators U_B and U_A:

$$\begin{aligned} U_B(|\phi_i\rangle|\Sigma\rangle|P_0\rangle) = {} & \sum_{k=1}^{m}\sqrt{r_{k,B}^{(i)}}|\psi_i\rangle^{\otimes(k)}|0\rangle^{\otimes(m-k+1)}\left|P_{k,B}^{(i)}\right\rangle \\ & + \sum_{l=m+1}^{N}\sqrt{f_{l,B}^{(i)}}\left|\Phi_l^{(B)}\right\rangle_{AB}|P_{l,B}\rangle, \quad (i=1,2), \end{aligned} \tag{19}$$

$$\begin{aligned} U_A(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = {} & \sum_{k=1}^{m}\sqrt{r_{k,A}^{(i)}}|\psi_i\rangle^{\otimes(k+1)}|0\rangle^{\otimes(m-k)}\left|P_{k,A}^{(i)}\right\rangle \\ & + \sum_{l=m+1}^{N}\sqrt{f_{l,A}^{(i)}}\left|\Phi_l^{(A)}\right\rangle_{AB}|P_{l,A}\rangle, \quad (i=1,2), \end{aligned} \tag{20}$$

where $|P_{1,B}^{(i)}\rangle, |P_{2,B}^{(i)}\rangle, \ldots, |P_{m,B}^{(i)}\rangle, |P_{m+1,B}\rangle, |P_{m+2,B}\rangle, \ldots, |P_{N,B}\rangle$ are orthonormal, and, also, $|P_{1,A}^{(i)}\rangle, |P_{2,A}^{(i)}\rangle, \ldots, |P_{m,A}^{(i)}\rangle, |P_{m+1,A}\rangle, |P_{m+2,A}\rangle, \ldots, |P_{N,A}\rangle$ are orthonormal for any $i \in \{1, 2\}$; $r_k^{(i)}, r_{k,B}^{(i)}$ and $r_{k,A}^{(i)}$ represent the success probabilities for producing $|\psi_i\rangle^{\otimes(k+1)}, |\psi_i\rangle^{\otimes k}$ and $|\psi_i\rangle^{\otimes(k+1)}$, respectively, in these three cloning devices.

Furthermore, it is satisfied that if the unitary transformation described by equation (18) holds, then there exist unitary transformations described by equations (19), (20), such that

$$\sum_{k=1}^{m} r_{k,B}^{(i)} + \left(1 - \sum_{k=1}^{m} r_{k,B}^{(i)}\right) \sum_{k=1}^{m} r_{k,A}^{(i)} \geqslant \sum_{k=1}^{m} r_i^{(k)}, \quad (i = 1, 2), \tag{21}$$

conversely, if equations (19), (20) hold, then there is unitary transformation by equation (18) satisfying

$$\sum_{k=1}^{m} r_{k,B}^{(i)} + \left(1 - \sum_{k=1}^{m} r_{k,B}^{(i)}\right) \sum_{k=1}^{m} r_{k,A}^{(i)} \leqslant \sum_{k=1}^{m} r_i^{(k)}, \quad (i = 1, 2). \tag{22}$$

In the interest of simplicity, we may represent the above equations (18), (19), (20) as

$$|\psi_i\rangle|\phi_i\rangle \xrightarrow{\sum_{k=1}^{m} r_k^{(i)}} \sum_{k=1}^{m} |\psi_i\rangle^{\otimes(k+1)}, \quad (i = 1, 2), \tag{23}$$

$$\Longleftrightarrow$$

$$|\phi_i\rangle \xrightarrow{\sum_{k=1}^{m} r_{k,B}^{(i)}} \sum_{k=1}^{m} |\psi_i\rangle^{\otimes(k)} \tag{24}$$

and

$$|\psi_i\rangle \xrightarrow{\sum_{k=1}^{m} r_{k,A}^{(i)}} \sum_{k=1}^{m} |\psi_i\rangle^{\otimes(k+1)}, \quad (i = 1, 2). \tag{25}$$

Note that transformation (20) is exactly the NCM studied by Pati [13] and stated above. The above equivalence shows that the optimal efficiency of the NCMSI in which the original party and the supplementary party can perform quantum communication equals the optimal efficiency achieved by the two-step cloning protocol wherein classical communication is only allowed between the original and the supplementary parties. Therefore, in regard to the optimal success probabilities, if $\sum_{k=1}^{m} r_{k,B}^{(i)} > 0$, then $\sum_{k=1}^{m} r_k^{(i)} > \sum_{k=1}^{m} r_{k,A}^{(i)}, (i = 1, 2)$, which implies that the NCMSI may increase the success probability. As well, if we take only one $r_{k,B}^{(i)}$ and one $r_{k,A}^{(i)}$ nonzero for some k, then our right implication reduces to the implication described by transformations (16) and (17). Therefore, our result generalizes and completes the result proved by Azuma *et al* [38].

3. Proofs of main results

Firstly, for the sake of readability, we still quickly review the results by Azuma *et al* [38], and present some transformations, some of which were indeed described before.

Probabilistic cloning machine firstly posed by Duan and Guo [29, 30] describes that for any state set $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle\}$, there exists the unitary operator U such that

$$U(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{r_i}|\psi_i\rangle|\psi_i\rangle|P^{(i)}\rangle + \sqrt{1 - r_i}|\Phi_{ABP}^{(i)}\rangle, \quad (i = 1, 2, \ldots, k), \tag{26}$$

if and only if the matrix $X^{(1)} - \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma^{\dagger}}$ is positive semidefinite, where $X^{(1)} = [\langle\psi_i|\psi_j\rangle], X^{(2)} = [\langle\psi_i|\psi_j\rangle^2\langle P^{(i)}|P^{(j)}\rangle], \sqrt{\Gamma} = \sqrt{\Gamma^{\dagger}} = \mathrm{diag}(\sqrt{r_1}, \sqrt{r_2}, \ldots, \sqrt{r_k})$. The

efficiency of cloning is as $\sum_{i=1}^{k} p_i r_i$ if p_i are the probabilities for choosing states $|\psi_i\rangle$ $(i = 1, 2, \ldots, k)$.

Azuma *et al* [38] showed that for two nonorthogonal states, $|\psi_i\rangle (i = 1, 2)$, if there exists the unitary operator $U : |\psi_i\rangle|\phi_i\rangle \to \sqrt{r_i}|\psi_i\rangle^{\otimes(m+1)}$ (for simplicity, they left out the failure item and the states of the probe device), then there also exist the unitary operator $U_A : |\psi_i\rangle \to \sqrt{r_i^A}|\psi_i\rangle^{\otimes(m+1)}$ and the unitary operator $U_B : |\phi_i\rangle \to \sqrt{r_i^B}|\psi_i\rangle^{\otimes(m)}$ satisfying $r_i^B + (1 - r_i^B) r_i^A \geqslant r_i$ $(i = 1, 2)$. For k states with $k \geqslant 3$, they verified that there exist state sets $\{|\psi_i\rangle\}$ and $\{|\phi_i\rangle\}$, as well as the unitary operator U above, such that for any unitary operators U_A and U_B above, it holds that $r_i^A = 0$ $(i = 1, 2, \ldots, n)$ and $\sum_{i=1}^{k} \frac{1}{n} r_i > \sum_{i=1}^{k} \frac{1}{n} r_i^B$.

We enter on our discussion. Suppose Alice holds the original copy $|\psi_i\rangle$ and Bob possesses the supplementary information $|\phi_i\rangle$ $(i = 1, 2)$. If Alice and Bob are allowed to communicate with one-way quantum channel from Bob to Alice, then a single party holding both the original and the supplementary information $|\psi_i\rangle|\phi_i\rangle$ performs the following cloning process described by the unitary operator U:

$$U(|\psi_i\rangle|\phi_i\rangle|P_0\rangle) = \sum_{k=1}^{m} \sqrt{r_k^{(i)}}|\psi_i\rangle^{\otimes(k+1)}|0\rangle^{\otimes(m-k)}\left|P_k^{(i)}\right\rangle + \sum_{l=m+1}^{N} \sqrt{f_l^{(i)}}|\Psi_l\rangle_{AB}|P_l\rangle, \quad (i = 1, 2), \tag{27}$$

where $0 \leqslant r_k^{(i)} \leqslant 1$ for $k = 1, 2, \ldots, m$ and $\sum_{k=1}^{m} r_k^{(i)} < 1$ (in terms of [13], $\sum_{k=1}^{m} r_k^{(i)} = 1$ is impossible), $|P_0\rangle$, $\left|P_k^{(i)}\right\rangle$ and $|P_l\rangle$ are the states of the probing device, satisfying that $\left|P_1^{(i)}\right\rangle, \left|P_2^{(i)}\right\rangle, \ldots, \left|P_m^{(i)}\right\rangle, |P_{m+1}\rangle, |P_{m+2}\rangle, \ldots, |P_N\rangle$ are orthonormal for $i = 1, 2$. Moreover, $N > m$, $|0\rangle$ is the state of the ancillary system B, $r_k^{(i)}$ and $f_l^{(i)}$ are the success and the failure probabilities, respectively. If p_i are *a priori* probabilities for choosing $|\psi_i\rangle|\phi_i\rangle$ $(i = 1, 2)$, then the global success probability P_s for copying is

$$P_s = \sum_{i=1}^{2} p_i \sum_{k=1}^{m} r_k^{(i)}. \tag{28}$$

If Alice and Bob only can use classical channel for communication, they may respectively run the following machines described by unitary operators U_A and U_B, where U_A is exactly Pati's NCM [13]:

$$\begin{aligned} U_A(|\psi_i\rangle|\Sigma\rangle|P_0\rangle) = {} & \sum_{k=1}^{m} \sqrt{r_{k,A}^{(i)}}|\psi_i\rangle^{\otimes(k+1)}|0\rangle^{\otimes(m-k)}\left|P_{k,A}^{(i)}\right\rangle \\ & + \sum_{l=m+1}^{N} \sqrt{f_{l,A}^{(i)}}\left|\Phi_l^{(A)}\right\rangle_{AB}|P_{l,A}\rangle, \quad (i = 1, 2), \end{aligned} \tag{29}$$

such that $0 \leqslant r_{k,A}^{(i)} \leqslant 1$ for $k = 1, 2, \ldots, m$, where $|P_0\rangle$, $\left|P_{k,A}^{(i)}\right\rangle$ and $|P_{l,A}\rangle$ are the states of the probe device, satisfying that $\left|P_{1,A}^{(i)}\right\rangle, \left|P_{2,A}^{(i)}\right\rangle, \ldots, \left|P_{m,A}^{(i)}\right\rangle, |P_{m+1,A}\rangle, |P_{m+2,A}\rangle, \ldots, |P_{N,A}\rangle$ are orthonormal for $i = 1, 2$. If $p_i^{(A)}$ are *a priori* probabilities for choosing $|\psi_i\rangle$ $(i = 1, 2)$, then the global success probability $P_s^{(A)}$ for copying is

$$P_s^{(A)} = \sum_{i=1}^{2} p_i^{(A)} \sum_{k=1}^{m} r_{k,A}^{(i)}. \tag{30}$$

U_B is as follows:

$$U_B(|\phi_i\rangle|\Sigma\rangle|P_0\rangle) = \sum_{k=1}^{m} \sqrt{r_{k,B}^{(i)}}|\psi_i\rangle^{\otimes k}|0\rangle^{\otimes(m-k+1)}\left|P_{k,B}^{(i)}\right\rangle + \sum_{l=m+1}^{N} \sqrt{f_{l,B}^{(i)}}\left|\Phi_l^{(B)}\right\rangle_{AB}|P_{l,B}\rangle, \quad (i=1,2), \tag{31}$$

such that $0 \leqslant r_{k,B}^{(i)} \leqslant 1$ for $k = 1, 2, \ldots, m$, where $|P_0\rangle$, $\left|P_{k,B}^{(i)}\right\rangle$ and $|P_{l,B}\rangle$ are the states of the probe device, satisfying that $\left|P_{1,B}^{(i)}\right\rangle$, $\left|P_{2,B}^{(i)}\right\rangle$, $\ldots$, $\left|P_{m,B}^{(i)}\right\rangle$, $|P_{m+1,B}\rangle$, $|P_{m+2,B}\rangle$, $\ldots$, $|P_{N,B}\rangle$ are orthonormal for $i = 1, 2$. If $p_i^{(B)}$ are *a priori* probabilities for choosing $|\psi_i\rangle$ $(i = 1, 2)$, then the global success probability $P_s^{(B)}$ for copying is

$$P_s^{(B)} = \sum_{i=1}^{2} p_i^{(B)} \sum_{k=1}^{m} r_{k,B}^{(i)}. \tag{32}$$

If Alice and Bob only can use *one-way* classical channel for communication from *Bob to Alice*, then Bob first performs machine described by equation (31), and tells Alice the result of success or failure. If Bob succeeds, Alice only preserves her copy as is; otherwise, Alice runs the machine described by equation (29). Therefore, in this case, the success probability for producing quantum superposition of multiple clones $\sum_{k=1}^{m}|\psi_i\rangle^{\otimes(k+1)}$ when inputting $|\psi_i\rangle|\phi_i\rangle$ is

$$\sum_{l=1}^{m} r_{k,B}^{(i)} + \left(1 - \sum_{l=1}^{m} r_{l,B}^{(i)}\right) \sum_{l=1}^{m} r_{k,A}^{(i)}. \tag{33}$$

Similarly, if Alice and Bob can use only *one-way* classical channel for communication from *Alice to Bob*, then Alice first performs Pati's machine described by equation (29), and then tells Bob the result of success or failure. If Alice succeeds, Bob does nothing; otherwise, Bob runs machine by equation (31). Thus, it is seen that the success probability for producing quantum superposition of multiple clones $\sum_{k=1}^{m}|\psi_i\rangle^{\otimes(k+1)}$ with input $|\psi_i\rangle|\phi_i\rangle$ is

$$\sum_{k=1}^{m} r_{k,A}^{(i)} + \left(1 - \sum_{l=1}^{m} r_{l,A}^{(i)}\right) r_{k,B}^{(i)}. \tag{34}$$

If Alice and Bob can use *two-way* classical channel for communication, i.e. they can communicate each other, then they first independently carry out machines described by equations (29), (31) and, afterwards, inform the other of the outcome produced. Therefore, the success probability for producing quantum superposition of multiple clones $\sum_{k=1}^{m}|\psi_i\rangle^{\otimes(k+1)}$ with input $|\psi_i\rangle|\phi_i\rangle$ will be

$$1 - \left(1 - \sum_{k=1}^{m} r_{k,A}^{(i)}\right)\left(1 - \sum_{k=1}^{m} r_{k,B}^{(i)}\right) = \sum_{k=1}^{m} r_{k,A}^{(i)} + \sum_{k=1}^{m} r_{k,B}^{(i)} - \sum_{k=1}^{m} r_{k,A}^{(i)} \sum_{k=1}^{m} r_{k,B}^{(i)}. \tag{35}$$

Notably, whichever classical communication we choose, it is clearly seen that with input $|\psi_i\rangle|\phi_i\rangle$, the success probabilities for producing quantum superposition of multiple clones $\sum_{k=1}^{m+1}|\psi_i\rangle^{\otimes(k+1)}$ are equal.

In what follows, we denote $\alpha = \langle\psi_1|\psi_2\rangle$, $\beta = \langle\phi_1|\phi_2\rangle$, $p_k = \left\langle P_k^{(1)}\middle|P_k^{(2)}\right\rangle$, $p_{k,A} = \left\langle P_{k,A}^{(1)}\middle|P_{k,A}^{(2)}\right\rangle$, $p_{k,B} = \left\langle P_{k,B}^{(1)}\middle|P_{k,B}^{(2)}\right\rangle$. Now we note that equations (27), (29), (31) hold if and

only if the matrices

$$Z^{(1)} - \sum_{k=1}^{m} \sqrt{\Gamma_k} G^{(m+1)} \sqrt{\Gamma_k^{\dagger}},$$

$$X^{(1)} - \sum_{k=1}^{m} \sqrt{\Gamma_{k,A}} G_A^{(m+1)} \sqrt{\Gamma_{k,A}^{\dagger}},$$

$$Y^{(1)} - \sum_{k=1}^{m} \sqrt{\Gamma_{k,B}} G_B^{(m+1)} \sqrt{\Gamma_{k,B}^{\dagger}},$$

are positive semidefinite, respectively, where $Z^{(1)} = [\langle\psi_i|\psi_j\rangle\langle\phi_i|\phi_j\rangle]$, $X^{(1)} = [\langle\psi_i|\psi_j\rangle]$, and $Y^{(1)} = [\langle\phi_i|\phi_j\rangle]$; $G^{(m+1)} = \left[\langle\psi_i|\psi_j\rangle^{m+1}\left\langle P_k^{(i)}\middle| P_k^{(j)}\right\rangle\right]$, $G_A^{(m+1)} = \left[\langle\psi_i|\psi_j\rangle^{m+1}\left\langle P_{k,A}^{(i)}\middle| P_{k,A}^{(j)}\right\rangle\right]$ and $G_B^{(m)} = \left[\langle\psi_i|\psi_j\rangle^{m}\left\langle P_{k,B}^{(i)}\middle| P_{k,B}^{(j)}\right\rangle\right]$; $\sqrt{\Gamma_k} = \operatorname{diag}\left(r_k^{(1)}, r_k^{(2)}\right)$, $\sqrt{\Gamma_{k,A}} = \operatorname{diag}\left(r_{k,A}^{(1)}, r_{k,A}^{(2)}\right)$ and $\sqrt{\Gamma_{k,B}} = \operatorname{diag}\left(r_{k,B}^{(1)}, r_{k,B}^{(2)}\right)$. Furthermore, we note that the three matrices above are positive semidefinite if and only if their determinants are nonnegative, respectively, that is,

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_k^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_k^{(2)}\right)} - \left|\alpha\beta - \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}}\,\alpha^{k+1} p_k\right| \geqslant 0, \tag{36}$$

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,A}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,A}^{(2)}\right)} - \left|\alpha - \sum_{k=1}^{m} \sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}}\,\alpha^{k+1} p_{k,A}\right| \geqslant 0, \tag{37}$$

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,B}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,B}^{(2)}\right)} - \left|\beta - \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}\,\alpha^{k} p_{k,B}\right| \geqslant 0. \tag{38}$$

If $|\beta| > \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}}\,|\alpha|^k$, then, by taking appropriate amplitudes of p_k, inequality (36) is equivalent to

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_k^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_k^{(2)}\right)} - |\alpha\beta| + \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}}\,|\alpha|^{k+1} \geqslant 0, \tag{39}$$

analogously, if $1 > \sum_{k=1}^{m} \sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}}\,|\alpha|^k$ and $|\beta| > \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}\,|\alpha|^k$ hold, respectively, then correspondingly, inequalities (38), (39) are respectively equivalent to

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,A}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,A}^{(2)}\right)} - |\alpha| + \sum_{k=1}^{m} \sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}}\,|\alpha|^{k+1} \geqslant 0, \tag{40}$$

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,B}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,B}^{(2)}\right)} - |\beta| + \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}\,|\alpha|^{k} \geqslant 0. \tag{41}$$

With input $|\psi_i\rangle|\phi_i\rangle$, the efficiency of producing quantum superposition of multiple clones $\sum_{k=1}^{m} |\psi_i\rangle^{\otimes(k+1)}$ which Alice and Bob achieve via quantum channel can always be achieved by a two-step cloning protocol in which Alice and Bob are only allowed to execute *one-way* or *two-way* classical communication. This is described by the following theorem 1.

Theorem 1. *If there exists a unitary operator U such that equation (27) holds, then there are unitary operators U_A and U_B satisfying equations (29) and (31), respectively, such that*

$$\sum_{k=1}^{m} r_k^{(i)} \leqslant \sum_{k=1}^{m} r_{k,B}^{(i)} + \left(1 - \sum_{k=1}^{m} r_{k,B}^{(i)}\right) \sum_{k=1}^{m} r_{k,A}^{(i)}, \tag{42}$$

for $i = 1, 2$.

Proof. As above, denote $\alpha = \langle \psi_1 | \psi_2 \rangle$, $\beta = \langle \phi_1 | \phi_2 \rangle$. □

Case 1 $|\beta| \leqslant \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}} |\alpha|^k$. In this case, we only take any $r_{k,B}^{(i)}$ satisfying $r_{k,B}^{(i)} \geqslant r_k^{(i)}$ for $k = 1, 2, \ldots, m$ and $\sum_{k=1}^{m} r_{k,B}^{(i)} = 1$ $(i = 1, 2)$. Clearly, $|\beta| \leqslant \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}} |\alpha|^k$ also holds. Then it suffices to take appropriate $p_{k,B}$ such that $\beta - \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}} \alpha^k p_{k,B} = 0$. Thus, inequality (38) holds. By taking $r_{k,A}^{(i)} = 0$ $(1 \leqslant k \leqslant m, 1 \leqslant i \leqslant 2)$, then inequality (37) holds. So, the theorem is proved in this situation.

Case 2 $|\beta| > \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}} |\alpha|^k$. We set a function F from $[0, 1]^m \times [0, 1]^m$ to $[0, +\infty)$ as

$$F(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots, y_m) = \frac{\sqrt{\left(1 - \sum_{k=1}^{m} x_k\right)\left(1 - \sum_{k=1}^{m} y_k\right)}}{|\beta| - \sum_{k=1}^{m} \sqrt{x_k y_k} |\alpha|^k}. \tag{43}$$

Clearly, the function F is continuous on $[0, 1]^m \times [0, 1]^m$ and

$$F(0, 0, \ldots, 0; 0, 0, \ldots, 0) = \frac{1}{|\beta|} \geqslant 1, \tag{44}$$

as well as, by inequality (39),

$$F\left(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}; r_1^{(2)}, r_2^{(2)}, \ldots, r_m^{(2)}\right) \geqslant |\alpha|. \tag{45}$$

To prove the theorem, we somewhat change the function F to set up a new function H that only has m variables at most. The main idea to establish H is to reduce the number $2m$ of the variables in F to not more than m, and we present the way of constructing function H from function F in detail:

(i) For $1 \leqslant k \leqslant m$, if $0 \neq r_k^{(1)} \geqslant r_k^{(2)}$, then the pair of variables (x_k, y_k) in F will be replaced by $(x_k, c_k x_k)$, where $\frac{r_k^{(2)}}{r_k^{(1)}} = c_k \leqslant 1$; if $0 = r_k^{(1)} \geqslant r_k^{(2)}$, then the pair of variables (x_k, y_k) in F will be replaced by the pair $(0, 0)$ of constants.

(ii) For $1 \leqslant k \leqslant m$, if $r_k^{(1)} < r_k^{(2)}$, we replace the pair of variables (x_k, y_k) in F by $(c'_k y_k, y_k)$, where $c'_k = \frac{r_k^{(1)}}{r_k^{(2)}} \leqslant 1$.

By means of the above way to adjust and decrease those variables in the function F, we obtain a new function H whose number of variables is at most m, instead of $2m$, that is the form: for $z_k \in \{x_k, y_k\}$, $1 \leqslant k \leqslant m$,

$$H(z_1, z_2, \ldots, z_m) = F(u_1, u_2, \ldots, u_m; v_1, v_2, \ldots, v_m), \tag{46}$$

where

(i) If $0 \neq r_k^{(1)} \geqslant r_k^{(2)}$, then $z_k = x_k$, and, $u_k = x_k$, $v_k = c_k x_k$, where $c_k = \frac{r_k^{(2)}}{r_k^{(1)}} \leqslant 1$.

(ii) If $0 = r_k^{(1)} \geqslant r_k^{(2)}$, then $z_k = u_k = v_k = 0$.

(iii) If $\frac{r_k^{(1)}}{r_k^{(2)}} < 1$, then $z_k = y_k$ and $u_k = c'_k y_k$, $v_k = y_k$, where $c'_k = \frac{r_k^{(1)}}{r_k^{(2)}}$.

Without loss of generality, we suppose that always $r_k^{(1)} \geqslant r_k^{(2)}$, $k = 1, 2, \ldots, m$. Then we have

$$H(x_1, x_2, \ldots, x_m) = F(x_1, x_2, \ldots, x_m; c_1x_1, c_2x_2, \ldots, c_mx_m), \tag{47}$$

where when $r_k^{(1)} = 0$, $x_k \equiv 0$, $(k = 1, 2, \ldots, m)$.

By inequalities (44) and (45),

$$\begin{aligned} &H(0, 0, \ldots, 0) \\ &= F(0, 0, \ldots, 0; 0, 0, \ldots, 0) &(48)\\ &= \frac{1}{|\beta|} \geqslant 1, &(49)\end{aligned}$$

and

$$\begin{aligned} &H\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}\big) \\ &= F\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}; r_1^{(2)}, r_2^{(2)}, \ldots, r_m^{(2)}\big) &(50)\\ &\geqslant |\alpha|. &(51)\end{aligned}$$

Next we consider two scenarios to complete the proof: (I) If $H\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}\big) \geqslant 1$, then

$$\begin{aligned} &F\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}; r_1^{(2)}, r_2^{(2)}, \ldots, r_m^{(2)}\big) \\ &= H\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}\big) &(52)\\ &\geqslant 1, &(53)\end{aligned}$$

and, therefore, by equation (43) we have

$$\begin{aligned} &F\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}; r_1^{(2)}, r_2^{(2)}, \ldots, r_m^{(2)}\big) \\ &= \frac{\sqrt{\big(1 - \sum_{k=1}^m r_k^{(1)}\big)\big(1 - \sum_{k=1}^m r_k^{(2)}\big)}}{|\beta| - \sum_{k=1}^m \sqrt{r_k^{(1)} r_k^{(2)}}|\alpha|^k} \\ &\geqslant 1. &(54)\end{aligned}$$

Therefore, by taking $r_{k,B}^{(i)} = r_k^{(i)}$, $(k = 1, 2, \ldots, m; i = 1, 2)$, inequality (41) holds. As a result, there exist unitary operators U_A and U_B such that equations (29), (31) hold, in which we can choose $r_{k,A}^{(i)} = 0$ and $r_{k,B}^{(i)} = r_k^{(i)}$, $(k = 1, 2, \ldots, m; i = 1, 2)$. In this case, the theorem is proved.

(II) If $H\big(r_1^{(1)}, r_2^{(1)}, \ldots, r_m^{(1)}\big) < 1$, then, together with $H(0, 0, \ldots, 0) \geqslant 1$ (i.e., equation (49)), by *intermediate value theorem of continuous functions*, there exist $r_{k,B}^{(1)}$ such that

$$0 \leqslant r_{k,B}^{(1)} \leqslant r_k^{(1)}, \quad (k = 1, 2, \ldots, m), \tag{55}$$

and

$$H\big(r_{1,B}^{(1)}, r_{2,B}^{(1)}, \ldots, r_{m,B}^{(1)}\big) = 1. \tag{56}$$

Now, for $k = 1, 2, \ldots, m$, we take

$$r_{k,B}^{(2)} = \begin{cases} 0, & \text{if } r_k^{(1)} = 0, \\ \frac{r_k^{(2)}}{r_k^{(1)}} r_{k,B}^{(1)}, & \text{otherwise.} \end{cases} \tag{57}$$

Denoting

$$c_k = \begin{cases} 0, & \text{if } r_k^{(1)} = 0, \\ \frac{r_k^{(2)}}{r_k^{(1)}}, & \text{otherwise,} \end{cases}$$

then clearly we have

$$r_{k,B}^{(2)} = c_k r_{k,B}^{(1)}, \qquad r_k^{(2)} = c_k r_k^{(1)}, \tag{58}$$

for $k = 1, 2, \ldots, m$ and $i = 1, 2$; as well, by inequalities (55), (58), $\sum_{k=1}^{m} r_{k,B}^{(i)} \leqslant \sum_{k=1}^{m} r_k^{(i)}$ holds for $i = 1, 2$. Now we take

$$r_{k,A}^{(i)} = \frac{r_k^{(i)} - r_{k,B}^{(i)}}{1 - \sum_{k=1}^{m} r_{k,B}^{(i)}}, \quad (i = 1, 2), \tag{59}$$

then

$$\begin{aligned} \sqrt{\left(1 - r_{k,A}^{(1)}\right)\left(1 - r_{k,A}^{(2)}\right)} &= \sqrt{\frac{\left(1 - \sum_{k=1}^{m} r_k^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_k^{(2)}\right)}{\left(1 - \sum_{k=1}^{m} r_{k,B}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,B}^{(2)}\right)}} \\ &\geqslant \frac{|\beta| - \sum_{k=1}^{m} \sqrt{r_k^{(1)} r_k^{(2)}}|\alpha|^k}{|\beta| - \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}|\alpha|^k}|\alpha|, \end{aligned} \tag{60}$$

and

$$\sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}} = \frac{\left(r_k^{(1)} - r_{k,B}^{(1)}\right)\left(r_k^{(2)} - r_{k,B}^{(2)}\right)}{|\beta| - \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}|\alpha|^k}. \tag{61}$$

By inequality (60) and equation (61), we have

$$\begin{aligned} &\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,A}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,A}^{(2)}\right)} - |\alpha| + \sum_{k=1}^{m} \sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}}|\alpha|^{k+1} \\ &\quad \geqslant \frac{\sum_{k=1}^{m} \left(\sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}} - \sqrt{r_k^{(1)} r_k^{(2)}} + \sqrt{\left(r_k^{(1)} - r_{k,B}^{(1)}\right)\left(r_k^{(2)} - r_{k,B}^{(2)}\right)}\right)|\alpha|^{k+1}}{|\beta| - \sum_{k=1}^{m} \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}}. \end{aligned} \tag{62}$$

Due to equation (58), i.e. $r_{k,B}^{(2)} = c_k r_{k,B}^{(1)}$, $r_k^{(2)} = c_k r_k^{(1)}$, we have

$$\sqrt{\left(r_k^{(1)} - r_{k,B}^{(1)}\right)\left(r_k^{(2)} - r_{k,B}^{(2)}\right)} = \sqrt{r_k^{(1)} r_k^{(2)}} - \sqrt{r_{k,B}^{(1)} r_{k,B}^{(2)}}. \tag{63}$$

By combining equation (63) and inequality (62), we conclude that

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,A}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,A}^{(2)}\right)} - |\alpha| + \sum_{k=1}^{m} \sqrt{r_{k,A}^{(1)} r_{k,A}^{(2)}}|\alpha|^{k+1} \geqslant 0. \tag{64}$$

Due to the above conditions, inequalities (64) and (37) are equivalent, and, therefore, the proof has been completed.

Remark 1. Theorem 1 shows that the two-step cloning protocol in terms of classical one-way or two-way communication can achieve the optimal efficiency by the NCMSI. This theorem generalizes theorem 2 of [38]. Indeed, for $i = 1, 2$, given integer $m > 0$, if we take $r_k^{(i)} = 0$

for any $k \neq m$, then from the above proof we can also take $r_{k,B}^{(i)} = 0$ and $r_{k,A}^{(i)} = 0$ for any $k \neq m$. In this case, theorem 1 reduces to theorem 2 of [38] as stated in the beginning of this section. As well, due to $\lim_{m\to\infty}\langle\psi_i|\psi_j\rangle^m = 0$ for any $i \neq j$, when $m \to \infty$ the unitary transformation

$$U(|\psi_i\rangle|\phi_i\rangle|P_0\rangle) = \sqrt{r_m^{(i)}}|\psi_i\rangle^{\otimes(m+1)}|0\rangle^{\otimes(m-k)}\left|P_m^{(i)}\right\rangle + \sum_{l=m+1}^{N}\sqrt{f_l^{(i)}}|\Psi_l\rangle_{AB}|P_l\rangle \tag{65}$$

carries out the unambiguous discrimination of the set $\{|\psi_1\rangle|\phi_1\rangle, |\psi_2\rangle|\phi_2\rangle\}$. Indeed, firstly, if $|\phi_1\rangle$ and $|\phi_2\rangle$ are orthogonal, then in inequality (36) we take $r_m^{(1)} = r_m^{(2)} = 1$ and $p_m = 0$, which is in accord with the result that $\{|\psi_1\rangle|\phi_1\rangle, |\psi_2\rangle|\phi_2\rangle\}$ can be exactly discriminated thanks to the orthogonality. If $|\phi_1\rangle$ and $|\phi_2\rangle$ are nonorthogonal, then $|\beta| > 0$, and we can take m big enough such that $|\beta| > |\alpha|^m$. Therefore, by using inequality (36) we have that

$$\frac{r_m^{(1)} + r_m^{(2)}}{2} \leqslant \frac{1 - |\alpha\beta|}{1 - |\alpha|^m|p_m|}. \tag{66}$$

By taking $p_m = 0$, we obtain that

$$\frac{r_m^{(1)} + r_m^{(2)}}{2} \leqslant 1 - |\alpha\beta|. \tag{67}$$

This has been dealt with by Chen and Yang [39] for achieving the optimal unambiguous discrimination of any two nonorthogonal pure product multipartite states with any *a priori* probabilities via local operation and classical communication.

Next we may ask whether or not the two-step protocol is strictly stronger than the NCMSI. By the following theorem 2 we show that the optimal efficiency obtained by the above two-step cloning protocol can also be achieved by some NCMSI. Therefore, they indeed have the same optimal efficiency.

Theorem 2. *For any unitary operators U_A and U_B satisfying equations (29), (31), there is a unitary operator U satisfying equation (27), such that*

$$r_k^{(i)} = r_{k,B}^{(i)} + \left(1 - \sum_{l=1}^{m} r_{l,B}^{(i)}\right) r_{k,B}^{(i)}, \tag{68}$$

for $k = 1, 2, \ldots, m$ and $i = 1, 2$.

Proof. Leave α and β as they are. If $|\beta| \leqslant \sum_{k=1}^{m}\sqrt{r_k^{(1)}r_k^{(2)}}|\alpha|^k$, where $r_k^{(i)} = r_{k,B}^{(i)} + \left(1 - \sum_{l=1}^{m} r_{l,B}^{(i)}\right)r_{k,B}^{(i)}$, then inequality (36) is always satisfied by taking appropriate p_k, i.e. the states $\left|P_k^{(i)}\right\rangle$ of the probe device for $k = 1, 2, \ldots, m$ and $i = 1, 2$. Hence, we assume that $|\beta| > \sum_{k=1}^{m}\sqrt{r_k^{(1)}r_k^{(2)}}|\alpha|^k$, in the following. First we note that

$$\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,A}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,A}^{(2)}\right)}\sqrt{\left(1 - \sum_{k=1}^{m} r_{k,B}^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_{k,B}^{(2)}\right)}$$
$$= \sqrt{\left(1 - \sum_{k=1}^{m} r_k^{(1)}\right)\left(1 - \sum_{k=1}^{m} r_k^{(2)}\right)}. \tag{69}$$

Since $|\beta| > \sum_{k=1}^{m}\sqrt{r_k^{(1)}r_k^{(2)}}|\alpha|^k$, inequalities (40), (41) hold, and by these two inequalities, we have

$$\begin{aligned}
&\sqrt{\left(1-\sum_{k=1}^{m}r_{k,A}^{(1)}\right)\left(1-\sum_{k=1}^{m}r_{k,A}^{(2)}\right)}\sqrt{\left(1-\sum_{k=1}^{m}r_{k,B}^{(1)}\right)\left(1-\sum_{k=1}^{m}r_{k,B}^{(2)}\right)}\\
&\quad\geqslant\left(|\alpha|-\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^{k+1}\right)\left(|\beta|-\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^{k}\right)\\
&\quad=|\alpha\beta|-\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^{k+1}-|\beta|\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^{k+1}\\
&\qquad+\left(\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^{k+1}\right)\left(\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^{k}\right).
\end{aligned}\tag{70}$$

Therefore, to show inequality (39), it suffices to verify that

$$\left(|\alpha|-\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^{k+1}\right)\left(|\beta|-\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^{k}\right)\geqslant|\alpha\beta|-\sum_{k=1}^{m}\sqrt{r_{k}^{(1)}r_{k}^{(2)}}|\alpha|^{k+1}.\tag{71}$$

In terms of equation (70), inequality (71) is equivalent to

$$\begin{aligned}
\sum_{k=1}^{m}\sqrt{r_k^{(1)}r_k^{(2)}}|\alpha|^k&\geqslant\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^k+|\beta|\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^k\\
&\quad-\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^k\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^k.
\end{aligned}\tag{72}$$

By using inequality (41), it is enough to show that

$$\begin{aligned}
\sum_{k=1}^{m}\sqrt{r_k^{(1)}r_k^{(2)}}|\alpha|^k&\geqslant\sum_{k=1}^{m}\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}}|\alpha|^k\\
&\quad+\sqrt{\left(1-\sum_{k=1}^{m}r_{k,B}^{(1)}\right)\left(1-\sum_{k=1}^{m}r_{k,B}^{(2)}\right)}\sum_{k=1}^{m}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}|\alpha|^k.
\end{aligned}\tag{73}$$

We can easily check that for any $k=1,2,\ldots,m$,

$$\sqrt{r_k^{(1)}r_k^{(2)}}\geqslant\sqrt{\left(1-\sum_{l=1}^{m}r_{l,B}^{(1)}\right)\left(1-\sum_{l=1}^{m}r_{l,B}^{(2)}\right)}\sqrt{r_{k,A}^{(1)}r_{k,A}^{(2)}}+\sqrt{r_{k,B}^{(1)}r_{k,B}^{(2)}},\tag{74}$$

which follows from the inequality

$$\begin{aligned}
&r_{k,B}^{(1)}\left(1-\sum_{k=1}^{m}r_{k,B}^{(2)}\right)r_{k,A}^{(2)}+r_{k,B}^{(2)}\left(1-\sum_{k=1}^{m}r_{k,B}^{(1)}\right)r_{k,A}^{(1)}\\
&\quad\geqslant2\sqrt{\left(1-\sum_{k=1}^{m}r_{k,B}^{(1)}\right)\left(1-\sum_{k=1}^{m}r_{k,B}^{(2)}\right)r_{k,B}^{(1)}r_{k,A}^{(2)}r_{k,B}^{(2)}r_{k,A}^{(1)}}.
\end{aligned}\tag{75}$$

Therefore, we complete the proof. □

Remark 2. Since cloning only *one* multiple copies is a special case of cloning superposition of multiple clones, theorem 2 above shows that in theorem 2 of [38], probabilistic cloning

with supplementary information and the two-step cloning protocol are equivalent. Therefore this completes theorem 2 of [38].

Remark 3. If $|\psi_1\rangle$, $|\psi_2\rangle$ are linearly independent, and $|\phi_1\rangle$, $|\phi_2\rangle$ are linearly dependent, then by virtue of lemma 1 in [38], the success probability of Bob running the cloning device described by the unitary operator U_B is zero. Therefore, in this case, the NCMSI has the same cloning efficiency as the NCM. However, if the supplementary information $|\phi_1\rangle$, $|\phi_2\rangle$ are linearly independent, then the success probabilities in the cloning machine described by U_B are likely bigger than zero, and, thus, from theorem 2 it follows that the success probability of the NCMSI for cloning is bigger than the NCM [13].

4. Concluding remarks

We have dealt with the novel cloning machine with the help of supplementary information (NCMSI) for producing quantum superposition of multiple copies. When two holders, say Alice and Bob, possess respectively the original and the supplementary information, we have derived that the optimal efficiencies of cloning achieved via quantum communication and via classical one-way or two-way communication between the two parties in these devices are indeed equivalent. Therefore, the NCMSI for producing quantum superposition of multiple copies may have bigger success probability than the NCM [13]. However, by classical communication we do not know how to obtain all the copies together in a quantum computer, so, in practice we may use the scenario of quantum communication, i.e. the NCMSI.

As stated in section 1, probabilistic cloning may get precise copies with certain probability, so, improving the success ratio is of importance. We hope that our results would provide some useful ideas in preserving important quantum information, parallel storage of quantum information in a quantum computer and quantum cryptography.

When cloning n states with $n \geqslant 3$, Azuma *et al* [38] demonstrated that the optimal efficiency of copying achieved via quantum communication between the original and the supplementary parties sometimes cannot be accomplished by using only classical channel. Then an interesting problem is what is the sufficient and necessary condition for retaining the equivalence as we proved in this paper. A possible method is to combine matrix theory [40] and the present paper. Moreover, if the supplementary information is given as a mixed state or we have multiple supplementary information, then the probabilistic or novel cloning devices are still worth considering. We would like to explore these questions in future.

Acknowledgments

I am very grateful to the referees for their invaluable comments and suggestions that help to improve the presentation of this paper. This work is supported by the National Natural Science Foundation (nos 90303024, 60573006), the Higher School Doctoral Subject Foundation of Ministry of Education (no 20050558015), and the Natural Science Foundation of Guangdong Province (nos 020146, 031541) of China.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[3] Dieks D 1982 *Phys. Lett.* **92A** 271

[4] Yuen H P 1986 *Phys. Lett.* **113A** 405
[5] Pati A K and Braunstein S L 2000 *Nature* **404** 164
[6] D'Ariano G M and Yuen H P 1996 *Phys. Rev. Lett.* **76** 2832
[7] Qiu D W 2002 *Phys. Rev.* A **65** 052303
[8] Barnum H, Caves C M, Fuchs C A, Jozsa R and Schumacher B 1996 *Phys. Rev. Lett.* **76** 2818
[9] Koashi M and Imoto N 1998 *Phys. Rev. Lett.* **81** 4264
[10] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[11] Jozsa R 2004 *IBM J. Res. Dev.* **48** 79
[12] Horodecki M, Horodecki R, Sen A and Sen U 2004 *Preprint* quant-ph/0407038
[13] Pati A K 1999 *Phys. Rev. Lett.* **83** 2849
[14] Fiurášek J 2004 *Phys. Rev.* A **70** 032308
[15] Bužek V and Hillery M 1996 *Phys. Rev.* A **54** 1844
[16] Bužek V, Braunstein S L, Hillery M and Bruß D 1997 *Phys. Rev.* A **56** 3446
[17] Gisin N 1998 *Phys. Lett.* A **242** 1
[18] Gisin N and Massar S 1997 *Phys. Rev. Lett.* **79** 2153
[19] Bruß D, Ekert A and Macchiavello C 1998 *Phys. Rev. Lett.* **81** 2598
[20] Werner R F 1998 *Phys. Rev.* A **58** 1827
[21] Bužek V and Hillery M 1998 *Phys. Rev. Lett.* **81** 5003
[22] Keyl M and Werner R F 1999 *J. Math. Phys.* **40** 3283
[23] Bruß D and Macchiavello C 1999 *Phys. Lett.* A **253** 249
[24] Cerf N J 2000 *J. Mod. Opt.* **47** 187
[25] Braunstein S L, Bužek V and Hillery M 2001 *Phys. Rev.* A **63** 052313
[26] D'Ariano G M and Lo Presti P 2001 *Phys. Rev.* A **64** 042308
[27] Qiu D W 2002 *Phys. Lett.* A **301** 112
[28] Adhikari S and Choudhury B S 2004 *J. Phys. A: Math. Gen.* **37** 1
[29] Duan L-M and Guo G-C 1998 *Phys. Lett.* A **243** 261
[30] Duan L-M and Guo G-C 1998 *Phys. Rev. Lett.* **80** 4999
[31] Chefles A and Barnett S M 1998 *J. Phys. A: Math. Gen.* **31** 10097
[32] Han C, Song W, Yang M and Cao Z-L 2005 *Physica* A **354** 220
[33] Bruß D, DiVincenzo D P, Ekert A, Fuchs C A, Macchiavello C and Smolin J A 1998 *Rhys. Rev.* A **57** 2368
[34] Chefles A and Barnett S M 1999 *Phys. Rev.* A **60** 136
[35] Fuchs C A *et al* 1997 *Phys. Rev.* A **56** 1163
[36] Niu C-S and Griffiths R B 1999 *Phys. Rev.* A **60** 2764
[37] Acín A, Gisin N and Scarani V 2004 *Phys. Rev.* A **69** 012309
[38] Azuma K, Shimamura J, Koashi M and Imoto N 2005 *Phys. Rev.* A **72** 032335
[39] Chen Y-X and Yang D 2001 *Phys. Rev.* A **64** 064303
[40] Horn R A and Johnson C R 1986 *Matrix Analysis* vol 1 (Cambridge: Cambridge University Press)