Minimal input sets determining phase-covariant and universal quantum cloning

Li Jing,[1] Yi-Nan Wang,[1] Han-Duo Shi,[1] Liang-Zhu Mu,[1,*] and Heng Fan[2,†]

[1]*School of Physics, Peking University, Beijing 100871, China*

[2]*Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*

(Received 23 August 2012; revised manuscript received 28 October 2012; published 18 December 2012)

We study the minimal input sets which can determine completely the universal and the phase-covariant quantum cloning machines. We find that the universal quantum cloning machine, which can copy an arbitrary input qubit to two identical copies, however, can be determined completely by only four input states located at the four vertices of a tetrahedron in a Bloch sphere. The phase-covariant quantum cloning machine, which can create two copies from an arbitrary qubit located on the equator of the Bloch sphere, can be determined by three qubits located symmetrically on the equator of the Bloch sphere with equal relative phase. These results sharpen further the well-known results that Bennett-Brassard 1984 protocol (BB84) states and six states used in quantum cryptography can determine completely the phase-covariant and universal quantum cloning machines. This can simplify the testing procedure of whether the quantum clone machines are successful or not; namely, we only need to check that the minimal input sets can be cloned optimally, which can ensure that the quantum clone machines can work well for all input states.

DOI: 10.1103/PhysRevA.86.062315 PACS number(s): 03.67.Ac, 03.65.Aa, 03.67.Dd

I. INTRODUCTION

The no-cloning theorem, which states that an unknown quantum state cannot be cloned perfectly [1], is fundamental for quantum information science [2]. However, one can attempt to clone quantum states imperfectly, but have optimal fidelity or the largest probability. In the past years, different schemes of quantum cloning have been proposed, and various quantum cloning machines are designed for different tasks [2–5]. The quantum cloning machine was first proposed to clone an arbitrary qubit to two equal qubits [3]; neither of them are identical to the original qubit, but both are close. The quality of the quantum cloning does not depend on the specified form of the input qubit, so it is called universal quantum cloning machine (UQCM). This cloning machine has been proven to be optimal in the sense that the fidelity between the input qubit and one of the two output qubits is optimal [6]. The UQCM is extended to the higher-dimensional case [5], the case with M identical input states to N equally copies [7], and some other cases [8–16], including the recent proposed unified forms [17,18].

A qubit can be represented as $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$, where $\theta \in [0,\pi], \phi \in [0,2\pi\}$; it corresponds to a point in a Bloch sphere (see Fig. 1). For the UQCM, the input can be arbitrary qubits; the fidelity is optimal and does not depend on the input qubit. However, if we restrict the input state to the equatorial qubit which is located in the equator of the Bloch sphere $|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$, one can find that we can clone it better using a different quantum cloning machine than that of UQCM. This cloning machine is phase covariant in the sense that the quality of the cloning, similarly quantified by the fidelity, does not depend on the phase parameter ϕ of the input state. This is the phase-covariant quantum cloning machine (PQCM) [11,14,15].

One important application of quantum cloning machines is to analyze the security of some protocols of quantum key distribution (QKD). The reason is that a simple quantum attack on QKD for an eavesdropper is to keep one copy of the quantum state encoding secret key while sending another copy to the legitimate receiver. For the well-known BB84 protocol [19], we use two sets of orthogonal qubits, $\{|0\rangle,|1\rangle\},\{(|0\rangle + |1\rangle)/\sqrt{2},(|0\rangle - |1\rangle)/\sqrt{2}\}$, to encode binary secret key 0 or 1. It seems straightforward that BB84 states correspond to four equatorial qubits: $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\},\{(|0\rangle \pm i|1\rangle)/\sqrt{2}\}$. Thus, at least we should use PQCM instead of UQCM for eavesdropping. The point is that it is possible that we can do better. Surprisingly, it is shown that PQCM is already the optimal one in copying those four equatorial qubits [11]. A similar phenomenon happens in the case of six-state QKD [20], where the involved six states are $\{|0\rangle,|1\rangle\},\{(|0\rangle + |1\rangle)/\sqrt{2},(|0\rangle - |1\rangle)/\sqrt{2}\},\{(|0\rangle \pm i|1\rangle)/\sqrt{2}\}$. We cannot do better in cloning those six states than a UQCM, which can clone optimally an arbitrary qubit.

This seems not to be the end. With continuous progress of quantum cloning theoretically and experimentally [21–28], it is still not known whether BB84 states and six states are the minimal input sets necessarily for PQCM and UQCM. The motivation for wanting to know this is that we cannot distinguish perfectly BB84 (six) states; it is as difficult as measuring exactly an equatorial (arbitrary) qubit. However, it is unknown whether the sets of BB84 and six states are the minimal sets when the levels of difficulty for cloning them remain the same. In this paper, we find that they are not. The minimal input sets which can determine completely the PQCM and UQCM are found. The minimal input sets contain only three and four states, respectively.

The importance of this result is that, experimentally, if we find that the quantum cloning machines can copy the corresponding minimal input sets optimally, we know that they are able to clone optimally all equatorial qubits and arbitrary qubits, respectively. This simplifies dramatically the testing step. Another importance of this result is that from the Heisenberg uncertainty principle in quantum mechanics, and similarly from the no-cloning theorem, an unknown quantum

*muliangzhu@pku.edu.cn
†hfan@iphy.ac.cn

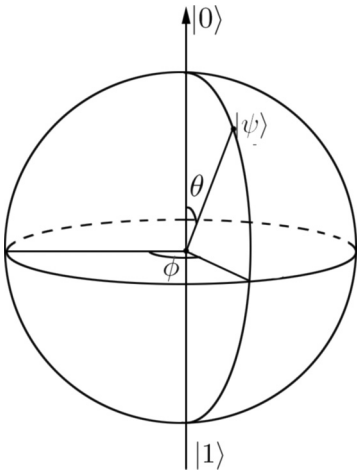

FIG. 1. A qubit in a Bloch sphere, $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$, which is characterized by amplitude parameter θ and phase parameter ϕ. An equatorial qubit is the qubit located on the equator of the Bloch sphere.

state with a single copy cannot be completely identified. So it can be expected that the minimal input sets for cloning machines would have the same uncertainty as the full input sets. Thus, our results may shed light on both the fundamental questions of the uncertainty principle and state and phase estimations [29,30] and potentially may lead to new applications in quantum cryptography, which relies on no cloning.

In this article, we first prove that a set of three qubits is the minimal set to determine PQCM. In Sec. II, we discuss the economic case. Cases with ancillas are discussed in Sec. III. In Sec. IV, we give more general results in $1 \to n$ PQCM to show the minimal set still works for this case. In Sec. V, the result that four qubits determine completely UQCM is proved. Section VI contains a brief conclusion and discussion.

II. OPTIMAL QUANTUM CLONING MACHINE FOR THREE STATES

We first study the case of PQCM. It is known that PQCM is needed to copy optimally four equatorial states equivalent to BB84 states. Here, we try to find whether it is possible to sharpen it further to three states. So now the question is whether we can find a set of three equatorial qubits; the cloning of these three states cannot be better than a PQCM. On the other hand, it is simple to find that two equatorial qubits can always be cloned better than a PQCM does, so the set of three states will be the minimal input set which can determine the PQCM. It is known that the optimal fidelity of PQCM is [11,14]

$$F_p = \frac{1}{2} + \frac{\sqrt{2}}{4}. \tag{1}$$

Thus, our goal is to find a set of three states; the fidelity of their cloning is upper bounded by F_p. It is apparent that this bound is achievable.

A quantum cloning machine generally needs ancillary states; if no ancillary states are available, it is the economic quantum cloning. In this paper, we start from the economical cloning for simplicity. We then show that ancillary states will not help to increase the fidelity.

We consider three equatorial qubits represented as

$$|\psi_i\rangle = (|0\rangle + e^{i\phi_i}|1\rangle)/\sqrt{2}, \tag{2}$$

where $i = 1,2,3$ represents three different phases. The economic quantum cloning transformation is a unitary transformation U on the input qubit and an initially blank state in which the copied qubit will be set. Its general form is

$$\begin{aligned} U|00\rangle &= a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \\ U|10\rangle &= e|00\rangle + f|01\rangle + g|10\rangle + h|11\rangle, \end{aligned} \tag{3}$$

where $a,\ldots,h$ are complex parameters to be determined, which should satisfy the constraints

$$\begin{aligned} a^*e + b^*f + c^*g + d^*h &= 0, \\ |a|^2 + |b|^2 + |c|^2 + |d|^2 &= 1, \\ |e|^2 + |f|^2 + |g|^2 + |h|^2 &= 1. \end{aligned} \tag{4}$$

The first equation shows the orthogonality of the unitary transformation, the next two equations are the normalization conditions. Now consider the input state $|\psi\rangle$, by performing the transformation U on $|\psi 0\rangle$, we obtain the density matrix for the whole system constituted by qubits A and B, $\rho_{AB} = U|\psi 0\rangle\langle\psi 0|U^\dagger$. Then we can trace out one of the particles to get one-particle reduced density matrices, ρ_A or ρ_B, which are two copies from the original input state $|\psi\rangle$. To quantify the quality of the cloning machine, we use the fidelities $F_A(\phi) = \langle\psi|\rho_A|\psi\rangle$ and $F_B(\phi) = \langle\psi|\rho_B|\psi\rangle$ to evaluate the distance between the input and two copies. As for our cloning machine (3), they are in the form

$$F_A(\phi) = \lambda_1\cos(2\phi + \psi_1) + \lambda_2\cos(\phi + \psi_2) + \lambda_3, \tag{5}$$

where λ_i are independent real numbers. The explicit expressions of these parameters are $\lambda_1 = \frac{1}{2}|ec^* + fd^*|$, $\psi_1 = \arg(ec^* + fd^*)$, $\lambda_2 = \frac{1}{2}|ac^* + eg^* + bd^* + fh^*|$, $\psi_2 = \arg(ac^* + eg^* + bd^* + fh^*)$, $\lambda_3 = \frac{1}{2}\mathrm{Re}(ag^* + bh^*) + \frac{1}{2}$. The expression of F_B is obtained just by interchanging $b \leftrightarrow c$ and $f \leftrightarrow g$.

Then we study three states with 120° intersection angles, that is, $\phi_1 = 0, \phi_2 = 2\pi/3, \phi_3 = 4\pi/3$ (see Fig. 2). We prove

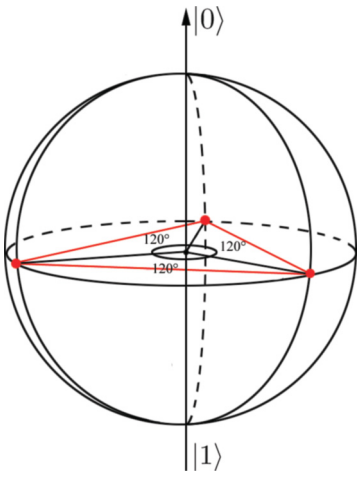

FIG. 2. (Color online) Three equatorial qubits with equal relative phases $\phi_1 = 0°, \phi_2 = 120°$, and $\phi_3 = 240°$, which determine a PQCM.

that the optimal fidelity is upper bounded by F_p, thus exactly equal to it.

In phase-covariant cloning we have the constraints

$$F_A(0) = F_A(2\pi/3) = F_A(4\pi/3),$$

which mean

$$\begin{aligned}&\lambda_1 \cos\left(\psi_1 - \frac{2\pi}{3}\right) + \lambda_2 \cos\left(\psi_2 + \frac{2\pi}{3}\right) + \lambda_3 \\ &= \lambda_1 \cos\left(\psi_1 + \frac{2\pi}{3}\right) + \lambda_2 \cos\left(\psi_2 - \frac{2\pi}{3}\right) + \lambda_3 \\ &= \lambda_1 \cos(\psi_1) + \lambda_2 \cos(\psi_2) + \lambda_3.\end{aligned}$$

They could be simplified further as

$$\lambda_1 \sin\psi_1 = \lambda_2 \sin\psi_2, \quad \lambda_1 \cos\psi_1 + \lambda_2 \cos\psi_2 = 0. \tag{6}$$

In the symmetric cloning case, we assume this cloning machine works in the symmetric subspace. So that $b = c$, $f = g$, and

$$F_A(\phi) = F_B(\phi) \equiv F. \tag{7}$$

This assumption is used in studying both PQCM and UQCM [6,11]. Therefore, by concluding the above constraints, fidelity for the three states can be written as

$$F = \lambda_3 = \tfrac{1}{2} + \tfrac{1}{2}\mathrm{Re}(af^* + bh^*). \tag{8}$$

The constraints may be simplified as follows:

$$\begin{aligned}ab^* + ef^* + bd^* + fh^* &= eb^* + fd^*, \\ \arg(ab^* + ef^* + bd^* + fh^*) + \arg(eb^* + fd^*) &= \pi, \\ |a|^2 + 2|b|^2 + |d|^2 &= 1, \\ |e|^2 + 2|f|^2 + |h|^2 &= 1, \\ ae^* + 2bf^* + dh^* &= 0.\end{aligned} \tag{9}$$

We are seeking the optimal cloning machine, so we try to find the tight bound of the fidelity as follows:

$$\begin{aligned}F &= \frac{1}{2} + \frac{1}{2}\mathrm{Re}(af^* + bh^*), \\ &= \frac{1}{2} + \frac{1}{2}\{|a||f|\cos[\arg(a) - \arg(f)] \\ &\quad + |b||h|\cos[\arg(b) - \arg(h)]\} \\ &\leqslant \frac{1}{2} + \frac{1}{2}(|a||f| + |b||h|) \\ &\leqslant \frac{1}{2} + \frac{1}{4\sqrt{2}}(|a|^2 + 2|f|^2 + |h|^2 + 2|b|^2) \\ &= \frac{1}{2} + \frac{1}{4\sqrt{2}}(1 - |d|^2 + 1 - |h|^2) \\ &\leqslant \frac{1}{2} + \frac{\sqrt{2}}{4}.\end{aligned}$$

By those algebraic inequalities, we obtain $F \leqslant 1/2 + \sqrt{2}/4$. The equality holds only when the following equations are satisfied: $\arg(a) = \arg(f)$, $\arg(b) = \arg(h)$, $|a| = \sqrt{2}|f|$, $|h| = \sqrt{2}|b|$, $|e| = 0$, $|d| = 0$, $2|b|^2 + 2|f|^2 = 1$, $|b||f| = 0$. This implies $\lambda_1 = \lambda_2 = 0$. Therefore,

$$F = \frac{1}{2} + \frac{\sqrt{2}}{4}. \tag{10}$$

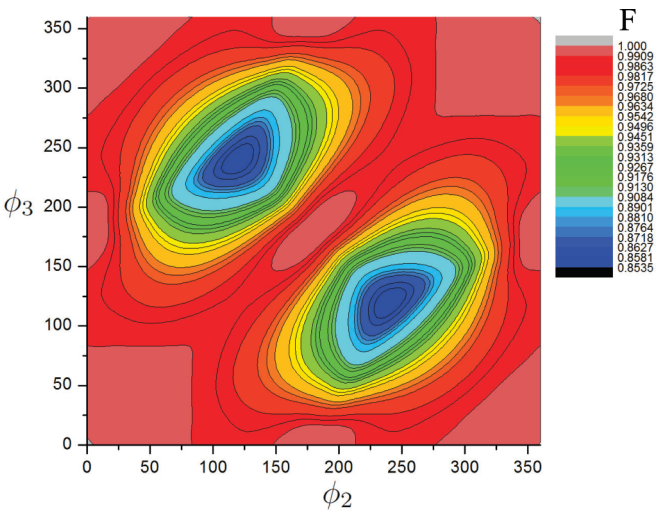

FIG. 3. (Color online) Contour plot for fidelity of different ϕ_2 and ϕ_3 (in degrees). Clearly, the minimum points are ($\phi_2 = 120^\circ$, $\phi_3 = 240^\circ$) and ($\phi_2 = 240^\circ$, $\phi_3 = 120^\circ$); those two cases are equivalent.

So we find that the optimal cloning fidelity of a set of three equatorial qubits with equal relative phases is exactly the optimal fidelity F_p of the phase-covariant case. All the possible parameters derived here are $|a| = 1, |f| = \frac{1}{\sqrt{2}}$, $\arg(a) = \arg(f)$, others $= 0$; or $|h| = 1, |b| = \frac{1}{\sqrt{2}}$, $\arg(b) = \arg(h)$, others $= 0$. This is exactly the PQCM presented in [11]. For completeness, we present it here explicitly:

$$U|00\rangle = |00\rangle, \quad U|10\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{11}$$

We remark that this is the optimal cloning machine for only three equatorial qubits.

The other three qubits on the equator with different intersection angles do not have this characteristic. Figure 3 shows some numerical results for different intersection angles. We set $\phi_1 = 0^\circ$, and the ranges of ϕ_2 and ϕ_3 are from 0° to 360°. We find that unless $\phi_2 = 120^\circ, \phi_3 = 240^\circ$, the fidelity is always larger than F_p. This is consistent with our analytic result. The numerical calculations are under the conditions of equal fidelity and symmetric cloning.

Since we can clone two arbitrary equatorial qubits better than a PQCM does, we then find the minimal input set determining completely a PQCM. Here we remark that this is for the economic case. Next we show that ancillary states do not help to increase the fidelity.

III. PHASE-COVARIANT QUANTUM CLONING MACHINE WITH ANCILLARY STATES

In order to solidify the equivalence between optimal three-state cloning machine and the PQCM, we should prove it for the more general case where the ancillary states are available since it is possible that we can clone them better. Here we show that the ancillary state does not help to increase the fidelity in cloning three equatorial qubits with equal relative phases. A noneconomic cloning machine is a unitary matrix acting on a

larger Hilbert space with the ancillas

$$\begin{aligned} U|00R\rangle &= a|00A\rangle + b|01B\rangle + c|10C\rangle + d|11D\rangle, \\ U|10R\rangle &= e|00E\rangle + f|01F\rangle + g|10G\rangle + h|11H\rangle. \end{aligned} \tag{12}$$

Similarly, we should have the orthogonal condition and normalization restrictions. With assumption of symmetric space for quantum cloning, we have $b = c$, $f = g$, $|B\rangle = |C\rangle$, $|F\rangle = |G\rangle$. We consider that the fidelity is invariant for different input qubits: $F(0) = F(2\pi/3) = F(4\pi/3)$. The resulted fidelity has a similar form:

$$\begin{aligned} F_A &= \lambda_1 \cos(2\phi + \psi_1) + \lambda_2 \cos(\phi + \psi_2) + \lambda_3 \\ &= \tfrac{1}{2} + \tfrac{1}{2}\mathrm{Re}(af^*\langle F|A\rangle + bh^*\langle H|B\rangle), \end{aligned} \tag{13}$$

where we use the notations $\lambda_1 = \frac{1}{2}|ec^*\langle C|E\rangle + fd^*\langle D|F\rangle|$, $\psi_1 = \arg(ec^*\langle C|E\rangle + fd^*\langle D|F\rangle)$, $\lambda_2 = \frac{1}{2}|ac^*\langle C|A\rangle + eg^*\langle G|E\rangle + bd^*\langle D|B\rangle + fh^*\langle H|F\rangle|$, $\psi_2 = \arg(ac^*\langle C|A\rangle + eg^*\langle G|E\rangle + bd^*\langle D|B\rangle + fh^*\langle H|F\rangle)$, $\lambda_3 = \frac{1}{2}\mathrm{Re}(ag^*\langle G|A\rangle + bh^*\langle H|B\rangle) + \frac{1}{2}$. Consider the restrictions mentioned above, similar to the economic cloning case; we find the the maximal fidelity is $F = \frac{1}{2} + \frac{1}{\sqrt{8}}$, which is obtained at $|a| = \sqrt{2}|f|, |h| = \sqrt{2}|b|, |d| = |e| = 0$, due to the presence of ancillary states. The restrictions can be rewritten as

$$\begin{aligned} 2|b|^2 + 2|f|^2 &= 1, \\ ab^*\langle B|A\rangle + fh^*\langle H|F\rangle &= 0, \\ \arg(ab^*\langle B|A\rangle + fh^*\langle H|F\rangle) &= \pi, \\ 2bf^*\langle F|B\rangle &= 0. \end{aligned} \tag{14}$$

If we set $|A\rangle = |B\rangle = |F\rangle = |H\rangle$, then the cloning machine reduces to the economic case. However, if we set $|A\rangle = |F\rangle = |0\rangle$, $|B\rangle = |H\rangle = |1\rangle$, then $\langle B|A\rangle = \langle H|F\rangle = 0$, so the only restriction is

$$2|b|^2 + 2|f|^2 = 1. \tag{15}$$

Under this condition, the noneconomic quantum cloning is always optimal. Explicitly, non-economic quantum cloning machine can take the following form by using Eq. (12):

$$\begin{aligned} U|00R\rangle &= a|00\rangle|0\rangle + b(|01\rangle + |10\rangle)|1\rangle, \\ U|10R\rangle &= f(|01\rangle + |10\rangle)|0\rangle + h|11\rangle|1\rangle. \end{aligned} \tag{16}$$

Note that $|a| = \sqrt{2}|f|, |h| = \sqrt{2}|b|$. This form is more general than the well-known PQCM, a special case, $a = h = 1/\sqrt{2}, b = f = 1/2$, is identical to the PQCM in [15].

IV. THE $1 \to n$ PQCM

Next, similar to the case of cloning one state to two copies, we show that the $1 \to n$ PQCM, which can clone one state to n copies, can be determined by these three equatorial qubits as well.

For the $1 \to n$ case, we still assume that our cloning machine is working in symmetric subspace, and it is economic. The transformations can be expressed as

$$|0\rangle \longrightarrow \sum_{i=0}^{n} a_i|i\rangle\rangle, \quad |1\rangle \longrightarrow \sum_{i=0}^{n} b_i|i\rangle\rangle, \tag{17}$$

where $|i\rangle\rangle$ is a complete symmetric state with i states in $|1\rangle$ among all n qubits. For example, if $n = 3$, $|1\rangle\rangle \equiv (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$. Analogously as in $1 \to 2$ case, parameters should satisfy the constraints, $\sum_{i=0}^{n} |a_i|^2 = 1$, $\sum_{i=0}^{n} |b_i|^2 = 1$, and $\sum_{i=0}^{n} a_i b_i^* = 0$.

The input is an equatorial qubit, $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$; we find the output state by cloning transformations, $\sum_{i=0}^{n}(a_i + e^{i\phi}b_i)|i\rangle\rangle$.

Without loss of generality, tracing off all states except the first one, we can obtain the one-qubit reduced-density matrix, ρ_1. By complicated but straightforward calculations, the fidelity can be found as

$$\begin{aligned} F = \frac{1}{2} + \frac{1}{2}\mathrm{Re}\Bigg[&\sum_{i=0}^{n-1}(a_i a_{i+1}^* e^{i\phi} + b_i b_{i+1}^* e^{i\phi} + a_i b_{i+1}^* \\ &+ a_{i+1}^* b_i e^{2i\phi})\Bigg]\frac{\sqrt{(n-i)(i+1)}}{n}. \end{aligned} \tag{18}$$

Here, we have used the following identities to simplify our expression, $C_{n-1}^{i} + C_{n-1}^{i+1} = C_n^i$, $\frac{C_{n-1}^{i}}{\sqrt{C_n^i C_n^{i+1}}} = \frac{\sqrt{(n-i)(i+1)}}{n}$. Therefore, as in the $1 \to 2$ case, we express the fidelity as

$$F = \lambda_1 \cos(2\phi + \psi_2) + \lambda_2 \cos(\phi + \psi_1) + \lambda_3, \tag{19}$$

where $\lambda_1 = \frac{1}{2}\sum_{i=0}^{n-1} |a_{i+1}^* b_i|$, $\lambda_2 = \frac{1}{2}\sum_{i=0}^{n-1} |a_i a_{i+1}^* + b_i b_{i+1}^*|$, and $\lambda_3 = \frac{1}{2}\sum_{i=0}^{n-1} |a_i b_{i+1}^*| + \frac{1}{2}$. Similarly, when three states are cloned equally well, we have $\lambda_1 = \lambda_2$, $\psi_1 + \psi_2 = \pi, (k \in \mathbb{Z})$, so that fidelity for them is $F = \lambda_3$

Next, we look for the maximal fidelity for them and find the corresponding values chosen by those parameters:

$$\begin{aligned} F &= \frac{1}{2} + \frac{1}{2}\mathrm{Re}\left[\sum_{i=0}^{n-1} a_i b_{i+1}^* \frac{\sqrt{(n-i)(i+1)}}{n}\right] \\ &\leqslant \frac{1}{2} + \frac{1}{4}\sum_{i=0}^{n-1}(|a_i|^2 + |b_{i+1}|^2)\frac{\sqrt{(n-i)(i+1)}}{n}. \end{aligned}$$

By considering the normalization conditions for a_i and b_i, we have the following results:

$$F \leqslant \frac{1}{2} + \frac{\sqrt{n(n+2)}}{4n}, \quad n \text{ is even}; \tag{20}$$

$$F \leqslant \frac{1}{2} + \frac{n+1}{4n}, \quad n \text{ is odd}. \tag{21}$$

For n is even, "=" is satisfied only when the following equations are satisfied, $\arg(a_i) = \arg(b_{i+1})$, $|a_{\frac{n}{2}}| = |b_{\frac{n}{2}+1}| = 1$; other parameters are zeros. For n is odd, "=" is satisfied only when the following equations are satisfied, $\arg(a_i) = \arg(b_{i+1})$, $|a_{\frac{n-1}{2}}| = |b_{\frac{n+1}{2}}| = 1$, other parameters are zeros. Note that now $\lambda_1 = \lambda_2 = 0$. Those results agree with the results for $1 \to n$ phase-covariant cloning machine in [14]. So we conclude that three equatorial qubits with equal relative phases can determine completely the optimal $1 \to n$ PQCM. Obviously, this general result is consistent with our previous $n = 2$ case. Our result is also true in the case $n \to \infty$. The implication of this result is that to identify one state from the minimal set which contains three states is as difficult as to find

the exact value of the phase in an equatorial qubit. This is quite surprising.

V. EQUIVALENCE BETWEEN FOUR-STATE CLONING AND A UQCM

A UQCM can copy optimally an arbitrary qubit. It is known that we cannot do better than a UQCM in cloning six states used in quantum cryptography [20]. The problem is that whether the number of states can be reduced from six to the minimal sets which contains only five or even four states. Considering that only three states can determine a PQCM, it might be possible that a UQCM, which has a lower fidelity than that of the PQCM, may be determined by four input states. This case must be the minimal input set. We show next that this is true.

Let us consider four states on the Bloch sphere with identical angular distance:

$$\begin{aligned} |\psi_0\rangle &= |0\rangle, \quad |\psi_1\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \\ |\psi_2\rangle &= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\frac{2\pi}{3}}|1\rangle, \\ |\psi_3\rangle &= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\frac{-2\pi}{3}}|1\rangle, \end{aligned} \tag{22}$$

where θ satisfies $\cos\frac{\theta}{2} = \frac{\sqrt{3}}{3}$. These four states form a tetrahedron (see Fig. 4). We need to show that the optimal fidelity in cloning those four states is the same as that of a UQCM.

The general cloning machine can be assumed as

$$\begin{aligned} U|00R\rangle &= a|00A\rangle + b|01B\rangle + c|10C\rangle + d|11D\rangle, \\ U|10R\rangle &= e|00E\rangle + f|01F\rangle + g|10G\rangle + h|11H\rangle. \end{aligned} \tag{23}$$

As usual, we assume the cloning machine works in symmetric subspace, that is, $b = c$, $f = g$, $|B\rangle = |C\rangle$, $|F\rangle = |G\rangle$. After some calculation similar to that in the phase-cloning case, and considering $\cos\frac{\theta}{2} = \frac{\sqrt{3}}{3}$, we obtain

$$\begin{aligned} F = {} & \tfrac{4}{9} - \tfrac{1}{9}(|a|^2 + |b|^2) + \tfrac{2}{9}(|f|^2 + |h|^2) \\ & + \tfrac{4}{9}|af^*\langle F|A\rangle + bh^*\langle H|B\rangle|. \end{aligned} \tag{24}$$

Then, we have

$$\begin{aligned} F + \frac{1}{3}F \leqslant {} & \frac{4}{9} - \frac{1}{9}(|a|^2 + |b|^2) + \frac{2}{9}(|f|^2 + |h|^2) \\ & + \frac{4}{9}(|a||f| + |b||h|) + \frac{1}{3}(|a|^2 + |b|^2) \\ \leqslant {} & \frac{4}{9} + \frac{2}{9}(|a|^2 + |b|^2 + |f|^2 + |h|^2) \\ & + \frac{4}{9}\left(\frac{|a|^2 + 4|f|^2}{4} + \frac{4|b|^2 + |h|^2}{4}\right) = \frac{10}{9}. \end{aligned} \tag{25}$$

So we have $F \leqslant \frac{5}{6}$. Then maximal fidelity equals to the fidelity of two-dimensional UQCM. The equality "=" is satisfied only when $|a| = |h| = \sqrt{\frac{2}{3}}$, $|b| = |f| = \sqrt{\frac{1}{6}}$, $|d| = |e| = 0$. Consider the constraints: We have $\langle B|F\rangle = 0$. Hence, we got the only possible form of $|A\rangle, |B\rangle, |F\rangle, |H\rangle$: $|A\rangle = |0\rangle, |B\rangle = |1\rangle, |F\rangle = |0\rangle, |H\rangle = |1\rangle$ with some possible phase factors.

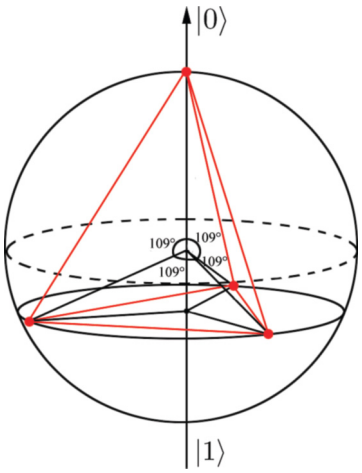

FIG. 4. (Color online) Four states located on vertices of an inscribed tetrahedron in the Bloch sphere can determine a UCQM.

[The requirement is $\mathrm{Im}(af^*\langle F|A\rangle) = \mathrm{Im}(bh^*\langle H|B\rangle) = 0$.] This is indeed the well-known UQCM.

By tricky but straightforward calculation, we can show that the fidelity F is upper bounded by $F = 5/6$, which is exactly the optimal fidelity of a UQCM. This optimal fidelity is achievable, so we conclude that the minimal input set of a UQCM contains only four states as presented in (22) which are located on vertices of a tetrahedron in Fig. 4.

VI. CONCLUSION

In summary, we have proved that the optimal cloner for three states symmetrically located on the equator of the Bloch sphere is equivalent to the PQCM. This minimal set is also valid in the $1 \to n$ cloning case. For the UQCM, the minimal input set contains only four states located on vertices of a tetrahedron. Those results sharpen further and are important supplements to the well-known results that the optimal quantum cloning machines for BB84 states and six states in QKDs are PQCM and UQCM, respectively.

Since no-cloning is a fundamental theorem in quantum mechanics and quantum information, it will be interesting to use those results for some applications, such as designing new QKD protocols or quantum gambling. We know that our results actually provide the sets which have the highest uncertainty levels. This may shed light on the study of uncertainty relationships, which constitute a cornerstone of quantum mechanics. By looking at the structures of those minimal input sets, we may observe that the states in these two sets have high symmetries. This fact provides an intuitive explanation that those states cannot be distinguished easily. One experimental application of those results is that, to test whether the cloning machines work, we only need to check that those minimal input sets can be cloned optimally. This will make the testing procedure of the cloning machines easier.

ACKNOWLEDGMENTS

This work is supported by NSFC (11175248), "973" Program (2010CB922904), and NFFTBS (J1030310).

[1] W. K. Wootters and W. H. ZureK, Nature (London) **299**, 802 (1982).
[2] M. A. Nielsen and I. C. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[3] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] R. F. Werner, Phy. Rev. A **58**, 1827 (1998).
[5] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[6] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[7] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[10] H. Fan, K. Matsumoto, and M. Wadati, Phys. Rev. A **64**, 064301 (2001).
[11] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
[12] D. Bruß and C. Macchiavello, J. Phys. A **34**, 6815 (2001).
[13] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[14] H. Fan, K. Matsumoto, X. B. Wang, and M. Wadati, Phys. Rev. A **65**, 012304 (2001).
[15] H. Fan, H. Imai, K. Matsumoto, and X. B. Wang, Phys. Rev. A **67**, 022317 (2003).
[16] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[17] Y. N. Wang, H. D. Shi, Z. X. Xiong, L. Jing, X. J. Ren, L. Z. Mu, and H. Fan, Phys. Rev. A **84**, 034302 (2011).
[18] Z. X. Xiong, H. D. Shi, Y. N. Wang, L. Jing, J. Lei, L. Z. Mu, and H. Fan, Phys. Rev. A **85**, 012334 (2012).
[19] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[20] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[21] E. Nagali *et al.*, Nat. Photon. **3**, 720 (2009).
[22] G. M. D'Ariano, S. Facchini, and P. Perinotti, Phys. Rev. Lett. **106**, 010501 (2011).
[23] P. Kurzynski, T. Paterek, R. Ramanathan, W. Laskowski, and D. Kaszlikowski, Phys. Rev. Lett. **106**, 180402 (2011).
[24] H. Chen, D. Lu, B. Chong, G. Qin, X. Zhou, X. Peng, and J. Du, Phys. Rev. Lett. **106**, 180404 (2011).
[25] J. Bae, W. Y. Hwang, and Y. D. Han, Phys. Rev. Lett. **107**, 170403 (2011).
[26] S. Raeisi, W. Tittel, and C. Simon, Phys. Rev. Lett. **108**, 120404 (2012).
[27] M. M. Wilde, P. Hayden, and S. Guha, Phys. Rev. Lett. **108**, 140501 (2012).
[28] G. Smith and J. A. Smolin, Phys. Rev. Lett. **108**, 230507 (2012).
[29] M. Paris and J. Řeháček (editors), *Quantum State Estimation*, Lecture Notes in Physics Vol. 649 (Springer, Berlin, Heidelberg, 2004).
[30] W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, and M. Mosca, Phys. Rev. Lett. **98**, 090501 (2007).