Approximate quantum state reconstruction without a quantum channel

Zichen Yang,[1] Ze-Yang Fan,[2] Liang-Zhu Mu,[1,*] and Heng Fan[3,4,5,†]
[1]*School of Physics, Peking University, Beijing 100871, China*
[2]*School of Astronautics, Harbin Institute of Technology, Harbin 150001, China*
[3]*Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*
[4]*CAS Center of Excellence in Topological Quantum Computation, University of Chinese Academy of Sciences, Beijing 100190, China*
[5]*Songshan Lake Material Laboratory, Dongguan 523000, China*

(Received 16 July 2018; published 11 December 2018)

We investigate the optimal quantum state reconstruction from the cloud to many spatially separated users by a measure-broadcast-prepare scheme without the availability of the quantum channel. The quantum state equally distributed from the cloud to an arbitrary number of users is generated at each port by an ensemble of known quantum states with assistance from classical information of measurement outcomes by broadcasting. The obtained quantum state for each user is optimal in the sense that the fidelity universally achieves the upper bound. We present the universal quantum state distribution by providing physical realizable measurement bases in the cloud as well as the reconstruction method for each user. The quantum state reconstruction scheme works for arbitrary many identical pure input states in the general dimensional system.

DOI: 10.1103/PhysRevA.98.062315

I. INTRODUCTION

In protocols of quantum information processing, entanglement and the quantum channel are in general assumed to be available. However, in a certain scenario we may need to distribute the quantum state to an arbitrary number of users, who are spatially separated, while neither entanglement nor the quantum channel is available. Each user may prepare his own quantum state according to classical information broadcasted from the "cloud" which can perform measurement on the quantum states that need to be distributed. This protocol can be named as classical quantum state reconstruction (CQSR). It is known that there is no-cloning theorem for quantum information which states that an arbitrary quantum state cannot be cloned perfectly [1–4]. For spatially separated users, approximate copies of a quantum state can also be obtained for a number of users by the combination of the quantum cloning machine and teleportation [5] which needs the resource of entangled states and classical communication [3,6,7], differing from CQSR. One may notice that CQSR can be achieved with the help of quantum estimation by a measure-and-prepare scheme [8–10], but with additional condition that the prepared states should not be entangled [11]. Additionally, CQSR should be physically realizable, which means that the number of measurements should be finite. We remark that the identically prepared quantum states can be compressed [12–14], resulting in that those states may be broadcasted economically. The quantum broadcast channels are also investigated in Ref. [15].

The general scheme of CQSR can be shown as in Fig. 1. The cloud will use universal measurement scheme for arbitrary input states, and broadcast the results of measurement. Each user can prepare the quantum state by using ensemble of known quantum states agreed in advance, which are thus in product forms, with probabilities depending on classical information. Next we generally equate the state estimation with CQSR, but bear in mind the difference that each user will prepare their state without the assistance of entanglement. The well-known estimation of quantum states shows that the *mean* fidelity for input states which are randomly and isotropically distributed can achieve the upper bound [8]. Here, we focus on the case of *universality* in the sense that each arbitrarily given input can be optimally distributed with the same fidelity.

II. STATEMENT OF THE PROBLEM

Here we consider the following case: the arbitrary M-copy quantum state ρ in the cloud is to be distributed to N users. Though it will be seen later that M does not necessarily equal to N, we will still start with the $M = N$ case, which meets the requirement of a standard quantum estimation problem. We first assume that the input is M independent and identically prepared arbitrary pure states in general d-dimension Hilbert space $\mathcal{H}$, $\rho = |\psi\rangle\langle\psi|^{\otimes M}$. It is known that this state is in the symmetric subspace $\mathcal{H}_+^M$ of $\mathcal{H}^{\otimes M}$ and has a dimension $d_M^+ = C_{M+d-1}^M$, where $C_{M+d-1}^M = \frac{(M+d-1)!}{M!(d-1)!}$. The basis of symmetric subspace $\mathcal{H}_+^M$ can be denoted by d-dimension vectors $\vec{m} = (m_0, m_1 \cdots m_{d-1})$ satisfying $\sum_{i=0}^{d-1} m_i = M$, where $|\vec{m}\rangle$ refers to the symmetric state in which there are m_i copies in the state $|i\rangle$, and $\{|i\rangle\}_{i=0}^{d-1}$ is the computational basis of Hilbert space $\mathcal{H}$.

The standard quantum estimation process can be considered as a quantum channel $\mathcal{E}(\rho)$ which maps $\mathcal{H}_+^M$ to itself,

$$\tilde{\rho} = \mathcal{E}(\rho) = \sum_{r=1}^{R} \mathrm{Tr}[\hat{O}_r\rho]|\Phi_r\rangle\langle\Phi_r|, \tag{1}$$

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

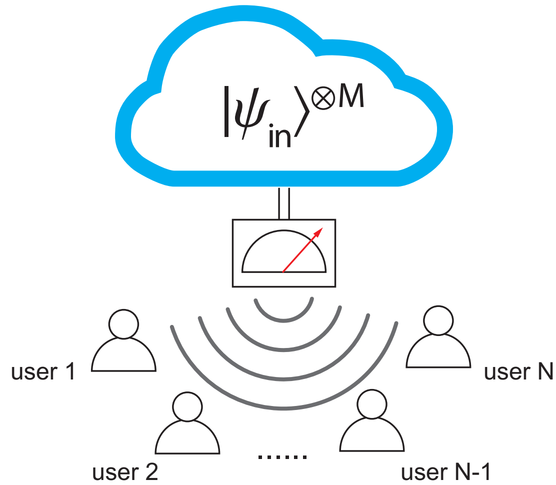

FIG. 1. Demonstration of quantum state reconstruction in the absence of the quantum channel. The input state $|\psi_{in}^{\otimes M}\rangle$ is stored and measured in the cloud. After the measurement, the corresponding measurement result is broadcast to the users. Having obtained the measurement results, each user can re-construct the initial state with the optimal fidelity.

where $\hat{O}_r$ is a set of positive operator valued measurements (POVMs), and $|\Phi_r\rangle\langle\Phi_r|$ is the corresponding guess in reconstructing the estimated state and also lies in $\mathcal{H}_+^M$. The case R being finite means physically realizable since measure and broadcast can be implemented finitely. The completeness requires

$$\sum_{r=1}^{R} \hat{O}_r = \mathbb{I}_+^M, \tag{2}$$

where $\mathbb{I}_+^M$ is the identity of symmetric subspace $\mathcal{H}_+^M$, to make sure the estimation is trace preserving.

For the CQSR protocol, we propose that the POVM is performed in the cloud. Additionally, we need to release the constraint of M users to arbitrary number N of users, meaning that there is no restriction on the number of audiences. Based on the measurement result, the users reconstruct the state by using a known ensemble of states $\{|\Phi_r\rangle\}$. We emphasize that state $|\Phi_r\rangle$ is not necessarily the product state for estimation, however, for spatially separated users in CQSR, $|\Phi_r\rangle$ should be in product form but without diminishing the fidelity.

For simplicity we use the notation $\rho^{(1)} = \mathrm{Tr}_{M-1}[\rho]$ and $\tilde{\rho}^{(1)} = \mathrm{Tr}_{M-1}[\rho]$, supposing $M = N$. Note again that here $\tilde{\rho}$ relies on the input $\rho = |\psi\rangle\langle\psi|^{\otimes M}$. The figure of merit for CQSR can be quantified by the fidelity between a single copy of the reconstructed state and a single input state $|\psi\rangle$, $f(\psi) = \mathrm{Tr}[\rho^{(1)}(\psi)\tilde{\rho}^{(1)}(\psi)]$.

The *mean* fidelity is defined as the following form,

$$\begin{aligned}\bar{f} &= \int d\psi \mathrm{Tr}[\rho^{(1)}(\psi)\tilde{\rho}^{(1)}(\psi)] \\ &= \int d\psi \sum_{r=1}^{R} \mathrm{Tr}[\hat{O}_r |\psi\rangle\langle\psi|^{\otimes M}] \\ &\quad \times \mathrm{Tr}[|\psi\rangle\langle\psi| \mathrm{Tr}_{M-1}(|\Phi_r\rangle\langle\Phi_r|)] \\ &= \int d\psi \sum_{r=1}^{R} \mathrm{Tr}[\hat{O}_r (U_\psi |0\rangle\langle 0| U_\psi^\dagger)^{\otimes M}] \\ &\quad \times \mathrm{Tr}[U_\psi |0\rangle\langle 0| U_\psi^\dagger \mathrm{Tr}_{M-1}(|\Phi_r\rangle\langle\Phi_r|)],\end{aligned} \tag{3}$$

where U_ψ is a unitary operator which transforms $|0\rangle$ to $|\psi\rangle$.

Our consideration is to have a *universal* fidelity for an arbitrary input state. It is clear that the optimal *universal* fidelity cannot exceed the optimal *mean* fidelity. We will find later that these two fidelities are actually the same, implying that the *universal* fidelity saturates the upper bound.

Here we define the M copy of ensemble of pure states $\{|\phi_r\rangle\}_{r=1}^R$ with corresponding probabilities $\{c_r\}_{r=1}^R$ as the completely symmetric set (CSS) if it satisfies the relation,

$$\sum_{r=1}^{R} c_r |\phi_r\rangle\langle\phi_r|^{\otimes M} = \frac{\mathbb{I}_+^M}{d_M^+}. \tag{4}$$

It means that the CSS corresponds to an identity in symmetric subspace.

We have the following lemma.

Lemma 1. If $\{|\phi_r\rangle\}_{r=1}^R$ and $\{c_r\}_{r=1}^R$ is an M-copy CSS, then it is also $M-1$, $M-2, \ldots, 1$-copy CSS.

The proof is straightforward. Taking trace over one Hilbert space denoted as Tr_1, on both sides of Eq. (4), we find that

$$\sum_{r=1}^{R} c_r |\phi_r\rangle\langle\phi_r|^{\otimes M-1} = \frac{1}{d_M^+}\mathrm{Tr}_1 \mathbb{I}_+^M = \frac{\mathbb{I}_+^{M-1}}{d_{M-1}^+}. \tag{5}$$

Here we need the relation,

$$|\vec{m}\rangle = \frac{1}{\sqrt{C_M^L}} \sum_{\vec{k}}^{C(\vec{k})=M-L} \prod_{j=0}^{d-1} \sqrt{\frac{m_j!}{(m_j-k_j)!k_j!}} |\vec{m}-\vec{k}\rangle|\vec{k}\rangle, \tag{6}$$

where we have used the notation $C(\vec{k}) = \sum_{i=0}^{d-1} k_i$. In the same way we have $\{|\phi_r\rangle\}_{r=1}^R$ and $\{c_r\}_{r=1}^R$ is also the $M-2$, $M-3, \ldots, 1$-copy CSS.

Obviously the basis of $\mathcal{H}$ can form a 1-copy CSS since $\sum_{i=0}^{d-1} \frac{1}{d}|i\rangle\langle i| = \mathbb{I}/d$. It is known that the states isomorphically distributed in $\mathcal{H}$ can form an arbitrary M-copy CSS, which is also related to the symmetric distribution of the information channel [11]. This infinite set takes the following form:

$$\int d\phi |\phi\rangle\langle\phi|^{\otimes M} = \frac{\mathbb{I}_+^M}{d_M^+}, \quad M = 1, 2, 3\ldots, \tag{7}$$

where the integral is taken over the Haar measurement and M is an arbitrary natural number. However, we need the number of measurements to be finite such that it is physically realizable.

III. OPTIMAL ESTIMATION PROTOCOL

Now, we present our main result.

Theorem. For state distribution to achieve optimal mean fidelity, the POVM must be the form of a M-copy CSS. Additionally, to make the fidelity identical for an arbitrary input, this CSS should also be the order of $(M+1)$ copy.

To study the optimal fidelity, it is useful to introduce the following operator,

$$\hat{\mathcal{F}} = \int d\psi |\psi\rangle\langle\psi|^{\otimes M} \mathrm{Tr}[|\psi\rangle\langle\psi||0\rangle\langle 0|]. \quad (8)$$

It is proved that the optimal *mean* fidelity $\bar{f}$ is upper bounded by the maximal eigenvalue λmax of $\hat{\mathcal{F}}$ multiplying the dimension d, i.e., $\bar{f} \leq d_M^+ \lambda_{\max}$. The corresponding POVM has to be $\hat{O}_r = \tilde{c}_r U_r^{\otimes M} |\psi_{\max}\rangle\langle\psi_{\max}| U_r^{\dagger\otimes M}$, $\tilde{c}_r$ is the probability, and $|\psi_{\max}\rangle\langle\psi_{\max}|$ is the eigenstate corresponding to the maximal eigenvalue [8].

By calculations, for dimension d, we can find that the operator $\hat{\mathcal{F}}$ defined in Eq. (8) is in the diagonal form,

$$\begin{aligned}
\hat{\mathcal{F}} &= \int d\psi |\psi\rangle\langle\psi|^{\otimes M} \mathrm{Tr}[|\psi\rangle\langle\psi|0\rangle\langle 0|] \\
&= \sum_{\vec{m},\vec{n}}^{M} |\vec{m}\rangle\langle\vec{n}| \int d\psi \langle\vec{m}|(|\psi\rangle\langle\psi|)^{\otimes M}|\vec{n}\rangle \mathrm{Tr}[|\psi\rangle\langle\psi|0\rangle\langle 0|] \\
&= \sum_{\vec{m},\vec{n}} |\vec{m}\rangle\langle\vec{n}| \mathrm{Tr}[|\vec{n}\rangle\langle\vec{m}| \otimes |0\rangle\langle 0| \int d\psi |\psi\rangle\langle\psi|^{\otimes M+1}] \\
&= \sum_{\vec{m},\vec{n}} \frac{1}{d_{M+1}^+} |\vec{m}\rangle\langle\vec{n}| \sum_{\vec{r}}^{C(\vec{r})=M+1} \mathrm{Tr}[(|\vec{n}\rangle\langle\vec{m}| \otimes |0\rangle\langle 0|)|\vec{r}\rangle\langle\vec{r}|] \\
&= \sum_{\vec{m}}^{M} \frac{1}{d_{M+1}^+} |\vec{m}\rangle\langle\vec{m}| \frac{m_0+1}{M+1},
\end{aligned} \quad (9)$$

where summation is taken over all the basis in $\mathcal{H}_+^M$. For this diagonal matrix $\hat{\mathcal{F}}$, the largest eigenvalue corresponds condition $m_0 = M$, $\lambda_{\max} = d_{M+1}^+$, the corresponding eigenstate is $|0\rangle^{\otimes M}$. The POVM thus takes the form of M-identical copies, $\hat{O}_r = \tilde{c}_r (U_r|0\rangle\langle 0|U_r^\dagger)^{\otimes M} = c_r d_M^+ |\phi_r\rangle\langle\phi_r|^{\otimes M}$, where $|\phi_r\rangle = U_r|0\rangle$. On the other hand, the completeness relation (2) requires $\{|\phi_r\rangle\}_{r=1}^R$ and $\{c_r\}_{r=1}^R$ to be a M-copy CCS. The optimal fidelity of state estimation is $\bar{f}_{\mathrm{opt}} = \frac{M+1}{M+d}$. This fidelity is the same as the optimal fidelity of a $M \to \infty$ quantum cloning machine. The relationship between the fidelity of state estimation and that of the cloning machine is already known; see [3] and the references therein. Here we specifically point out that the POVM takes the form as $\hat{O}_r = c_r (U_r|0\rangle\langle 0|U_r^\dagger)^{\otimes M}$, which simplifies the original result $\hat{O}_r = c_r U_r^{\otimes M} |\psi_{\max}\rangle\langle\psi_{\max}| U_r^{\dagger\otimes M}$, where $|\psi_{\max}\rangle$ is generally unknown and may not necessarily be a product state [8].

However, even if the state estimation achieves optimal *mean* fidelity, it is still far from enough, because for some input states, the fidelity could be undesirably small, which is an unwanted case. Here we further demand that CQSR yields the *universal* fidelity for any input state. Obviously the *universal* fidelity is upper bounded by the *mean* fidelity, namely $\frac{M+1}{M+d}$. We now prove that this upper bound is achievable for a $(M+1)$-copy CSS.

We can consider the input to be M-copy pure states $|\psi\rangle^{\otimes M}$, which is in the symmetric subspace. Here, we present a more general form for an arbitrary matrix in the symmetric subspace for the input,

$$\rho = \sum_{\vec{m},\vec{n}} A_{\vec{m},\vec{n}} |\vec{m}\rangle\langle\vec{n}|. \quad (10)$$

Simply, we know that $|\psi\rangle\langle\psi|^{\otimes M} \in \rho$, meaning that the form of identical pure states is a special case. After tracing out $M-1$ copies, the single-copy state is

$$\rho^{(1)} = \frac{1}{M} \sum_{\alpha,\beta=1}^{d} \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sqrt{m_\alpha n_\beta} |\alpha\rangle\langle\beta| \delta_{\vec{m}-\vec{\alpha},\vec{n}-\vec{\beta}}, \quad (11)$$

where $\vec{\alpha}$ denotes the vector with its αth entry to be 1 and other entries to be 0. If the POVM is $(M+1)$-copy CSS, $d_{M+1}^+ \sum_{r=1}^R c_r |\phi_r\rangle\langle\phi_r|^{\otimes M+1} = \mathbb{I}_+^{M+1}$, after some calculations, we can find that the single copy of the output state takes the form,

$$\begin{aligned}
\tilde{\rho}^{(1)} &= \mathrm{Tr}_{M-1}[\mathcal{E}(\rho)] \\
&= \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{r=1}^{R} d_M^+ c_r \mathrm{Tr}[|\phi_r\rangle\langle\phi_r|^{\otimes M} |\vec{m}\rangle\langle\vec{n}|] |\phi_r\rangle\langle\phi_r| \\
&= \frac{M}{M+d} \rho^{(1)} + \frac{1}{M+d} \mathbb{I}.
\end{aligned} \quad (12)$$

The calculation details can be found in the Appendix. These results show that in the sense of a single-copy state, the CQSR is equivalent to a polarization channel with a *universal* fidelity $F = \frac{M+1}{M+d}$. So the single-copy output state is written universally as the input state with a shrinking factor and a completely mixed state with a corresponding probability. For identical pure input states $\rho = |\psi\rangle\langle\psi|^{\otimes M}$, we have $\rho^{(1)} = |\psi\rangle\langle\psi|$. We emphasize that the fidelity is defined between single input and output states.

Here we would like to address more discussions upon the number of users N, and the copy number of the input state M. The general quantum estimation scheme requires the input and output states to have the same copy number. However, as we used single-copy fidelity $\mathrm{Tr}[\rho^{(1)}\tilde{\rho}^{(1)}]$ instead of overall fidelity $\mathrm{Tr}[\rho\tilde{\rho}]$ as the figure of merit, the preparation state may take the direct product form. During this process we actually discarded all the entanglement contained in the original state, which enables us to go beyond the quantum estimation scheme to extend the user number to arbitrary N. Correspondingly the definition of single-copy fidelity is slightly modified from $\mathrm{Tr}_{M-1}[\cdot]$ to $\mathrm{Tr}_{N-1}[\cdot]$ for the partial trace, while leaving the main conclusions of this paper unchanged.

For the protocol of CQSR, the importance of our results is that we only need to find a $(M+1)$-copy CSS; the state $|\psi\rangle\langle\psi|^{\otimes M}$ can be optimally distributed to an arbitrary number of users, provided each user can reconstruct the quantum state by a known ensemble of states based on the classical information broadcasted. It is then crucial that the CSS contains only a finite number of states, so that it is physically realizable. Operationally, by using $(M+1)$-copy CSS with a finite number of states, we can optimally distribute the quantum state to an arbitrary number of spatially separated parties without a quantum channel. We remark that the optimal fidelity corresponds to that of a universal quantum cloning machine for infinite copies, however, the cloning machine needs a quantum channel to achieve this aim.

IV. EXAMPLES

In the following we show the protocol of CQSR by two insightful examples.

Example A. First let us consider the case where a single qudit (state in d-dimension Hilbert space) is measured and broadcasted. Our results suggest that if a 2-copy CSS with finite states is found, a single qudit can be distributed with the optimal fidelity $\frac{2}{d+1}$. To construct this CSS set, we introduce the so-called mutually unbiased bases (MUBs); see, for example, [16,17]. For a Hilbert space with dimension d, the MUBs contain $d+1$ sets of the orthogonal basis $\{|\psi_t^k\rangle\}$, $t = 0,\dots d-1$, $k = 0,\dots d$. Any states belong to different basis $|\psi_t^k\rangle$ and $|\psi_{t'}^{k'}\rangle (k \neq k')$ satisfy the condition, $|\langle\psi_t^k|\psi_{t'}^{k'}\rangle| = 1/\sqrt{d}$, meaning unbiased for all states. The construction of MUBs for the case that d is an odd prime number is already well studied and known to take the following form, $|\psi_t^0\rangle = |t\rangle$, $|\psi_t^k\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}(\omega^t)^{d-j}(\omega^{-k})^{s_j}|j\rangle$, $(k \neq 0)$, $t = 0,\dots d-1$, where $\{|j\rangle\}_0^{d-1}$ is the computational basis, $s_j = j + \dots + (d-1)$, and $\omega = \exp(2\pi i/d)$.

We point out that MUBs set constitutes a 2-copy CSS,

$$\frac{1}{d(d+1)}\sum_{k=0}^{d}\sum_{t=0}^{d-1}|\psi_t^k\rangle\langle\psi_t^k|^{\otimes 2} = \frac{\mathbb{I}_+^2}{d_2^+}. \tag{13}$$

This identity can be proved by direct calculations (see the Appendix). According to our results, we know that by measurement corresponding to MUBs, a single qudit can be optimally distributed without the availability of the quantum channel,

$$\begin{aligned}\tilde{\rho} &= \frac{1}{d(d+1)}\sum_{k=0}^{d}\sum_{t=0}^{d-1}\mathrm{Tr}\big(|\psi_t^k\rangle\langle\psi_t^k|\rho\big)|\psi_t^k\rangle\langle\psi_t^k| \\ &= \frac{1}{d+1}\rho + \frac{1}{d+1}I_d.\end{aligned} \tag{14}$$

The fidelity is $F = 2/(d+1)$ which is optimal. Explicitly, the state ρ is measured in the cloud by projective measurement corresponding to MUBs; the results are broadcasted. Based on broadcasting information, each user can construct a quantum state $\tilde{\rho}$ by ensemble states of MUBs with optimal fidelity.

However, the MUBs set is not a general $(M+1)$-copy CSS for $M \geqslant 1$. We propose that the construction of general $(M+1)$-copy CSS should be an open problem.

Example B. Now we consider the qubit situation for case $M = 2$, $d = 2$. The two-dimensional MUBs can also be applied to this problem, where MUBs correspond to the known six bases denoted as (see, for example, [3])

$$|0\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle), \quad |\tilde{+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle),$$
$$|1\rangle, |-\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle), \quad |\tilde{-}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle).$$

By straightforward calculation, one can find that the six states form a 3-copy CSS,

$$\frac{1}{6}\sum_{\alpha=0,1,+,-,\tilde{+},\tilde{-}}|\alpha\rangle\langle\alpha|^{\otimes 3} = \frac{\mathbb{I}_+^3}{d_3^+}. \tag{15}$$

With these six bases, one can estimate two identical qubits $|\psi\rangle^{\otimes 2}$ with optimal fidelity,

$$\tilde{\rho} = \frac{1}{6}\sum_{\alpha}\mathrm{Tr}(|\alpha\rangle\langle\alpha|^{\otimes 2}|\psi\rangle\langle\psi|^{\otimes 2})|\alpha\rangle\langle\alpha|^{\otimes N}, \tag{16}$$

where we write explicitly N in the equation to point out that the number of users N is arbitrary. One can check that a single-qubit output takes the form,

$$\tilde{\rho}^{(1)} = \tfrac{1}{2}|\psi\rangle\langle\psi| + \tfrac{1}{4}I_2. \tag{17}$$

The fidelity is optimal corresponding to the universal quantum cloning machine $2 \to \infty$, which confirms that our method is applicable.

We emphasize here that the MUB-constructed CSS is only valid for limited cases. For arbitrary M and d, the completeness relationship is not fulfilled. On the other hand, we conjecture that ∞-copy CSS could only be realized by infinite sets. If it is true, then any effort to find out a physical realizable finite CSS would be futile, making the construction of CSS of arbitrary dimension and copies a crucial task. However, when given a fixed copy number M and dimension d, the construction of M-copy CSS could be achievable. Assume that the POVM $\{\hat{O}_r\}_{r=1}^R$, or more specifically, the states $|\phi_r\rangle\langle\phi_r|$, are randomly given; then one only needs to find out a set of positive numbers $\{c_r\}_{r=1}^R$ to satisfy the completeness relationship (4). This simplifies the CSS construction to solving $d_M^+(d_M^+ + 1)/2$ linear equations with R unknown variables. By increasing R, which is the total number of POVMs contained in CSS, these equations will be heavily under-determined so that there are enough free parameters to make the R unknown variables all positive. However, it remains a complicated task when M is very large and decreasing the number of equations should be considered. It is proved in [8] that by applying a set of rotations $|\phi_r^m\rangle = \exp(i\tilde{X}\theta_m)|\phi_r\rangle$, where operator $\tilde{X}$ and constant θ_m are carefully chosen, one can decrease the number of equations to d_M^+, that is, as long as the diagonal elements in (2) are satisfied, the off-diagonal elements are satisfied as well.

V. CONCLUSION

In conclusion, we have studied the CQSR protocol meaning the quantum state reconstruction method in the absence of a quantum channel and provided a physical realizable measurement-and-prepare scheme which achieves the optimal mean fidelity. The measurement bases of an optimal CQSR must take the form of M-copy CSS. The universal case is also taken into consideration, and we prove that to make the fidelity uniform for arbitrary input, one only needs to further require the bases to be $(M+1)$-copy CSS. Two examples for qudit and qubit are given to show the applicability of our method. We expect that CQSR may stimulate investigations on quantum information distribution and concentration.

ACKNOWLEDGMENTS

This work was supported by the National Key R & D Plan of China (Grants No. 2016YFA0302104 and No. 2016YFA0300600), the National Natural Science Foundation of China (Grants No. 91536108 and No. 11774406), and Strategic Priority Research Program of Chinese Academy of Sciences (Grant No. XDB28000000).

APPENDIX

1. Single-copy outcome in quantum state reconstruction

After the quantum state distribution process, the single-copy state of the outcome $\tilde{\rho}$ is

$$\tilde{\rho}^{(1)} = \mathrm{Tr}_{M-1}[\mathcal{E}(\rho)]$$
$$= \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{r=1}^{R} d_M^+ c_r \mathrm{Tr}[|\phi_r\rangle\langle\phi_r|^{\otimes M}|\vec{m}\rangle\langle\vec{n}|]|\phi_r\rangle\langle\phi_r|$$
$$= \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{r=1}^{R} d_M^+ c_r \sum_{\alpha,\beta=0}^{d-1} |\alpha\rangle\langle\beta|,$$
$$\mathrm{Tr}[|\phi_r\rangle\langle\phi_r|^{\otimes M}|\vec{m}\rangle\langle\vec{n}|]\mathrm{Tr}[|\phi_r\rangle\langle\phi_r||\beta\rangle\langle\alpha|]$$
$$= \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{\alpha,\beta=0}^{d-1} |\alpha\rangle\langle\beta|\mathrm{Tr}\Bigg[(|\vec{m}\rangle\otimes|\beta\rangle)(\langle\vec{n}|\otimes\langle\alpha|) \times \sum_{r=1}^{R} d_M^+ c_r |\phi_r\rangle\langle\phi_r|^{\otimes M+1}\Bigg].$$

Then we take into account the CSS relation (4) in the main text, and note that $\mathbb{I}_+^{M+1} = \sum_{\vec{s}}^{C(\vec{s})=M+1} |\vec{s}\rangle\langle\vec{s}|$, we have

$$\tilde{\rho}^{(1)} = \frac{d_M^+}{d_{M+1}^+} \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{\alpha,\beta=0}^{d-1} |\alpha\rangle\langle\beta| \times \mathrm{Tr}\Bigg[(|\vec{m}\rangle\otimes|\beta\rangle)(\langle\vec{n}|\otimes\langle\alpha|) \sum_{\vec{s}}^{C(\vec{s})=M+1} |\vec{s}\rangle\langle\vec{s}|\Bigg]$$
$$= \frac{d_M^+}{d_{M+1}^+} \sum_{\vec{m},\vec{n}} A_{\vec{m}\vec{n}} \sum_{\alpha,\beta=0}^{d-1} |\alpha\rangle\langle\beta| \times \sum_{\vec{s}}^{C(\vec{s})=M+1} \frac{\sqrt{m_\beta+1}}{\sqrt{M+1}} \frac{\sqrt{n_\alpha+1}}{\sqrt{M+1}} \delta_{\vec{s},\vec{m}+\vec{\beta}} \delta_{\vec{s},\vec{n}+\vec{\alpha}}$$
$$= \sum_{\alpha,\beta=0}^{d-1} \sum_{\vec{m},\vec{n}} \frac{A_{\vec{m}\vec{n}} \delta_{\vec{m}+\vec{\beta},\vec{n}+\vec{\alpha}} \sqrt{(m_\beta+1)(n_\alpha+1)}}{M+d} |\alpha\rangle\langle\beta|. \tag{A1}$$

The Kronecker-δ requires when $\alpha \neq \beta$, we have $m_\beta + 1 = n_\beta$ and $n_\alpha + 1 = m_\alpha$, and when $\alpha = \beta$, we have $\vec{m} = \vec{n}$. Then the above equation takes a more concise form,

$$\tilde{\rho}^{(1)} = \sum_{\alpha=0}^{d-1} \sum_{\vec{m}} \frac{m_\alpha+1}{M+d} A_{\vec{m}\vec{m}} |\alpha\rangle\langle\alpha| + \sum_{\alpha\neq\beta} \sum_{\vec{m},\vec{n}} \frac{\sqrt{m_\alpha n_\beta}}{M+d} A_{\vec{m}\vec{n}} |\alpha\rangle\langle\beta|. \tag{A2}$$

By tedious but straightforward calculations, we obtain Eq. (12) in the main text:

$$\tilde{\rho}^{(1)} = \frac{M}{M+d}\rho^{(1)} + \frac{1}{M+d}\mathbb{I}. \tag{A3}$$

2. Two-copy CSS for d-dimensional case

Next we will prove that

$$\hat{Q} = \frac{1}{d(d+1)} \left(\sum_j |j\rangle\langle j|^{\otimes 2} + \sum_{k=1}^{d} \sum_{t=0}^{d-1} \big|\psi_t^{(k)}\big\rangle\big\langle\psi_t^{(k)}\big|^{\otimes 2} \right) = \mathbb{I}_+^2 / d_M^+. \tag{A4}$$

In fact, direct calculation gives

$$\langle j_1 j_1|\hat{Q}|j_2 j_2\rangle = \frac{1}{d(d+1)} \times \left(\sum_{k=1}^{d} \sum_{t=0}^{d-1} \langle j_1 j_1| \big(\big|\psi_t^{(k)}\big\rangle\big\langle\psi_t^{(k)}\big|\big)^{\otimes 2} |j_2 j_2\rangle \right) = \frac{1}{d(d+1)} \frac{1}{d} \sum_{k=1}^{d} \sum_{t=0}^{d-1} \omega^{2t(j_2-j_1)+k(s_{j_2}-s_{j_1})},$$

$$\langle j_1, j_2|\hat{Q}|jj\rangle = \frac{1}{d(d+1)} \times \left(\sum_{k=1}^{d} \sum_{t=0}^{d-1} \langle j_1, j_2| \big(\big|\psi_t^{(k)}\big\rangle\big\langle\psi_t^{(k)}\big|\big)^{\otimes 2} |jj\rangle \right) = \frac{1}{d(d+1)} \frac{1}{d^2} \times \sum_{k=1}^{d} \sum_{t=0}^{d-1} \omega^{t(2j-j_1-j_2)-k(s_{j_1}+s_{j_2}-2s_j)},$$

$$\langle j_1, j_2|\hat{Q}|j_3, j_4\rangle = \frac{1}{d(d+1)} \times \sum_{k=1}^{d} \sum_{t=0}^{d-1} \langle j_1, j_2| \big(\big|\psi_t^{(k)}\big\rangle\big\langle\psi_t^{(k)}\big|\big)^{\otimes 2} |j_3, j_4\rangle = \frac{1}{d(d+1)} \frac{\sqrt{2}}{d^2} \times \sum_{k=1}^{d} \sum_{t=0}^{d-1} \omega^{t(j_3+j_4-j_1-j_2)-k(s_{j_1}+s_{j_2}-s_{j_3}-s_{j_4})}.$$

We can verify that only $\langle jj|\hat{Q}|jj\rangle$- and $\langle j_1, j_2|\hat{Q}|j_1, j_2\rangle$- type elements are nonzero, which indicates $\hat{Q}$ is diagonalized. Further direct calculation proves that the diagonal elements corresponding to these two types have the same value $2/d(d+1)$, i.e., $\hat{Q} = \mathbb{I}_+^2/d_2^+$.

3. Necessary condition for M-copy universal optimal estimation

Now we prove the necessity for the measurement basis to be $(M{+}1)$-copy CSS. Suppose that there exists a set of states which forms an optimal estimation measurement operator,

$$\sum_{r=1}^{R} c_r|\psi_r\rangle\langle\psi_r|^{\otimes M+1} = \mathbb{I}_+^{M+1}/d_{M+1}^+ + \hat{P}.$$

Operator $\hat{P}$ lies in symmetric subspace $\mathcal{H}_+^{M+1}$ because the left-hand side of the equation belongs to the symmetric subspace. We prove that there must be $\hat{P}=0$. The output single-copy state is

$$\tilde{\rho}^{(1)} = \frac{M+1}{M+d}\rho^{(1)} + \frac{1}{M+d}\mathbb{I} + \sum_{k,l=0}^{d-1}|k\rangle\langle l|\mathrm{Tr}[(\rho\otimes|l\rangle\langle k|)\hat{P}]. \tag{A5}$$

To make sure that for arbitrary input the fidelity is optimal, the second term must always be equal to 0, that is,

$$\Delta_{lk} = \mathrm{Tr}[(\rho\otimes|l\rangle\langle k|)\hat{P}] = 0, \quad \forall\rho\in\mathcal{H}_+^{\otimes M}, |k\rangle, |l\rangle\in\mathcal{H}.$$

This condition is satisfied only when $\hat{P}=0$. The following part gives a detailed proof.

Since $\hat{P}\in\mathcal{H}_+^{M+1}$, we apply the following expansion form of the operator:

$$\hat{P} = \sum_{\vec{r},\vec{s}}^{C(\vec{r})=C(\vec{s})=M+1} P_{rs}|\vec{r}\rangle\langle\vec{s}|. \tag{A6}$$

First consider the diagonal elements P_{rr}. Suppose that $r_k\neq 0$, choose $\rho = |\vec{r}-\vec{k}\rangle\langle\vec{r}-\vec{k}|$, and (A6) gives

$$0 = \Delta_{kk} = P_{rr}\times\frac{r_k}{M} \Rightarrow P_{rr}=0, \tag{A7}$$

that is, the diagonal elements are all zeros.

Then consider the off-diagonal elements P_{rs}, suppose $r_k\neq 0$, $s_l\neq 0$, and for simplicity, let $\vec{m}=\vec{r}-\vec{k}$, $\vec{n}=\vec{s}-\vec{l}$. For state $\rho = \frac{1}{\lambda_1^2+\lambda_2^2}(\lambda_1|\vec{m}\rangle + \lambda_2 e^{i\phi}|\vec{n}\rangle)(\lambda_1\langle\vec{m}| + \lambda_2 e^{-i\phi}\langle\vec{n}|)$, where λ_1,λ_2,ϕ are non-negative real numbers, $\phi\in[0,2\pi]$. Then (A6) gives

$$\Delta_{kl} = \frac{1}{\lambda_1^2+\lambda_2^2}\big(\lambda_1^2 A + \lambda_2^2 B + \lambda_1\lambda_2(Ce^{i\phi}+De^{-i\phi})\big) = 0,$$

which is satisfied for arbitrary λ_1,λ_2,ϕ. Here

$$A = \mathrm{Tr}[(|\vec{m}\rangle\langle\vec{m}|\otimes|l\rangle\langle k|)\hat{P}], \tag{A8}$$

$$B = \mathrm{Tr}[(|\vec{n}\rangle\langle\vec{n}|\otimes|l\rangle\langle k|)\hat{P}], \tag{A9}$$

$$C = \mathrm{Tr}[(|\vec{n}\rangle\langle\vec{m}|\otimes|l\rangle\langle k|)\hat{P}], \tag{A10}$$

$$D = \mathrm{Tr}[(|\vec{m}\rangle\langle\vec{n}|\otimes|l\rangle\langle k|)\hat{P}]. \tag{A11}$$

Then we have $A=B=C=D=0$, and $C=0$ gives

$$\frac{\sqrt{r_k s_l}}{M+1}P_{rs} = 0 \Rightarrow P_{rs}=0, \tag{A12}$$

that is, the off-diagonal elements are also zeros. Therefore $\hat{P}=0$, which indicates that the quantum estimation is universal only when its measurement bases are $(M{+}1)$-copy CSS.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[2] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[3] H. Fan, Y. N. Wang, L. Jing, J. D. Yue, H. D. Shi, Y. L. Zhang, and L. Z. Mu, Phys. Rep. **544**, 241 (2014).

[4] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Rev. Mod. Phys. **77**, 1225 (2005).

[5] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[6] Y. L. Zhang, Y. N. Wang, X. R. Xiao, L. Jing, L. Z. Mu, V. E. Korepin, and H. Fan, Phys. Rev. A **87**, 022302 (2013).

[7] M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).

[8] R. Derka, V. Bužek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).

[9] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[10] W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, and M. Mosca, Phys. Rev. Lett. **98**, 090501 (2007).

[11] G. Chiribella and G. M. D'Ariano, Phys. Rev. Lett. **97**, 250503 (2006).

[12] Y. X. Yang, G. Chiribella, and D. Ebler, Phys. Rev. Lett. **116**, 080501 (2016).

[13] Y. X. Yang, G. Chiribella, and M. Hayashi, Phys. Rev. Lett. **117**, 090502 (2016).

[14] G. Chiribella and Y. X. Yang, Front. Phys. **11**, 110304 (2016).

[15] Q. L. Wang, S. Das, and M. M. Wilde, Quant. Info. Proc. **16**, 248 (2017).

[16] S. Bandyopadhyay *et al.*, Algorithmica **34**, 512 (2002).

[17] H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).