ARTICLE   OPEN

Optimal verification of general bipartite pure states

Xiao-Dong Yu [1]*, Jiangwei Shang [2,3]* and Otfried Gühne [1]*

The efficient and reliable verification of quantum states plays a crucial role in various quantum information processing tasks. We consider the task of verifying entangled states using one-way and two-way classical communication and completely characterize the optimal strategies via convex optimization. We solve these optimization problems using both analytical and numerical methods, and the optimal strategies can be constructed for any bipartite pure state. Compared with the nonadaptive approach, our adaptive strategies significantly improve the efficiency of quantum state verification. Moreover, these strategies are experimentally feasible, as only few local projective measurements are required.

INTRODUCTION

A basic yet important step in most quantum information processing tasks is to efficiently and reliably characterize a quantum state. The standard approach is to perform quantum state tomography by fully reconstructing the density matrix.[1] However, tomography is known to be both time consuming and computationally hard due to the exponentially increasing number of parameters to be reconstructed;[2,3] moreover, the underlying approximations may be conceptually problematic.[4] In fact, full tomographic information is often not required, and a lot of effort has been devoted to characterizing quantum states with non-tomographic methods.[5–8] Recently, an alternative statistical approach, namely quantum state verification, has triggered much research interest due to its powerful efficacy.[9–13]

Quantum state verification is a procedure for gaining confidence that the output of some quantum device is a particular state by employing local measurements.[9] Consider a device that is supposed to produce the target state $|\psi\rangle$, but may in practice produce $\sigma_1, \sigma_2, \ldots, \sigma_N$ in N runs. In the ideal scenario, the verifier has the promise that either $\sigma_k = |\psi\rangle\langle\psi|$ for all k or that σ_k have a finite distance to $|\psi\rangle$, i.e., $\langle\psi|\sigma_k|\psi\rangle \leq 1 - \varepsilon$ for all k. Given access to some set of allowed measurements, the verifier must certify that the source prepares $|\psi\rangle$. One cannot exclude that he certifies the source to be correct although it is not, but this failure probability δ should be as small as possible.

In general, for each state σ_k the verifier may apply a different measurement with some predefined probability. So a state verification strategy can be expressed as $\Omega = \sum_{i=1}^{n} p_i \Omega_i$, where $(p_1, p_2, \ldots, p_n)$ is a probability distribution, and $\{\Omega_i, \mathbb{1} - \Omega_i\}$ are allowed measurements with outcomes labeled by "pass" and "fail", respectively. For each output state σ_k, the verifier randomly chooses a measurement $\{\Omega_i, \mathbb{1} - \Omega_i\}$ with probability p_i, then performs the test. In a pass instance, the verifier continues to state σ_{k+1}, otherwise the verification ends and the verifier concludes that the state was not $|\psi\rangle$. To guarantee that the perfect state $|\psi\rangle$ is never rejected we assume Ω_i satisfies $\langle\psi|\Omega_i|\psi\rangle = 1$; it has been observed in ref. [9] that such strategies are better than others. The worst-case failure probability of each run is given by $\max_{\langle\psi|\sigma|\psi\rangle\leq 1-\varepsilon}\text{Tr}(\Omega\sigma) = 1 - \varepsilon v(\Omega)$, where $v(\Omega)$ represents the spectral gap between the largest and the second largest eigenvalues of Ω.[9]

In the case that all N states pass the test, we achieve the confidence $1 - \delta$ with

$$\delta \leq [1 - \varepsilon v(\Omega)]^N. \tag{1}$$

In reality, however, quantum devices are never perfect, so the verifier cannot be promised that either $\sigma_k = |\psi\rangle\langle\psi|$ or $\langle\psi|\sigma_k|\psi\rangle \leq 1 - \varepsilon$ for all k. Instead, a more practical task is to certify with high confidence that the fidelity of the output state is larger than a threshold value $1 - \varepsilon$. In this case, the verifier measures the frequency f of the pass instances. If $f > 1 - \varepsilon v(\Omega)$, the confidence $1 - \delta$ can be derived from the Chernoff bound[14,15]

$$\delta \leq e^{-D[f\|(1-\varepsilon v(\Omega))]N}, \tag{2}$$

where $D(x \| y) = x\log(\frac{x}{y}) + (1 - x)\log(\frac{1-x}{1-y})$ is the Kullback–Leibler divergence.

The advantage of the state verification approach is that the failure probability δ decreases exponentially with N, hence the target state $|\psi\rangle$ can be potentially verified using only few copies of the state. As seen from Eqs. (1) and (2), the performance of a verification strategy depends solely on $v(\Omega)$. Therefore, to achieve an optimal strategy, we need to maximize $v(\Omega)$ over all accessible measurements. Although lots of effort has been devoted to this research line, few optimal strategies have been found. To the best of our knowledge, the only optimal strategy reported by now is the verification of two-qubit pure states with local projective measurements (PMs).[9]

In this work, we introduce adaptive measurements, i.e., measurements assisted by local operations and classical communication (LOCC)[16,17] to the task of quantum state verification. We show that the efficiency of the verification can be significantly improved by considering adaptive measurements. For any $d_1 \times d_2$ bipartite pure state, we explicitly construct the optimal one-way, as well as near-optimal two-way adaptive verification strategies. Best of all, in these strategies, only few local PMs are needed for their implementation in the laboratory.

RESULTS

Optimal state verification as convex optimization

In the following, we derive two convex optimization problems that completely characterize the optimal adaptive state verification

strategies assisted by one-way and one-round two-way classical communication, respectively. In general, to get an optimal verification strategy, we need to consider the optimization problem

$$\underset{p_i, \Omega_i}{\text{maximize}} \quad v(\Omega)$$

$$\text{subject to} \quad \Omega = \sum_{i=1}^{n} p_i \Omega_i,$$

$$\sum_{i=1}^{n} p_i = 1, p_i \geq 0, \text{for all } i, \tag{3}$$

$$\langle \psi | \Omega_i | \psi \rangle = 1, \Omega_i \in \mathcal{M}, \text{for all } i,$$

where $|\psi\rangle$ is the target state we want to verify, and $\mathcal{M}$ denotes the set of all allowed measurements. Be reminded that $v(\Omega)$ represents the spectral gap between the largest and the second largest eigenvalues of Ω. As $\Omega_i \leq \mathbb{1}$, the last constraint leads to $\Omega_i |\psi\rangle = |\psi\rangle$ and $P^\perp \Omega_i P^\perp = \Omega_i - |\psi\rangle\langle\psi|$, where $P^\perp = \mathbb{1} - |\psi\rangle\langle\psi|$. Hence, $v(\Omega)$ admits an alternative expression

$$v(\Omega) = 1 - ||P^\perp \Omega P^\perp||, \tag{4}$$

where $|| \cdot ||$ denotes the largest eigenvalue.

Generally speaking, the optimization in Eq. (3) is difficult to solve, if not impossible at all, because the set of all possible measurements cannot be easily characterized. Here, we give a complete characterization of Ω for both one-way and one-round two-way adaptive measurements, then reduce the corresponding problems to convex optimization. These optimization problems can be further simplified and solved. For succinctness, hereafter we restrict the two-way adaptive measurements to one-round communication only. In addition, the accessible measurements allowed in our verification strategies are not restricted to PMs, i.e., positive operator-valued measures (POVMs) are possible, although in the end we show that the optimal strategies can be achieved with PMs in most cases.

Without loss of generality, a bipartite pure state can be written as $|\psi\rangle = \sum_{i=1}^{d} \lambda_i |ii\rangle$, where the Schmidt coefficients satisfy $\lambda_1 \geq \lambda_2 \geq \dots \lambda_d > 0$ and $\sum_{i=1}^{d} \lambda_i^2 = 1$.[18]

We start with the analysis of one-way communication. In this case, Alice first performs a measurement, and sends the measurement outcome to Bob. Bob then chooses his measurement in accordance with Alice's measurement outcome. Hence, the one-way adaptive strategy $\Omega^\rightarrow$ takes the form

$$\Omega^\rightarrow = \sum_{i=1}^{n} p_i \Omega_i^\rightarrow, \quad \Omega_i^\rightarrow = \sum_a M_{a|i} \otimes N_{a|i}, \tag{5}$$

where $\{M_{a|i}\}_a$ are measurements on Alice's system, and each $\{N_{a|i}, \mathbb{1} - N_{a|i}\}$ is a "pass" or "fail" measurement on Bob's system depending on Alice's measurement outcome. Here, we can assume that the $M_{a|i}$ are rank-one, otherwise some further decomposition can make this assumption satisfied. If the joint system is in state $|\psi\rangle$, Bob's subsystem would collapse to some pure state $P_{a|i} = \text{Tr}_A(M_{a|i} \otimes \mathbb{1} |\psi\rangle\langle\psi|)/\text{Tr}(M_{a|i} \otimes \mathbb{1} |\psi\rangle\langle\psi|)$ after Alice's measurement $\{M_{a|i}\}_a$. Then the best strategy for Bob is to perform the measurement $\{P_{a|i}, \mathbb{1} - P_{a|i}\}$ to verify whether his subsystem is in state $P_{a|i}$. Mathematically, to ensure that $\langle\psi|\Omega_i^\rightarrow|\psi\rangle = 1$, $N_{a|i}$ must satisfy that $N_{a|i} \geq P_{a|i}$. If all $N_{a|i}$ satisfy $N_{a|i} = P_{a|i}$, we call the one-way adaptive strategy $\Omega^\rightarrow$ semi-optimal. Hence, to maximize $v(\Omega^\rightarrow)$, i.e., to minimize $||\sum_i p_i P^\perp \Omega_i^\rightarrow P^\perp||$, we can restrict $\Omega^\rightarrow$ to be semi-optimal strategies.

From the definition, we get the following necessary conditions for $\Omega^\rightarrow$ being semi-optimal

$$\Omega^\rightarrow \in \mathcal{S}, \quad \text{Tr}_B(\Omega^\rightarrow) = \mathbb{1}, \quad \langle\psi|\Omega^\rightarrow|\psi\rangle = 1, \tag{6}$$

where $\mathcal{S}$ is the set of separable operators, i.e., unnormalized separable states.[17] Next, we show that these constraints are also sufficient. $\Omega^\rightarrow$ is separable implies that there exists a

decomposition $\Omega^\rightarrow = \sum_a M_a \otimes N_a$, such that M_a are positive semidefinite and N_a are rank-one projectors. Then, $\text{Tr}_B(\Omega^\rightarrow) = \mathbb{1}$ implies $\sum_a M_a = \mathbb{1}$, i.e., $\{M_a\}_a$ is a measurement on Alice's system. This concludes our proof by taking into account the last constraint. Thus, the optimization in Eq. (3) can be written as

$$\underset{\Omega^\rightarrow}{\text{maximize}} \quad v(\Omega^\rightarrow)$$

$$\text{subject to} \quad \Omega^\rightarrow \in \mathcal{S},$$

$$\text{Tr}_B(\Omega^\rightarrow) = \mathbb{1}, \tag{7}$$

$$\langle\psi|\Omega^\rightarrow|\psi\rangle = 1,$$

for one-way adaptive verification strategies.

We move on to discuss the one-round two-way communication scenario. In this case, Alice and Bob use shared randomness to decide who performs the measurement first. After the measurement, he/she sends the measurement outcome to the other party. Then the receiver chooses her/his measurement according to the received measurement outcome. Thanks to the permutation symmetry of $|\psi\rangle = \sum_{i=1}^{d} \lambda_i |ii\rangle$, the optimization in this setting can be easily simplified. Let S be the SWAP operator, i.e., $S|i\rangle|j\rangle = |j\rangle|i\rangle$ for all $i, j = 1, 2, \dots, d$, then we have $S|\psi\rangle = |\psi\rangle$. This indicates that, for two-way adaptive measurements, if Ω satisfies the constraints in Eq. (3), so does $\frac{1}{2}(\Omega + S\Omega S^\dagger)$. Furthermore, Eq. (4) implies

$$v\left[\frac{1}{2}(\Omega + S\Omega S^\dagger)\right] \geq \frac{1}{2}\left[v(\Omega) + v(S\Omega S^\dagger)\right] = v(\Omega). \tag{8}$$

Hence, we can focus on the two-way adaptive strategies $\Omega^\leftrightarrow$ that are invariant under the SWAP operation, i.e., $\Omega^\leftrightarrow = \frac{1}{2}(\Omega^\rightarrow + \Omega^\leftarrow)$, where $\Omega^\rightarrow$ is a one-way adaptive strategy and $\Omega^\leftarrow = S\Omega^\rightarrow S^\dagger$. Similarly, to optimize $v(\Omega^\leftrightarrow)$, we can also restrict $\Omega^\rightarrow$ to be semi-optimal. Thus, the optimization in Eq. (3) can be written as

$$\underset{\Omega^\rightarrow}{\text{maximize}} \quad v\left[\frac{1}{2}(\Omega^\rightarrow + \Omega^\leftarrow)\right]$$

$$\text{subject to} \quad \Omega^\rightarrow \in \mathcal{S},$$

$$\text{Tr}_B(\Omega^\rightarrow) = \mathbb{1}, \tag{9}$$

$$\langle\psi|\Omega^\rightarrow|\psi\rangle = 1,$$

for two-way adaptive verification strategies.

Optimal verification of two-qubit states

Without loss of generality, we write the two-qubit entangled pure state as $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $0 < \theta \leq \pi/4$. Then the subspace $P^\perp$ is spanned by $\{|\psi_i\rangle\}_{i=1}^{3} := \{|01\rangle, |10\rangle, \sin\theta|00\rangle - \cos\theta|11\rangle\}$.

First, we need a group G to simplify the optimizations. The group G is defined to be generated by the unitary operator $g = \Phi \otimes \Phi^\dagger$, where Φ is the phase gate, i.e., $\Phi|0\rangle = |0\rangle$ and $\Phi|1\rangle = i|1\rangle$. Then we can show

$$\tilde{\Omega} := \frac{1}{4}\sum_{k=0}^{3} g^k \Omega g^{-k} = \sum_{i=1}^{3} w_i |\psi_i\rangle\langle\psi_i| + |\psi\rangle\langle\psi|, \tag{10}$$

for some w_i; see Supplementary Note A for the proof. As $g|\psi\rangle = |\psi\rangle$, $\tilde{\Omega}$ also satisfies the constraints in Eqs. (7) and (9) if Ω does. Furthermore, Eq. (4) implies

$$v(\tilde{\Omega}) \geq \frac{1}{4}\sum_{k=0}^{3} v(g^k \Omega g^{-k}) = v(\Omega). \tag{11}$$

Thus, we can restrict to the diagonal $\Omega^\rightarrow$ as in Eq. (10) for the optimizations in Eqs. (7) and (9).

Then, we consider the case of one-way adaptive verification. For two-qubit quantum states, the positive partial transpose (PPT) criterion is necessary and sufficient to characterize their separability.[19,20] Thus, by combining Eq. (10) with the PPT criterion, the

optimization in Eq. (7) can be written as

$$\begin{aligned}
\underset{w_i}{\text{maximize}} \quad & \min_i\{1 - w_i\} \\
\text{subject to} \quad & w_i \geq 0, i = 1, 2, 3, \\
& w_1 = \sin^2\theta(1 - w_3), \\
& w_2 = \cos^2\theta(1 - w_3),
\end{aligned} \tag{12}$$

where the constraints arise only from $\Omega^{\rightarrow} \geq 0$ and $\text{Tr}_B(\Omega^{\rightarrow}) = \mathbb{1}$, since the PPT criterion gives the redundant condition $w_1 w_2 \geq \sin^2\theta\cos^2\theta(1 - w_3)^2$. As $0 < \theta \leq \pi/4$, we have $w_2 \geq w_1$. Thus, the solution of Eq. (12) is attained when $w_2 = w_3$, and

$$\max_{\Omega^{\rightarrow}} v(\Omega^{\rightarrow}) = \frac{1}{1 + \cos^2\theta}. \tag{13}$$

In general, the measurements associated with the optimal solution are POVMs. However, one can directly calculate that the bound in Eq. (13) can be achieved already with PMs

$$\Omega^{\rightarrow} = \frac{\cos^2\theta}{1 + \cos^2\theta}P_{ZZ}^+ + \frac{1}{2(1 + \cos^2\theta)}X_\psi^{\rightarrow} + \frac{1}{2(1 + \cos^2\theta)}Y_\psi^{\rightarrow}, \tag{14}$$

where

$$\begin{aligned}
P_{ZZ}^+ &= |0\rangle\langle0| \otimes |0\rangle\langle0| + |1\rangle\langle1| \otimes |1\rangle\langle1|, \\
X_\psi^{\rightarrow} &= |\varphi_0\rangle\langle\varphi_0| + |\varphi_2\rangle\langle\varphi_2|, \\
Y_\psi^{\rightarrow} &= |\varphi_1\rangle\langle\varphi_1| + |\varphi_3\rangle\langle\varphi_3|,
\end{aligned} \tag{15}$$

with $|\varphi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)$ and $|\varphi_k\rangle = g^k|\varphi_0\rangle$.

Next, we discuss the case of two-way adaptive verification. By combining Eq. (10) and the PPT criterion, we can get a simplification of the optimization in Eq. (9) by simply replacing the objective function in Eq. (12) with

$$\underset{w_i}{\text{maximize}} \quad \min\left\{1 - \frac{1}{2}(w_1 + w_2), 1 - w_3\right\}, \tag{16}$$

whose solution is given by

$$\max_{\Omega^{\leftrightarrow}} v(\Omega^{\leftrightarrow}) = \frac{2}{3}. \tag{17}$$

Again, we explicitly write down the PMs

$$\Omega^{\leftrightarrow} = \frac{1}{3}P_{ZZ}^+ + \frac{1}{6}X_\psi^{\rightarrow} + \frac{1}{6}X_\psi^{\leftarrow} + \frac{1}{6}Y_\psi^{\rightarrow} + \frac{1}{6}Y_\psi^{\leftarrow}, \tag{18}$$

where $P_{ZZ}^+, X_\psi^{\rightarrow}$, and $Y_\psi^{\rightarrow}$ are defined as in Eq. (15), and $X_\psi^{\leftarrow} = SX_\psi^{\rightarrow}S^\dagger$ and $Y_\psi^{\leftarrow} = SY_\psi^{\rightarrow}S^\dagger$.

Finally, we compare the adaptive strategies with the non-adaptive approach in ref. [9]. For two-qubit entangled states, we plot the optimal values of $v(\Omega)$ for different strategies in Fig. 1. As can be seen, the two-way strategy works much better than the one-way strategy, whereas both the adaptive strategies significantly outperform the nonadaptive one. Concerning the resources used in each strategy, we have the following remarks. Although no classical communication is involved in the measurement process of the nonadaptive strategy, it is still a necessary resource for the data processing after the measurement. On the contrary, the one-way adaptive strategy relies on classical communication for the measurements, but no classical communication is needed for the data processing as one party alone can determine whether the result is a pass or fail instance. The case for the two-way adaptive strategy is similar, but to obtain the final frequency of the pass instances, the two parties need to cooperate.

Optimal verification of general bipartite states

We move on to discuss the optimal adaptive verification of general bipartite states. Firstly, we need a larger group G for the general bipartite (two-qudit) pure state $|\psi\rangle = \sum_{i=1}^{d}\lambda_i|ii\rangle$, where the Schmidt coefficients satisfy $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_d > 0$ and $\sum_{i=1}^{d}\lambda_i^2 = 1$.
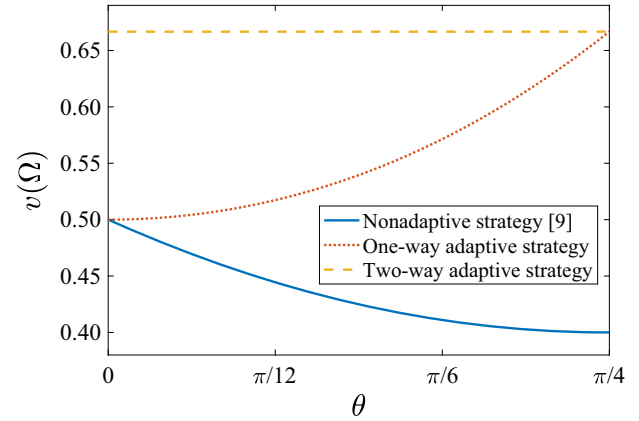

Fig. 1 Optimal values of $v(\Omega)$ with different verification strategies for the two-qubit entangled pure state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ **with** $0 < \theta < \pi/4$. Note that when $\theta = \pi/4$, i.e., $|\psi\rangle$ is the maximally entangled state, all three strategies give the same optimal value $v(\Omega) = 2/3$.

The group G is defined to be generated by the unitary operators $\{g_k = \Phi_k \otimes \Phi_k^\dagger, k = 1, 2, \ldots, d\}$, where $\Phi_k|j\rangle = i|j\rangle$ when $j = k$, and $\Phi_k|j\rangle = |j\rangle$ otherwise. Then we can show

$$\tilde{\Omega} := \frac{1}{|G|}\sum_{g \in G} g\Omega g^\dagger = \sum_{j \neq i, i=1}^{d} w_{ij}|ij\rangle\langle ij| + \sum_{i,j=1}^{d}\rho_{ij}|ii\rangle\langle jj|, \tag{19}$$

for some w_{ij} and ρ_{ij}, where $|G|$ is the order of G; see Supplementary Note A for the proof. Similar to the two-qubit case, if Ω satisfies the constraints in Eqs. (7) and (9), so does $\tilde{\Omega}$, since $g|\psi\rangle = |\psi\rangle$ for all $g \in G$. Furthermore, Eq. (4) implies

$$v(\tilde{\Omega}) \geq \frac{1}{|G|}\sum_{g \in G} v(g\Omega g^\dagger) = v(\Omega). \tag{20}$$

Hence, we can restrict $\Omega^{\rightarrow}$ to be of the form in Eq. (19) for the optimizations in Eqs. (7) and (9). Additionally, $\langle\psi|\Omega|\psi\rangle = 1$, i.e., $\Omega|\psi\rangle = |\psi\rangle$, means $\rho\boldsymbol{\lambda} = \boldsymbol{\lambda}$, where $\rho := (\rho_{ij})_{i,j=1}^{d}$ is Hermitian, and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_d)^\mathsf{T}$.

Secondly, we consider the case of one-way adaptive verification with the help of the group G. The main difference between two-qudit and two-qubit states is that the PPT criterion is only necessary but not sufficient to characterize the separability for $d \geq 3$.[20] Hence, by replacing $\Omega^{\rightarrow} \in \mathcal{S}$ with $(\Omega^{\rightarrow})^{T_B} \geq 0$, Eqs. (7) and (19) only give us a relaxation of the original optimization

$$\begin{aligned}
\underset{w_{ij}, \rho_{ij}}{\text{maximize}} \quad & \min\{1 - w_{ij}, 1 - \|\rho - \boldsymbol{\lambda}\boldsymbol{\lambda}^\mathsf{T}\|\} \\
\text{subject to} \quad & 0 \leq \rho \leq \mathbb{1}, w_{ij} \geq 0, \quad \text{for all } i \neq j, \\
& w_{ij}w_{ji} \geq |\rho_{ij}|^2, \quad \text{for all } i \neq j, \\
& \sum_{j \neq i} w_{ij} + \rho_{ii} = 1, \quad \text{for all } i, \\
& \rho\boldsymbol{\lambda} = \boldsymbol{\lambda},
\end{aligned} \tag{21}$$

where the constraints arise from $0 \leq \Omega^{\rightarrow} \leq \mathbb{1}$, the PPT criterion, $\text{Tr}_B(\Omega^{\rightarrow}) = \mathbb{1}$, and $\langle\psi|\Omega^{\rightarrow}|\psi\rangle = 1$ respectively. Therefore, the solution of this relaxed problem sets an upper bound of the optimal $v(\Omega^{\rightarrow})$. To show that the solution is a valid strategy, we still need to prove that the optimal $\Omega^{\rightarrow}$ obtained from Eq. (21) is separable. Here, instead of resorting to numerical methods, we can analytically solve the optimization in Eq. (21), which gives

$$\max_{\Omega^{\rightarrow}} v(\Omega^{\rightarrow}) \leq \frac{1}{1 + \lambda_1^2}, \tag{22}$$

for all $d \geq 2$. Moreover, the bound in Eq. (22) can be achieved with PMs

$$\Omega^{\rightarrow} = wP_{ZZ} + \frac{1-w}{|G|} \sum_{g \in G} gX_{\psi}^{\rightarrow} g^{\dagger}, \qquad (23)$$

where

$$P_{ZZ} = \sum_{k=1}^{d} |k\rangle\langle k| \otimes |k\rangle\langle k|, \quad X_{\psi}^{\rightarrow} = \sum_{k=1}^{d} |f_k\rangle\langle f_k| \otimes |\phi_k\rangle\langle\phi_k|,$$

$$|f_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} \gamma_d^{jk} |j\rangle, \quad |\phi_k\rangle = \sum_{j=1}^{d} \gamma_d^{-jk} \lambda_j |j\rangle, \qquad (24)$$

with $\gamma_d = e^{\frac{2\pi i}{d}}$ and $w = \lambda_1^2/(1 + \lambda_1^2)$; see Supplementary Note B for more details. In passing, we note two special cases of Eq. (24). When $|\psi\rangle$ is separable, i.e., $d = 1$, Eq. (24) gives the optimal nonadaptive strategy with $v(\Omega) = 1$. When $|\psi\rangle$ is maximally entangled, $\{|\phi_k\rangle\}_{k=1}^{d}$ forms an orthogonal basis. Hence, Eq. (24) gives the optimal nonadaptive strategy.[9,21]

In practice, the above strategy can be easily implemented. Alice first randomly chooses one of the two measurements $\{|k\rangle\}_{k=1}^{d}$ and $\{|f_k\rangle\}_{k=1}^{d}$ with probabilities w and $1 - w$, respectively. The former measurement can be performed directly, while the latter one requires some random phase shifts from G in advance. Then Alice sends all the information to Bob via classical communication, upon receiving which Bob can proceed to perform the corresponding test.

Lastly, we consider the case of two-way adaptive verification. By the same token, the efficiency can be improved by averaging $\Omega^{\rightarrow}$ and its swap $\Omega^{\leftarrow}$. Specifically, we can get

$$v(\Omega^{\leftrightarrow}) = v\left[\frac{1}{2}(\Omega^{\rightarrow} + \Omega^{\leftarrow})\right] = \frac{1}{1 + \lambda^2}, \qquad (25)$$

when $\Omega^{\rightarrow}$ is of the form in Eq. (23) with $w = \lambda^2/(1 + \lambda^2)$ and $\lambda^2 = \frac{1}{2}(\lambda_1^2 + \lambda_2^2)$. However, unlike the two-qubit case, this strategy is only near-optimal for general bipartite states. To get the optimal strategy, we can numerically solve the optimization in Eq. (25), then explicitly decompose the obtained strategy with the method in ref. [22]. Our testing results show that the optimal strategy is at most 4% better in efficiency than the near-optimal strategy for all $d \leq 10$, whereas the measurement settings of the optimal strategies may involve complicated POVMs; instead the near-optimal strategies in Eq. (25) only involve PMs; see Supplementary Note C for more details.

Before concluding, two remarks are in order. First, Eqs. (22) and (25) imply that $v(\Omega) \geq 1/2$ for all of our adaptive strategies. This implies that $N \lesssim 2\varepsilon^{-1} \log \delta^{-1}$ copies of states are enough for verifying any bipartite states, which is independent of the dimension d. This is of the same scale with the best global strategies with entangled measurements, which need $N \approx \varepsilon^{-1} \log \delta^{-1}$ copies.[9] On the contrary, the best nonadaptive strategies known so far need $N \gtrsim d\varepsilon^{-1} \log \delta^{-1}$ to verify a generic two-qudit state for $d \geq 3$,[23] which is worse than our adaptive strategies by an order $O(d)$. Second, it is possible to further improve the efficiency of the adaptive strategies by involving many-round communication. However, these strategies require coherence-preserving measurements and can only improve the efficiency up to a constant factor c with $c \leq 2$ for all dimensions.

DISCUSSION

Quantum state verification is an efficient and reliable method for gaining confidence about the quality of quantum devices, which is a crucial step in almost all quantum information-processing tasks and foundational studies. In this work, we integrated adaptive measurements to the problem of state verification and formulated two convex optimization problems that completely characterize the optimal adaptive strategies for one-way and one-round two-way classical communication. We solve these optimization problems using both analytical and numerical methods, and the optimal or near-optimal strategies are constructed explicitly for any bipartite pure state. As a demonstration, we compared the optimal adaptive strategies with the nonadaptive one, and find that the verification efficiency can be significantly improved if classical communication is allowed. Finally, our adaptive verification strategies are readily applicable in experiments as only few local PMs are involved. For future research, it is very interesting to consider the multipartite case, which is more relevant for applications. Moreover, it is meaningful to discuss how the present approach needs to be modified, if the measurement devices are not perfectly characterized. Statistical tools developed for quantum state discrimination[24,25] may be helpful for this purpose.

Note added. During the preparation of the manuscript we became aware of related works by Wang and Hayashi[26] and Li et al.[27]

DATA AVAILABILITY

The data that support the results of this study are available from the corresponding authors upon request.

CODE AVAILABILITY

The codes that support the results of this study are available from the corresponding authors upon request.

REFERENCES

1. Paris, M. & Řeháček, J. (eds) *Quantum State Estimation*, Vol. 649 of *Lecture Notes in Physics* (Springer, Heidelberg, 2004).
2. Häffner, H. et al. Scalable multiparticle entanglement of trapped ions. *Nature* **438**, 643–646 (2005).
3. Shang, J., Zhang, Z. & Ng, H. K. Superfast maximum-likelihood reconstruction for quantum tomography. *Phys. Rev. A.* **95**, 062336 (2017).
4. Schwemmer, C. et al. Systematic errors in current quantum state tomography tools. *Phys. Rev. Lett.* **114**, 080403 (2015).
5. Tóth, G. & Gühne, O. Detecting genuine multipartite entanglement with two local measurements. *Phys. Rev. Lett.* **94**, 060501 (2005).
6. Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).
7. Flammia, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106**, 230501 (2011).
8. daSilva, M. P., Landon-Cardinal, O. & Poulin, D. Practical characterization of quantum devices without tomography. *Phys. Rev. Lett.* **107**, 210404 (2011).
9. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
10. Dimić, A. & Dakić, B. Single-copy entanglement detection. *npj Quantum Inf.* **4**, 11 (2018).
11. Morimae, T., Takeuchi, Y. & Hayashi, M. Verification of hypergraph states. *Phys. Rev. A.* **96**, 062321 (2017).
12. Takeuchi, Y. & Morimae, T. Verification of many-qubit states. *Phys. Rev. X.* **8**, 021060 (2018).
13. Zhu, H. & Hayashi, M. Efficient verification of hypergraph states. *Phys. Rev. Appl.* **12**, 054047 (2019).
14. Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Statist.* **23**, 493–507 (1952).
15. Hoeffding, W. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**, 13–30 (1963).
16. Bennett, C. H. et al. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725 (1996).
17. Watrous, J. *The Theory of Quantum Information.* (Cambridge University Press, Cambridge, UK, 2018).
18. Peres, A. *Quantum Theory: Concepts and Methods.* (Kluwer Academic Publishers, 2002).

19. Peres, A. Separability criterion for density matrices. *Phys. Rev. Lett.* **77**, 1413–1415 (1996).

20. Horodecki, M., Horodecki, P. & Horodecki, R. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A.* **223**, 1–8 (1996).

21. Zhu, H. & Hayashi, M. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A.* **99**, 052346 (2019).

22. Shang, J. & Gühne, O. Convex optimization over classes of multiparticle entanglement. *Phys. Rev. Lett.* **120**, 050506 (2018).

23. Liu, Y.-C., Yu, X.-D., Shang, J., Zhu, H. & Zhang, X. Efficient verification of Dicke states. *Phys. Rev. Appl.* **12**, 044020 (2019).

24. Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photonics* **1**, 238–278 (2009).

25. Bae, J. & Kwek, L.-C. Quantum state discrimination and its applications. *J. Phys. A: Math. Theor.* **48**, 083001 (2015).

26. Wang, K. & Hayashi, M. Optimal verification of two-qubit pure states. *Phys. Rev. A.* **100**, 032315 (2019).

27. Li, Z., Han, Y.-G. & Zhu, H. Efficient verification of bipartite pure states. *Phys. Rev. A.* **100**, 032316 (2019).

AUTHOR CONTRIBUTIONS

X.-D.Y. and J.S. did the theoretical analysis and performed the numerical simulations. O.G. supervised the project. All authors contributed to interpreting the results and writing the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information is available for this paper at https://doi.org/10.1038/s41534-019-0226-z.

Correspondence and requests for materials should be addressed to X.-D.Y., J.S. or O.G.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.