Quantum gate verification and its application in property testing

Pei Zeng [1], You Zhou [2,3,1,*] and Zhenhuan Liu [4,1]

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[2] *Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA*

[3] *CAS Centre for Excellence and Synergetic Innovation Centre in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

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

(Received 30 December 2019; accepted 20 May 2020; published 9 June 2020)

To guarantee the normal functioning of quantum devices in different scenarios, appropriate benchmarking tool kits are quite significant. Inspired by the recent progress on quantum state verification, here we establish a general framework of verifying a target unitary gate. In both the nonadversarial and adversarial scenarios, we provide efficient methods to evaluate the performance of verification strategies for any qudit unitary gate. Furthermore, we figure out the optimal strategy and its realization with the prepare-and-measurement setting. Specifically, for the commonly used quantum gates like single-qubit and qudit gates, multiqubit Clifford gates, and multiqubit generalized controlled-Z(X) gates, we provide efficient local verification protocols. Besides, we discuss the application of gate verification to the detection of entanglement-preserving property of quantum channels, and further quantify the robustness measure of them. We believe that the gate verification is a promising way to benchmark a large-scale quantum circuit as well as to test its property.

DOI: 10.1103/PhysRevResearch.2.023306

To build a large-scale and stable quantum system, efficient and robust benchmarking tools are essential [1]. The core aim of quantum benchmarking is to establish the correct functioning of a quantum device so that one can gain confidence in the final information processing results. A benchmarking process is usually composed of several elements: the unknown target devices, some trusted (or partially characterized) benchmarking devices, and a benchmarking protocol with classical data processing.

While quantum mechanics endows us a large Hilbert space for information processing, whose size increases exponentially with the increase of the qubit number, it also introduces a challenging problem of characterizing the devices in this space. In general, without any prior knowledge on the target device, it at the same time takes exponentially increasing resources to get the full tomographic image of it [2,3]. Fortunately, in most of the cases, one holds some prior knowledge on the possible structure of the target device. With the assistance of this prior knowledge, it is in principle feasible to reduce the benchmarking resources and even characterize the system efficiently with a polynomial number of trials. Some common benchmarking tool kits developed in this spirit and widely applied in experiments are quantum tomography based on compressed sensing [4,5], tensor-network-based quantum tomography [6–8], permutation-invariant quantum tomography [9–11], and direct fidelity estimation [12], ordered by less information gain or higher efficiency.

On the other hand, the correctness of the benchmarking results usually relies on some assumptions made on the benchmarking devices as well as the target devices. In practice, the quantum gate benchmarking protocols with fewer assumptions on the benchmarking devices have been proposed, such as gate-set tomography [13,14] and randomized benchmarking [15–17], which can in some sense eliminate the effect of the state preparation and measurement error. Meanwhile, in some quantum information tasks such as quantum key distribution [18,19] and blind quantum computation [20], the quantum objects might be produced by some adversarial party, which may be correlated among different trials. In these tasks, one should make possibly less or no assumption on the target devices. Currently, the protocol with the least device assumption both on benchmarking and target devices are the self-testing ones [21,22], which, however, are not efficient to extend to the multipartite systems in general. As a result, a robust benchmarking protocol against correlated noise is significant to explore for practical applications.

Recently, a highly efficient benchmarking protocol called quantum state verification has been introduced [23,24]. In the verification, one aims to know whether the prepared state ρ is close to the ideal pure state $|\psi\rangle$ in some precision ϵ for a given significance level δ. The verification is accomplished by a few rounds of two-outcome verification tests, which constitute the verification operator Ω. Conditioning on the pass of all the tests, one can lower bound the fidelity within a high precision. The efficiency of the verification is determined by the spectral gap of the operator Ω. Comparing to the direct fidelity estimation protocols [12], the verification protocol is shown to

*you_zhou@g.harvard.edu

achieve the same fidelity precision with a quadratically fewer number of trials.

Inspired by the quantum state verification studies [23–25], we propose a general framework of the quantum gate verification based on the prepare-and-measure strategies, where the verifier prepares local pure states, acts the target gates on them, and then performs projective measurements to verify the gates. The main idea is to reformulate the gate verification problem in the Choi representation. We remark that the gate verification problem cannot be simply regarded as the verification of the corresponding Choi states due to the extra locality and sequential limitation of the verification strategy and the restriction of the Choi states. We first introduce some background knowledge on the Choi representation and the gate fidelity in Sec. I. Then, we provide a general framework of quantum gate verification on both nonadversarial and adversarial scenarios in Sec. II. In the nonadversarial scenario, we express the efficiency of a given verification scheme with a semidefinite program and figure out the optimal strategy and its realizations. In the adversarial scenario, we formulate the efficiency of verification as an optimization problem and obtain the optimal strategy within a subset of the strategy. In Sec. III, we focus on some typical quantum gates and discuss their verification strategies. Especially, we show that any single-partite (qubit and qudit) gates and Clifford gates can be efficiently verified. In Sec. IV, we discuss the application of the gate verification in testing the properties of quantum channels, such as the robustness of quantum memory [26,27]. Finally, in Sec. V, we summarize our work, discuss the possible future direction, and compare it to recent related works.

I. PRELIMINARIES

In this section we first review some essential properties of quantum channels that are related to our discussion.

A. Choi state representation of quantum channels

For a quantum system A, denote its Hilbert space as $\mathcal{H}^A$. The set of linear operations on A is denoted as $\mathcal{L}(\mathcal{H}^A)$ and the set of quantum states as $\mathcal{D}(\mathcal{H}^A)$. Suppose the systems A and $\bar{A}$ own the same dimension and $\mathcal{B}_A = \{|j\rangle_A\}_{j=0}^{d-1}$, $\mathcal{B}_{\bar{A}} = \{|j\rangle_{\bar{A}}\}_{j=0}^{d-1}$ are two orthonormal bases of them. The maximally entangled state (with respect to $\mathcal{B}_A$ and $\mathcal{B}_{\bar{A}}$) on systems $A, \bar{A}$ is defined to be

$$|\Phi_+\rangle_{A\bar{A}} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle_{A\bar{A}}, \tag{1}$$

and we denote the density matrix $\Phi_+^{A\bar{A}} := |\Phi_+\rangle_{A\bar{A}} \langle\Phi_+|$ for simplicity.

A linear map $\mathcal{E}^{A\to B} : \mathcal{L}(\mathcal{H}^A) \to \mathcal{L}(\mathcal{H}^B)$ is a quantum channel if and only if (iff) it is a completely positive and trace-preserving (CPTP) map. Denote $\mathcal{I}_d$ the d-dimension identity map. On account of the state-channel duality, the (normalized) Choi state representation of a quantum linear map is defined to be

$$\Phi_{\mathcal{E}}^{AB} = (\mathcal{I}^{A\to A} \otimes \mathcal{E}^{\bar{A}\to B})(\Phi_+^{A\bar{A}}), \tag{2}$$

that is, the output state of the map $\mathcal{I}^{A\to A} \otimes \mathcal{E}^{\bar{A}\to B}$ with the maximally entangled state as the input state.

The linear map $\mathcal{E}^{A\to B}$ is completely positive iff $\Phi_{\mathcal{E}}^{AB}$ is positive semidefinite; $\mathcal{E}^{A\to B}$ is trace preserving iff $\mathrm{Tr}_B[\Phi_{\mathcal{E}}^{AB}] = \mathbb{I}_A/d_A$. In this work, we focus on the case when the output dimension d_B is the same as the input dimension d_A. We denote $d := d_A = d_B$. Meanwhile, we omit the superscript of $\mathcal{E}^{A\to B}$ standing for the system when no ambiguity occurs. Note that as the channel $\mathcal{E}$ being an unitary U, the Choi state is a maximally entangled (pure) state, and we denote the unitary channel as $\mathcal{U}(\cdot) = U \cdot U^\dagger$.

The Choi state encodes all the information of the corresponding quantum channel, and one can also obtain the output of the channel by the following relation:

$$\mathcal{E}(\rho) = d\,\mathrm{Tr}_A\big[\big(\rho_A^T \otimes \mathbb{I}_B\big)\Phi_{\mathcal{E}}^{AB}\big]. \tag{3}$$

The state-channel duality is essential to our work, which indicates that verifying the quantum channel is equivalent to verifying the Choi state. We show in Sec. II that many results in the state verification can be applied to the current study.

B. Average gate fidelity and entanglement fidelity

In this work, we focus on benchmarking the quantum gate, say a unitary U on the Hilbert space $\mathcal{H}_d$. Due to the unavoidable noise, the actual operation realized in an experiment may be a noisy channel $\mathcal{E}$. Here, we use the average gate fidelity to characterize the difference between the ideal unitary gate $\mathcal{U}$ and the noisy channel $\mathcal{E}$:

$$F_A(\mathcal{U}, \mathcal{E}) := \int d\psi\, \mathrm{Tr}[\mathcal{U}(\psi), \mathcal{E}(\psi)], \tag{4}$$

where the integration is over all the pure state under Haar measure. The average gate fidelity is widely used in the quantum gate benchmarking experiment.

For the corresponding Choi states, the entanglement fidelity is defined as

$$F_E(\mathcal{U}, \mathcal{E}) := \mathrm{Tr}(\Phi_{\mathcal{U}}\Phi_{\mathcal{E}}) = \langle\Phi_+|\,\Phi_\Lambda|\Phi_+\rangle. \tag{5}$$

Here, $\Lambda := \mathcal{U}^\dagger \circ \mathcal{E}$ is a composite channel. In fact, there is a direct relation between the average gate fidelity and the entanglement fidelity:

$$F_A(\mathcal{U}, \mathcal{E}) = \frac{dF_E(\mathcal{U}, \mathcal{E}) + 1}{d + 1}. \tag{6}$$

As a result, one can investigate the practical figure of merit $F_A(\mathcal{U}, \mathcal{E})$ with $F_E(\mathcal{U}, \mathcal{E})$, which is related to the following theoretical derivation. In in the following discussion, we simply use $F(\mathcal{U}, \mathcal{E}) := F_E(\mathcal{U}, \mathcal{E})$ to denote the entanglement fidelity. We also denote $r_E(\mathcal{U}, \mathcal{E}) := 1 - F_E(\mathcal{U}, \mathcal{E})$ as the entanglement infidelity, and call it infidelity without ambiguity.

II. GENERAL FRAMEWORK OF QUANTUM GATE VERIFICATION

In this section, we introduce a general framework of quantum gate verification. We first analyze the performance of verification strategies in nonadversarial scenario in Sec. II A. We then discuss the optimal verification protocol in Sec. II B, which can be realized in a quite experiment-friendly way.

After that, in Sec. II C we extend the verification task to the adversarial scenario, which can be useful in the quantum communication tasks with untrusted quantum channels.

A. Nonadversarial scenario

We start from the i.i.d. (identical and independent distribution) scenario, where a device named Eve is going to produce N rounds of the same quantum channel $\mathcal{E}$, which should be the unitary gate $\mathcal{U}$ in the ideal case. Similar as the state verification, as a user of the channel Alice would like to verify whether the underlying channel is close to the ideal unitary within some ϵ using N tests under some significance level δ.

On account of the state-channel duality introduced in Sec. I A, a natural method is to input maximally entangled state and verify the output Choi state directly. However, from a practical point of view, the verification with the maximally entangled state preparation is consumptive and also not robust to the state preparation error. Therefore, in the following discussion, we adopt the strategy that only employs single-partite input states and measurements without ancillaries, that is, in a prepare-and-measure manner.

During each round, Alice prepares a state ρ_l, lets it get through the channel $\mathcal{E}$, and measures it using two-outcome positive-operator-valued measurement (POVM) operators $\{E_l, \mathbb{1} - E_l\}$, with $0 \leqslant E_l \leqslant \mathbb{1}$. The state ρ_l and POVM element E_l satisfy

$$\mathrm{Tr}[\mathcal{U}(\rho_l)E_l] = 1. \tag{7}$$

We name the combination (ρ_l, E_l) satisfying Eq. (7) as a verification pair for $\mathcal{U}$.

In different rounds, Alice may adopt different verification pairs (ρ_l, E_l) for testing. Suppose she chooses the pairs with probability p_l. The verification pairs (ρ_l, E_l) as well as the probability p_l together compose a strategy $W := \{p_l, (\rho_l, E_l)\}_l$. The verification protocol is listed as follows:

(1) For each trial, Alice randomly chooses a verification pair (ρ_l, E_l) with probability p_l from the strategy W.

(2) Alice prepares state ρ_l, inputs it to the quantum channel $\mathcal{E}$ to be verified, measures the output state using POVM $\{E_l, \mathbb{1} - E_l\}$, and records the test outcome.

(3) Alice performs the above tests for N times. If all the tests pass, Alice estimates the average gate fidelity $F(\mathcal{E}, U) \geqslant 1 - \epsilon$ with a significance level δ.

On account of the state-channel duality in Eq. (3), Eq. (7) can be reformulated as

$$d\,\mathrm{Tr}\big[\big(\rho_l^T \otimes E_l\big)\Phi_{\mathcal{U}}\big] = 1, \tag{8}$$

and we define the verification operator being

$$\Omega := d\sum_l p_l\big(\rho_l^T \otimes E_l\big). \tag{9}$$

Note that, for the verification pair (ρ_l, E_l), there is an extra transposition in the corresponding operator term $\rho_l^T \otimes E_l$.

From this point of view, the verification scheme of a channel is (mathematically) closely related to the one of a maximally entangled state $\Phi_{\mathcal{U}}$ [25]. The operator Ω from the strategy W is denoted as the corresponding verification operator. However, there are still differences between the maximally entangled state verification and the gate verification:

(1) In the maximally entangled state verification, the possible noisy objects are bipartite states; while in the gate verification, the possible noisy objects are noisy quantum channels, which puts extra limitations on the Choi states compared with the bipartite states.

(2) In the gate verification, the state is prepared deterministically, and the measurement is decided according to the state preparation. Thus, one is restricted to the one-way LOCC strategy, comparing to the former bipartite state analysis [28–30].

Now, we study the performance of the verification protocol, which is usually characterized by the minimum number of trials $N(\epsilon, \delta, \Omega)$ for a given infidelity upper bound ϵ, significance level δ, and verification operator Ω. That is, if the verification succeeds in N rounds, one can confirm that the fidelity between the underlying noisy channel and the target unitary is larger than $1 - \epsilon$ with probability $1 - \delta$.

The minimum number of trials $N(\epsilon, \delta, \Omega)$ is directly related to the maximal passing probability $P(\epsilon, \Omega)$. For the noisy channel with entanglement infidelity $r_E(\mathcal{U}, \mathcal{E})$ not smaller than ϵ, the maximal passing probability (corresponding to the type-II error of hypothesis testing) is [23,24]

$$\begin{aligned} P(\epsilon, \Omega) &= \max_{r_E(\mathcal{U},\mathcal{E})\geqslant\epsilon} \mathrm{Tr}[\Omega\Phi_{\mathcal{E}}] \\ &\leqslant \max_{\mathrm{Tr}[\Phi_{\mathcal{U}}\rho]\leqslant 1-\epsilon} \mathrm{Tr}[\Omega\rho] = 1 - \nu(\Omega)\epsilon. \end{aligned} \tag{10}$$

Here, the first maximization is on all the possible channel $\mathcal{E}$, and the Choi state should satisfy an additional constraint $\mathrm{Tr}_B[\Phi_{\mathcal{E}}^{AB}] = \mathbb{I}_A/d_A$ compared with the quantum state verification. Thus, the followed inequality acts as a useful upper bound of the passing probability. Here, $\nu(\Omega) := 1 - \beta(\Omega)$ is the spectral gap of Ω, with $\beta(\Omega)$ being the second largest eigenvalue. Note that $P(\epsilon, \Omega)$ can be written as a semidefinite program

$$\begin{aligned} \max\quad & \mathrm{Tr}\big[\Omega\Phi_{\mathcal{E}}^{AB}\big] \\ \text{s.t.}\quad & \mathrm{Tr}\big[\Phi_{\mathcal{U}}^{AB}\Phi_{\mathcal{E}}^{AB}\big] \leqslant 1 - \epsilon, \\ & \mathrm{Tr}_B\big[\Phi_{\mathcal{E}}^{AB}\big] = \frac{\mathbb{I}_d}{d}, \\ & \Phi_{\mathcal{E}}^{AB} \geqslant 0. \end{aligned} \tag{11}$$

Given a verification operator Ω, under the condition of all the N test trials pass, for the significance level δ, i.e., $P(\epsilon, \Omega)^N \leqslant \delta$, the minimal number of the verification trials N is

$$\begin{aligned} N(\epsilon, \delta, \Omega) &= \left\lceil \frac{\ln \delta^{-1}}{\ln P(\epsilon, \Omega)^{-1}} \right\rceil \\ &\leqslant \left\lceil \frac{\ln \delta^{-1}}{\ln[1 - \nu(\Omega)\epsilon]^{-1}} \right\rceil \leqslant \left\lceil [\nu(\Omega)\epsilon]^{-1} \ln \delta^{-1} \right\rceil. \end{aligned} \tag{12}$$

Here, the first inequality is due to the upper bound in Eq. (10), which is generally not tight.

To reduce the trial number, one should minimize the passing probability in Eq. (10) for all possible verification

operator, that is,

$$P^{op}(\epsilon) = \min_{\Omega} P(\epsilon, \Omega) = \min_{\Omega} \max_{r_E(\mathcal{U},\mathcal{E})\geqslant\epsilon} \mathrm{Tr}(\Omega\Phi_{\mathcal{E}}), \tag{13}$$

where the operator Ω is from all verification strategies W given by Eq. (9). The optimal trial number is then $N^{op}(\epsilon,\delta) = \lceil \frac{\ln\delta^{-1}}{\ln P^{op}(\epsilon)^{-1}} \rceil$. In the following, we show some properties of $P(\epsilon,\Omega)$, which are helpful for its optimization in the next section.

Observation 1. The passing probability $P(\epsilon,\Omega)$ defined in Eq. (10) is a nondecreasing convex function on the verification operator Ω. That is, $P(\epsilon,\Omega') \geqslant P(\epsilon,\Omega)$ if $\Omega' - \Omega \geqslant 0$ is positive semidefinite, and

$$P(\epsilon,\Omega') \leqslant p_1 P(\Omega_1,\epsilon) + p_2 P(\Omega_2,\epsilon), \tag{14}$$

with $\Omega' = p_1\Omega_1 + p_2\Omega_2$, $p_1 + p_2 = 1$, $p_1, p_2 \geqslant 0$.

In practice, the noisy channels $\{\mathcal{E}_k\}$ during different trials may be different with each other. In this case, a well-defined estimation value would be the averaged infidelity over different rounds

$$\bar{r}(\mathcal{U},\{\mathcal{E}_k\}) = \frac{1}{N}\sum_{k=1}^{N} r(\mathcal{U},\mathcal{E}_k). \tag{15}$$

Similar to the discussion of the quantum state verification [31], with the same verification schemes W, one can actually bound the average infidelity $\bar{r}(\mathcal{U},\{\mathcal{E}_k\})$ using Eq. (12).

B. Optimal verification with pure state inputs and projective measurements

In this section, we provide the optimal verification of any unitary channel $\mathcal{U}$ under pure state inputs and project measurements (PVM), which is easier for the experiment realization. Suppose there is a verification strategy $W := \{p_l, (\rho_l, E_l)\}_l$ for the identity channel $\mathcal{I}$, then any unitary $\mathcal{U}$ can be verified with $W' := \{p_l, (\rho_l, \mathcal{U}(E_l))\}_l$. Consequently, without loss of generality we focus on the optimal verification of $\mathcal{I}$ in the following discussion.

To find the optimal verification of $\mathcal{I}$, we have the following two lemmas to convert an arbitrary verification operator Ω to the corresponding Bell-diagonal form without reducing its preformance.

Lemma 1. Under the unitary transformation $\mathcal{V}$, the verification strategy $W := \{p_l, (\rho_l, E_l)\}_l$ of the identity channel $\mathcal{I}$ becomes $W' := \{p_l, (\mathcal{V}(\rho_l), \mathcal{V}(E_l))\}_l$. The passing probability is invariant under the transformation

$$P(\epsilon,\Omega') = P(\epsilon,\Omega), \tag{16}$$

where the verification operators Ω and Ω' are from W and W', respectively, and

$$\Omega' = d\sum_l p_l (\mathcal{V}(\rho_l)^T \otimes \mathcal{V}(E_l)) = d\sum_l p_l \mathcal{V}^*(\rho_l^*)\otimes\mathcal{V}(E_l) = \mathcal{V}^*\otimes\mathcal{V}(\Omega). \tag{17}$$

Proof. First, note that $\mathrm{Tr}[\Omega'\Phi_+] = \mathrm{Tr}[\Omega[\mathcal{V}^*\otimes\mathcal{V}]^\dagger(\Phi_+)] = \mathrm{Tr}[\Omega\Phi_+] = 1$ with Φ_+ the Choi state of $\mathcal{I}$, thus can pass the verification also for Ω'. Suppose a state $\Phi_{\mathcal{E}}$ reaches the maximal value of $P(\epsilon,\Omega)$ according to Eq. (10), then one can find $\Phi'_{\mathcal{E}} = \mathcal{V}^*\otimes\mathcal{V}(\Phi_{\mathcal{E}})$ such that $\mathrm{Tr}[\Omega'\Phi'_{\mathcal{E}}] = \mathrm{Tr}[\Omega\Phi_{\mathcal{E}}]$. As a result, $P(\epsilon,\Omega') \geqslant P(\epsilon,\Omega)$. Since the unitary is reversible, similarly one can also get that $P(\epsilon,\Omega') \leqslant P(\epsilon,\Omega)$, and thus $P(\epsilon,\Omega') = P(\epsilon,\Omega)$. ■

Lemma 2. For a verification operator Ω of the identity channel $\mathcal{I}$, one can find the corresponding Bell-diagonal verification operator

$$\Omega' = \frac{1}{d^2}\sum_{u,v=0}^{d-1} \mathcal{W}^*(u,v)\otimes\mathcal{W}(u,v)(\Omega) = \sum_{u,v=0}^{d-1} \lambda_{u,v}\Phi_{u,v}, \tag{18}$$

where $\mathcal{W}(u,v)$ labeled by u, v are d^2 unitary channels of the Weyl operator introduced in Appendix A, such that the passing probability does not increase, i.e., $P(\epsilon,\Omega') \leqslant P(\epsilon,\Omega)$.

The proof of Lemma 2 is in Appendix B.

Theorem 1. For any unitary $\mathcal{U}$ on $\mathcal{H}_d$, one can construct the optimal verification strategy with pure state inputs and projective measurements. The optimal verification operator is

$$\Omega_{op} = \frac{\mathbb{I} + d\Phi_{\mathcal{U}}}{1+d} \tag{19}$$

and the optimal passing probability and trial number are

$$P^{op}(\epsilon) = 1 - \frac{d}{d+1}\epsilon,$$
$$N^{op}(\epsilon,\delta) = \left\lceil \frac{\ln\delta^{-1}}{\ln\left(1-\frac{d}{d+1}\epsilon\right)^{-1}} \right\rceil \leqslant \left\lceil \frac{d+1}{d\epsilon}\ln\delta^{-1} \right\rceil. \tag{20}$$

Proof. Without loss of generality, we consider the identity channel $\mathcal{I}$ here. Based on Lemma 2, to find the optimal verification one only needs to investigate Ω in the Bell-diagonal form. In this case, the channel verification and the state verification become coincident, that is, the first inequality in Eq. (10) is saturated. To be specific, the maximization of $\mathrm{Tr}[\Omega\rho] = \mathrm{Tr}[\Omega\rho_{\mathrm{diag}}]$ is equivalent for the Bell-diagonal states, which are legal Choi states.

At the same time, for the state verification, the optimal verification operator with separable measurements [25,32] is

$$\Omega_{op} = \frac{\mathbb{I} + d\Phi_+}{1+d}, \tag{21}$$

which is clearly Bell diagonal, thus can be reached by quantum channel verification. It is clear that the optimal gap here is $\nu(\Omega_{op}) = \frac{d}{d+1}$.

Now, we show that Ω_{op} can be constructed in a preparation and measurement manner. The optimal operator Ω_{op} can be realized by the so-called conjugate-basis (CB) projector of an orthogonal basis $\mathcal{B} = \{\psi_i\}_{i=0}^{d-1}$ in $\mathcal{H}_d$ [25]:

$$P(\mathcal{B}) = \sum_{\psi_i\in\mathcal{B}} \psi_i^*\otimes\psi_i. \tag{22}$$

That is, $\Omega_{op} = \frac{1}{d+1}\sum_{l=1}^{d+1} P(\mathcal{B}_l)$, when B_l are $d+1$ mutually unbiased bases (MUBs). We name the verification strategy $W = \{\frac{1}{d(d+1)}, (\psi_l^i, \psi_l^i)\}$ as the conjugate-basis (CB) test for

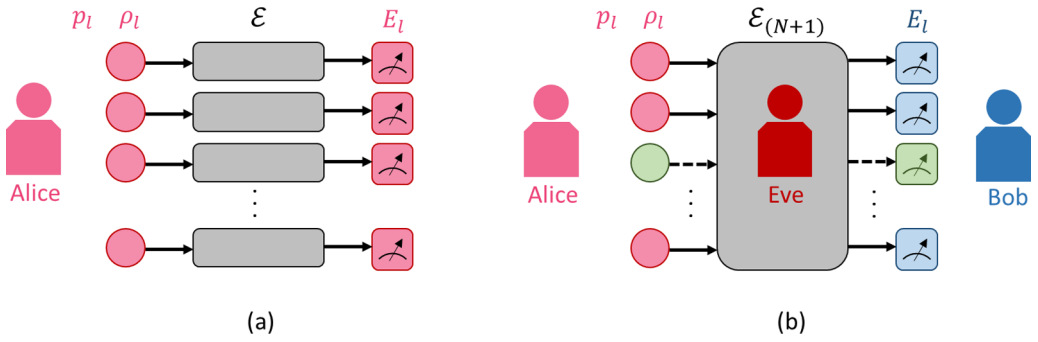

FIG. 1. The nonadversarial scenario and adversarial scenario. (a) In the nonadversarial scenario, Alice prepares the state ρ_l, sends it to an uncharacterized channel, and performs measurement E_l on it. The channels of different trials are independent with each other. (b) In the adversarial scenario with two communication parties, Alice prepares the state ρ_l, sends it to an untrusted channel, Bob then receives output states from the channel. After Alice announces the random test rounds, Bob performs measurement E_l on them and estimates the gate for the left turn (shown in green). The channels of different trials are correlated with each other.

prime power d, where ψ_l^i is chosen from $(d+1)$ MUB bases B_l.

If the dimension is not a prime power, the verification operator can be realized by $\Omega_{op} = \sum_\alpha \omega_\alpha \phi_\alpha^* \otimes \phi_\alpha$ and $\sum_\alpha \omega_\alpha = d$, with the weighted complex projective 2-design $\{\omega_\alpha, \phi_\alpha\}$ [25,33,34]. In this case, the CB test is defined to be a weighted verification strategy $W = \{\omega_\alpha/d, (\phi_\alpha, \phi_\alpha)\}$.

Finally, according to Eq. (3), the corresponding verification strategy of $\mathcal{I}$ shows $\{\frac{1}{d(d+1)}, (\psi_l^i, \psi_l^i)\}$, where ψ_l^i is from $(d+1)$ MUB B_l. That is, we input ψ_l^i and measure ψ_l^i with equal probability. For the unitary $\mathcal{U}$, the verification strategy is $\{\frac{1}{d(d+1)}, (\psi_l^i, \mathcal{U}(\psi_l^i))\}$. One can find the strategy of Ω constructed from 2-designs in a similar manner. ■

Practically, one may prefer to implement the verification with less MUBs because there are no enough MUBs in the Hilbert space or to reduce the experiment resources. The verification can be built with less MUBs, $\Omega = \frac{1}{g}\sum_{l=1}^{g} P(\mathcal{B}_l)$, and the spectral gap is $\nu(\Omega) = (g-1)/g$ [25]. According to Eq. (12), the trial number is upper bounded by

$$N(\epsilon, \delta) \leqslant \left\lceil \frac{\ln \delta^{-1}}{\ln\left(1 - \frac{g-1}{g}\epsilon\right)^{-1}} \right\rceil \leqslant \left\lceil \frac{g}{(g-1)\epsilon} \ln \delta^{-1} \right\rceil. \quad (23)$$

Note that the bound may be not tight, however, it is economical. For example, one can finish the verification with only two bases with the trial number only about two times overhead than the optimal one.

C. Adversarial scenario

In the discussion above, we suppose the implemented quantum gates are independent for different rounds. However, this may not be true in general. In some practical quantum information tasks, the quantum channels in different rounds will be correlated. For example, when Alice produces the uncharacterized gates with memory effect, the gate noise in the former rounds may affect the latter gate realization. On the other hand, in some quantum communication tasks, the quantum channels may be held by some untrusted parties Eve, e.g., entangled state distribution and quantum key distribution [19]. In this case, the adversarial Eve may be even more powerful so that she can take advantage of the correlations between different rounds [31]. Eve may produce a large composite quantum channel

$$\mathcal{E}_{(N+1)} : \mathcal{D}((\mathcal{H}^A)^{\otimes(N+1)}) \to \mathcal{D}((\mathcal{H}^B)^{\otimes(N+1)}) \quad (24)$$

with arbitrarily correlated noise. We will leave out the subscript $(N+1)$ in the later discussion in this section, i.e., $\mathcal{E} := \mathcal{E}_{(N+1)}$.

To verify the quantum channel in this case, we suppose Alice (and Bob) is able to randomly choose N rounds from the overall $(N+1)$ rounds to perform the verification test. She (they) leaves the remaining round to perform the real quantum information processing task. In Fig. 1(b), we describe the adversarial channel verification with two parties.

The possibility that the N rounds of tests pass is

$$p_{\mathcal{E}} = \mathrm{Tr}\left[(\Omega^{\otimes N} \otimes I)\Phi_{\mathcal{E}_{(N+1)}}\right], \quad (25)$$

where without loss of generality, we assume the test is on the first N qubits, and in the same time $\Phi_{\mathcal{E}_{(N+1)}}$ is permutation invariant. Conditioning on the passing of N rounds tests, Alice would like to confirm that the reduced $(N+1)$th round quantum channel given by the reduced Choi state

$$\Phi_{\mathcal{E}'} = p_{\mathcal{E}}^{-1}\mathrm{Tr}_{1\sim N}\left[(\Omega^{\otimes N} \otimes I)\Phi_{\mathcal{E}_{(N+1)}}\right] \quad (26)$$

is closed to the target unitary U. The entanglement fidelity between $\Phi_{\mathcal{E}'}$ and U is

$$\begin{aligned} F(\mathcal{E}', \mathcal{U}) &= \mathrm{Tr}(\Phi_{\mathcal{E}'}\Phi_{\mathcal{U}}) \\ &= p_{\mathcal{E}}^{-1}\mathrm{Tr}\left[(\Omega^{\otimes N} \otimes \Phi_{\mathcal{U}})\Phi_{\mathcal{E}_{(N+1)}}\right] = p_{\mathcal{E}}^{-1} f_{\mathcal{E}}, \end{aligned} \quad (27)$$

where

$$f_{\mathcal{E}} := \mathrm{Tr}\left[(\Omega^{\otimes N} \otimes \Phi_{\mathcal{U}})\Phi_{\mathcal{E}_{(N+1)}}\right]. \quad (28)$$

The core task in adversarial scenario is to verify whether the channel used for the task round is the target unitary channel $\mathcal{U}$. Similarly to the state verification discussion in Ref. [31], we define the estimated (entanglement) fidelity lower bound with respect to the number of test rounds N, a failure probability of δ, and the verification strategy Ω:

$$F(N, \delta, \Omega) := \min_{\Phi_{\mathcal{E}}} \left\{ p_{\mathcal{E}}^{-1} f_{\mathcal{E}} | p_{\mathcal{E}} \geqslant \delta \right\}, \quad 0 < \delta < 1 \quad (29)$$

where $\Phi_{\mathcal{E}}$ take values over all Choi states. The number of trials lower bound with respect to a precision of ϵ, a failure probability of δ, and the verification strategy Ω is defined to be

$$N(\epsilon, \delta, \Omega) := \min\{N | F(N, \delta, \Omega) \geqslant 1 - \epsilon\}. \tag{30}$$

For convenience of the later discussion, we also define the bipartite *state* verification parameters

$$\begin{aligned} F_S(N, \delta, \Omega) &:= \min_{\rho} \left\{ p_\rho^{-1} f_\rho \middle| p_\rho \geqslant \delta \right\}, \\ N_S(\epsilon, \delta, \Omega) &:= \min\{N | F_S(N, \delta, \Omega) \geqslant 1 - \epsilon\}. \end{aligned} \tag{31}$$

Here, the optimization is taken over all the $2(N+1)$-qudit $(\bigotimes_{i=1}^{N+1} \mathcal{H}_i)^{\otimes 2}$ bipartite state ρ, and p_ρ, f_ρ is defined by replacing $\Phi_{\mathcal{E}}$ in Eqs. (25) and (28) with ρ. It is obvious that $F(N, \delta, \Omega) \geqslant F_S(N, \delta, \Omega)$ and $N(\epsilon, \delta, \Omega) \leqslant N_S(\epsilon, \delta, \Omega)$. Therefore, the bipartite state verification parameters $F_S(N, \delta, \Omega)$ and $N_S(\epsilon, \delta, \Omega)$ are the lower bound and upper bound of $F(N, \delta, \Omega)$ and $N(\epsilon, \delta, \Omega)$, respectively. One can apply the analysis in Refs. [24,31] to estimate $N_S(\epsilon, \delta, \Omega)$ and $F_S(N, \delta, \Omega)$, which provides a useful bound for $N(\epsilon, \delta, \Omega)$ and $F(N, \delta, \Omega)$.

For a general strategy Ω, $F(N, \delta, \Omega)$ can be expressed as the following programming problem:

$$\begin{aligned} \min \quad & \mathrm{Tr}[(\Omega^{\otimes N} \otimes \Phi_{\mathcal{U}})\Phi_{\mathcal{E}}]/\mathrm{Tr}[(\Omega^{\otimes N} \otimes I)\Phi_{\mathcal{E}}] \\ \text{s.t.} \quad & \mathrm{Tr}[(\Omega^{\otimes N} \otimes I)\Phi_{\mathcal{E}}] \geqslant \delta, \\ & \mathrm{Tr}_B[\Phi_{\mathcal{E}}] = \left(\frac{\mathbb{I}_d}{d}\right)^{\otimes (N+1)}, \\ & \Phi_{\mathcal{E}} \geqslant 0, \end{aligned} \tag{32}$$

which is not easy to find an analytical solution in general.

In the following paragraphs, we show the method to find the optimal verification schemes as well as to analyze its performance. We first consider the verification operator in the Bell-diagonal form, and show that the figure of merits equal to the ones of the state. Then, we extend the analysis to a general type of verification operators which are called Bell supported, and show that they are always suboptimal to a homogeneous strategy. Finally, we solve the optimal homogeneous strategy and the performance of it.

Observation 2. For a verification strategy Ω of a quantum gate U which is bell diagonal under a local unitary transformation, i.e.,

$$\Omega = \sum_{u,v=0}^{d-1} \lambda_{u,v} \tilde{\Phi}_{u,v}^{AB}, \tag{33}$$

where $\{\tilde{\Phi}_{u,v}^{AB}\}$ are the qudit Bell states $\{\Phi_{u,v}^{AB}\}$ under local unitary transformation on systems A and B, and $\tilde{\Phi}_{0,0}^{AB} = \Phi_{\mathcal{U}}^{AB}$, $\lambda_{0,0} = 1$, we have

$$\begin{aligned} F(N, \delta, \Omega) &= F_S(N, \delta, \Omega), \\ N(\epsilon, \delta, \Omega) &= N_S(\epsilon, \delta, \Omega). \end{aligned} \tag{34}$$

Proof. We first simplify the expression of $F(N, \delta, \Omega)$. Due to the random assignment of test rounds, without loss of generality, we can restrict our discussion to the permutation-invariant states $\Phi_{\mathcal{E}}$. Similar to the discussion in Ref. [31], one can define the permutation-invariant Bell basis

$$\tilde{\Phi}_{\mathbf{k}} = \hat{\mathbf{P}}_S\left(\tilde{\Phi}_{0,0}^{\otimes k_{0,0}} \otimes \tilde{\Phi}_{0,1}^{\otimes k_{0,1}} \otimes \cdots \otimes \tilde{\Phi}_{d-1,d-1}^{\otimes k_{d-1,d-1}}\right), \tag{35}$$

where $\hat{\mathbf{P}}_S$ is the symmetrization operator, mixing all possible permutation with respect to different rounds, $\mathbf{k} := [k_{0,0}, k_{0,1}, \ldots, k_{d-1,d-1}]$ is a sequence of non-negative integer number with $\sum_{u,v} k_{u,v} = N + 1$.

Since $p_{\mathcal{E}}$ and $f_{\mathcal{E}}$ in Eqs. (25) and (28) only depend on the diagonal elements of $\Phi_{\mathcal{E}}$ in the Bell basis, without loss of generality, we may assume that the Choi state is diagonal in the product basis of $\tilde{\Phi}_{u,v}$. We only need to consider the Choi state $\Phi_{\mathcal{E}}$ as the mixture of $\tilde{\Phi}_{\mathbf{k}}$,

$$\Phi_{\mathcal{E}} = \sum_{\mathbf{k} \in \mathbf{K}} c_{\mathbf{k}} \tilde{\Phi}_{\mathbf{k}}, \tag{36}$$

where $\{c_{\mathbf{k}}\}$ are the non-negative mixing coefficients with $\sum_{k \in \mathbf{K}} c_{\mathbf{k}} = 1$, and $\mathbf{K}$ is the set of all possible $\mathbf{k}$. Note that the $\tilde{\Phi}_{u,v}$ basis naturally meets the requirements of Choi states, i.e., $\mathrm{Tr}_B[\Phi_{u,v}^{AB}] = I_d/d$. As a result, the optimization is over the whole convex hull made by $\{\Phi_{\mathbf{k}}\}$, similar to the state case in Ref. [31]. Therefore,

$$\begin{aligned} F(N, \delta, \Omega) &= \min_{\Phi_{\mathcal{E}}} \left\{ p_{\mathcal{E}}^{-1} f_{\mathcal{E}} | p_{\mathcal{E}} \geqslant \delta \right\} \\ &= \min_{\{c_{\mathbf{k}}\}} \left\{ p_{\mathcal{E}}^{-1} f_{\mathcal{E}} | p_{\mathcal{E}} \geqslant \delta \right\} \\ &= F_S(N, \delta, \Omega). \end{aligned} \tag{37}$$

■

A strategy Ω for unitary $\mathcal{U}$ with the form

$$\Omega = \Phi_{\mathcal{U}} + \lambda(1 - \Phi_{\mathcal{U}}) \quad (0 \leqslant \lambda < 1), \tag{38}$$

is called homogeneous. Note that the homogeneous strategy is a specific case of the Bell-diagonal strategies. The eigenvalues of such Ω except the largest one are all degenerated to be λ. It was shown in Ref. [31] that the following optimization of the quantum state verification

$$\max_{\Omega} F_S(N, \delta, \Omega) \tag{39}$$

can always be achieved by the homogeneous strategy for given N and δ.

Now, we discuss the optimal strategy Ω for the quantum gate verification and first introduce some notations. We call a strategy Ω *useless* under given N and δ if no Choi state $\Phi_{\mathcal{E}}$ meets the requirement

$$p_{\mathcal{E}} \geqslant \delta. \tag{40}$$

By spectrum decomposition, a strategy Ω can be written in the following unique form:

$$\Omega = \sum_{j=0}^{J-1} \lambda_j \Pi_j, \tag{41}$$

where $J < d$ is the number of different eigenvalues, $\lambda_0 = 1 > \lambda_1 > \cdots > \lambda_{J-1} \geqslant 0$, and Π_j is the projector onto the eigenspace with eigenvalue λ_j, whose rank may be larger than 1. If there exists a maximally entangled state Φ_e such that $\Phi_e \subseteq \Pi_j$, we call the Π_j space *Bell supported*. Denote the set of Bell-supported $\{\Pi_j\}$ of Ω as $\mathbf{S}(\Omega)$. Obviously, $\Pi_0 \subseteq \mathbf{S}(\Omega)$. If a strategy has Bell-supported projector set $\mathbf{S}(\Omega)$ with

at least one element other than Π_0, we call the strategy Ω Bell supported. The Bell-diagonal strategies are the extreme cases of Bell-supported strategies, where $\mathbf{S}(\Omega)$ span the whole operator space of Ω.

For the Bell-supported strategies, we have the following lemma.

Lemma 3. For a Bell-supported strategy Ω, denote a subset of $\mathbf{S}(\Omega)$ as $\mathbf{S}_0(\Omega) \subseteq \mathbf{S}(\Omega)$ which contains Π_0 and at least another element Π_j. Denote the set of eigenvalues corresponding to the projects in $\mathbf{S}_0(\Omega)$ as $\lambda(\mathbf{S}_0(\Omega))$. If we construct a new strategy Ω' with the form

$$\Omega' = \sum_{j|\Pi_j \in \mathbf{S}_0(\Omega)} \lambda_j \Pi_j + \sum_{j|\Pi_j \notin \mathbf{S}_0(\Omega)} \tilde{\lambda}_j \Pi_j, \tag{42}$$

where $\tilde{\lambda}_j$ can take any value in $\lambda(\mathbf{S}_0(\Omega))$ except for $\lambda_0 = 1$, then

$$F(N, \delta, \Omega') \geqslant F(N, \delta, \Omega) \tag{43}$$

if Ω' is not useless given N and δ.

Lemma 3 implies that, for the Bell-supported strategy Ω, one can always find a strategy with degenerated eigenvalue which is not worse than Ω. Therefore, for a given N and δ, and among all the Bell-supported strategies Ω, by applying the Lemma 3, one can see that the optimal strategy can always be achieved by homogeneous strategy. The proof of Lemma 3 is in Appendix C.

For the homogeneous strategy Ω, according to Observation 2, one can directly calculate $F_S(N, \delta, \Omega)$ and $N_S(\epsilon, \delta, \Omega)$. In the high-precision limit, i.e., $\epsilon, \delta \to 0$, the optimal homogeneous strategy to verify U is [25]

$$\Omega = \Phi_{\mathcal{U}} + \frac{1}{e}(1 - \Phi_{\mathcal{U}}). \tag{44}$$

To realize this, based on the optimal CB-test strategy introduced in Eq. (22) in Sec. II, one may add some "trivial test" into it. In the "trivial test," Alice and Bob perform no operation to realize the identity test. To realize the optimal homogeneous test in the high-precision limit, one may perform the trivial test with probability $p = \frac{d+1-e}{ed}$ and original optimal CB test with probability $1 - p$. In this case, the required number of trials is [25]

$$N(\epsilon, \delta, \lambda) = N_S(\epsilon, \delta, \lambda) \approx e\epsilon^{-1} \ln \delta^{-1}. \tag{45}$$

III. VERIFICATION OF SOME TYPICAL QUANTUM GATES

In the previous section, we introduce the general framework of the quantum gate verification. Especially, we show that any unitary channel $\mathcal{U}$ on $\mathcal{H}_d$ can be efficiently verified with pure state inputs and projective measurements, in both nonadversarial and adversarial scenarios. In this section, we apply such verification protocol to several typical quantum gates involved in quantum computing, such as any single-qubit gates, multiqubit Clifford gates, and beyond. Hereafter, we focus on the nonadversarial scenario.

A. Single-qubit gates

We first study the qubit identity channel $\mathcal{I}$, and latter directly extend it to any single-qubit gate $\mathcal{U}$ by some unitary transformation. The Choi state of $\mathcal{I}$ is Φ_+. According to Theorem 1, we can utilize 3 MUBs from the Pauli bases,

$$\begin{aligned} P_X &= \frac{X \otimes X + \mathbb{I}}{2} = |{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|, \\ P_Y &= \frac{-Y \otimes Y + \mathbb{I}}{2} = |{+}i - i\rangle\langle{+}i - i| + |{-}i + i\rangle\langle{-}i + i|, \\ P_Z &= \frac{Z \otimes Z + \mathbb{I}}{2} = |00\rangle\langle 00| + |11\rangle\langle 11|, \end{aligned} \tag{46}$$

which account for three subspaces, and $|\pm i\rangle$ denote the eigenstates of the Y basis. Note that these three projectors can also be derived from the stabilizer of the Choi state, which is helpful for the derivation of multiqubit gates. The verification operator is $\Omega = \frac{1}{3}(P_X + P_Y + P_Z)$ [23]. By Theorem 1, the qubit gate can be verified with optimal trial number $N^{op}(\epsilon, \delta) = \lceil \frac{\ln \delta^{-1}}{\ln(1-\frac{2}{3}\epsilon)^{-1}} \rceil \leqslant \lceil \frac{3}{2\epsilon} \ln \delta^{-1} \rceil$.

The corresponding verification strategy W for the identity qubit channel $\mathcal{I}$ is to choose the following verification pairs (ρ_l, E_l):

$$\begin{aligned} &(|+\rangle, |+\rangle),\ (|-\rangle, |-\rangle), \\ &(|+i\rangle, |+i\rangle),\ (|-i\rangle, |-i\rangle), \\ &(|0\rangle, |0\rangle),\ (|1\rangle, |1\rangle) \end{aligned} \tag{47}$$

with equal probability 1/6. For example, $(|+\rangle, |+\rangle)$ means that one inputs the $|+\rangle$ and performs measurement using POVM $\{|+\rangle\langle+|, \mathbb{I} - |+\rangle\langle+|\}$. If the measurement result is $|+\rangle\langle+|$, the test passes. For any single-qubit gate $\mathcal{U}$, verification pairs should be updated to $(\rho_l, \mathcal{U}(E_l))$. For example, for the Z gate the verification strategy is to choose

$$\begin{aligned} &(|+\rangle, |-\rangle),\ (|-\rangle, |+\rangle), \\ &(|+i\rangle, |-i\rangle),\ (|-i\rangle, |+i\rangle), \\ &(|0\rangle, |0\rangle),\ (|1\rangle, |1\rangle) \end{aligned} \tag{48}$$

with equal probability 1/6. In the same way, the non-Clifford T gate can also be verified. In addition, general qudit gates can be verified according to Sec. II B.

B. Clifford gates

In this and the next section, we consider the multiqubit gates, where the underlying Hilbert space is $\mathcal{H}_d = \mathcal{H}_2^{\otimes n}$. In this case, it is not easy to implement the optimal strategy given in Sec. II B since the input states and the measurements could be entangled ones. Thus, in the following we show how to verify the Clifford and $C^{n-1}Z(X)$ gates locally, inspired by the verification of stabilizer(like) states.

Let us first take the controlled-Z (CZ) gate as an example. The overall Choi state, shown in Fig. 2, is

$$|\Phi_{\mathrm{CZ}}\rangle = \tfrac{1}{2}\mathrm{CZ}_{3,4}(|00\rangle + |11\rangle)_{1,3} \otimes (|00\rangle + |11\rangle)_{2,4}. \tag{49}$$

Note that CZ gate operates on the final two qubits. The stabilizer generators of the initial Bell states are

$$g_1 = X_1X_3,\ g_2 = Z_1Z_3,\ g_3 = X_2X_4,\ g_4 = Z_2Z_4, \tag{50}$$

and the generators of the state $|\Phi_{\mathrm{CZ}}\rangle$ is updated to $g_i' = \mathcal{U}(g_i)$, where U is the corresponding gate (CZ here):

$$g_1' = X_1X_3Z_4,\ g_2' = Z_1Z_3,\ g_3' = X_2Z_3X_4,\ g_4' = Z_2Z_4, \tag{51}$$

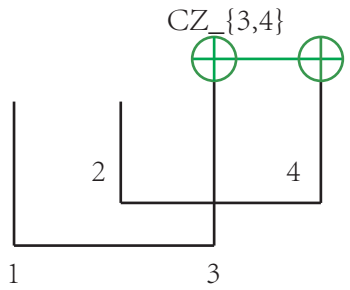

FIG. 2. The Choi state: CZ gate operates on the Bell pairs. The green (horizontal) line labels the CZ gate, and the black U-type line labels the Bell pair.

on account of the commuting relations,

$$\begin{aligned} \mathrm{CZ}_{i,j} X_{i(j)} \mathrm{CZ}_{i,j} &= X_i Z_j (Z_i X_j), \\ \mathrm{CZ}_{i,j} Z_{i(j)} \mathrm{CZ}_{i,j} &= Z_{i(j)}. \end{aligned} \tag{52}$$

To verify the Choi state, we can use the four stabilizer generators g_i' to construct the projection $P_i = \frac{g_i' + \mathbb{I}}{2}$, and the verification operator is $\Omega = \frac{1}{2n} \sum_i P_i$ (here $n = 2$) with the gap being $\nu(\Omega) = 1/2n$. In fact, one can utilize all the nontrivial $2^{2n} - 1$ stabilizers to enhance the gap to $2^{2n-1}/(2^{2n} - 1)$ [23,31], but may cost more state preparation and measurement settings. In some cases, the measurement settings can be reduced by the coloring of the corresponding graph states [35–37], which is equivalent to the stabilizer states under local Clifford gates [38]. For example, for the n-qubit Clifford circuit with only CZ gates operating between each two neighboring qubits, the corresponding Choi state is a two-color graph state. In this case, the verification involves two kinds of stabilizer configurations. We remark that, when there are CZ gates between two nonadjacent qubits, the Choi state may not be a two-color one.

Now, we translate the strategy expressed by verification operator Ω to the realization with verification pairs (ρ_l, E_l). For the projector P_i, the corresponding subspace is the $+1$ subspace of $g_i' = A_i \otimes B_i$, where A_i, B_i are two Pauli tensor operators. Thus, the verification strategy (ρ_l, E_l) is to input the eigenstate $|\psi_A\rangle$ in the $+1$ (-1) subspace and project the eigenstate to the $+1$ (-1) subspace of B_i. Since A_i, B_i are Pauli operators, the verification can be accomplished with inputting product pure states in the Pauli basis and Pauli measurements. For instance, the verification pairs of projector P_1 and P_2 are

$$\begin{aligned} &\{|+\rangle_1,\ (X_3Z_4)^+\},\ \{|-\rangle_1,\ (X_3Z_4)^-\}, \\ &\{|0\rangle_1,\ Z_3^+\},\ \{|1\rangle_1,\ Z_3^-\}, \end{aligned} \tag{53}$$

and the verification pairs for P_3 and P_4 are similar. To be specific, here $\{|+\rangle_1,\ (X_3Z_4)^+\}$ means that one inputs $|+\rangle$ on the first qubit ($\mathbb{I}/2$ on the second qubit), and performs measurement on the $+1$ basis of X_3Z_4. It is clear that $(X_3Z_4)^{\pm}$ can be finished by local X_3 and Z_4 measurements and classical postprocessings.

The above analysis can be generalized to the verification of any Clifford gates, and we summarize it in the following observation.

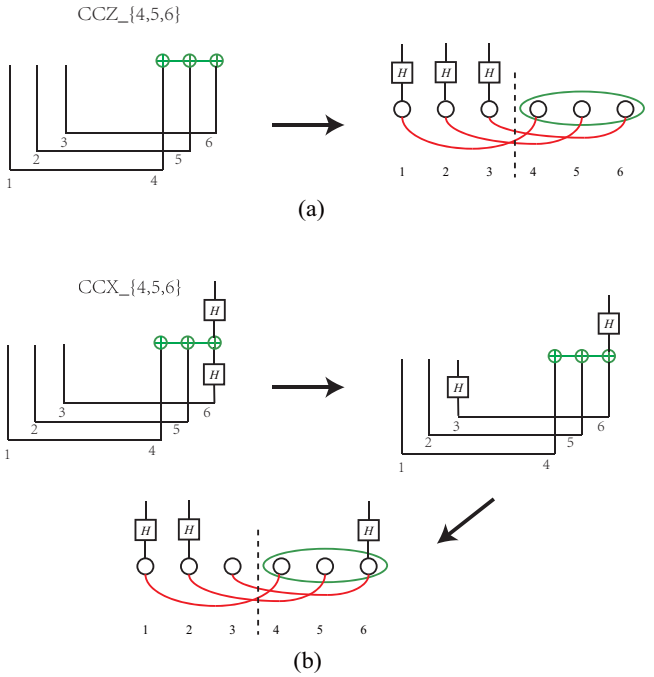

FIG. 3. The Choi state: CCZ gate operates on the Bell pairs. The green (horizontal) line labels the CCZ gate, and the black U-type line labels the Bell pair. Here, we transform the Choi states of $C^{n-1}Z$ and $C^{n-1}X$ to the hypergraph states $|\mathrm{HG}\rangle$ in (a) and (b), respectively. Here, the hypergraph state $|\mathrm{HG}\rangle$ owns three (red) normal edge and one (green) $n = 3$ hyperedge, and the graph is $n + 1 = 4$ colorable.

Observation 3. Any n-qubit Clifford gate can be verified under entanglement infidelity ϵ and significance level δ with verification trial number upper bounded by

$$N \leqslant \left\lceil \frac{2n}{\epsilon} \ln \delta^{-1} \right\rceil. \tag{54}$$

This bound can be further reduced with more input states and measurement settings,

$$N \leqslant \left\lceil \frac{2^{2n} - 1}{2^{2n-1}} \epsilon^{-1} \ln \delta^{-1} \right\rceil, \tag{55}$$

where the input states are in the Pauli basis and the measurements are local Pauli ones.

C. Multiqubit control-Z and control-X gates

In this section, we show the verification protocol of the $C^{n-1}Z$ and $C^{n-1}X$, where

$$C^{n-1}Z := \mathbb{I} - 2|00\ldots0\rangle\langle 00\ldots0|, \tag{56}$$

and $C^{n-1}X := H_n C^{n-1} X H_n$.

Similar as Sec. III B, we can find the updated "stabilizer" generators, however, now the stabilizers are not in the Pauli tensor form since the $C^{n-1}Z(X)$ gate is not a Clifford one. Because the $C^{n-1}Z$ gate can generate a hypergraph state [39], in the following we adopt the verification operator of a hypergraph state [36]. As shown in Fig. 3, the Choi state of the $C^{n-1}Z(X)$ state is equivalent to the hypergraph state under

local unitary, i.e., the single-qubit Hadamard gate,

$$|\Phi_{C^{n-1}Z}\rangle = \bigotimes_{i=1}^{n} H_i|\mathrm{HG}\rangle,$$
$$|\Phi_{C^{n-1}X}\rangle = \bigotimes_{i=1}^{n-1} H_i \otimes H_{2n}|\mathrm{HG}\rangle. \quad (57)$$

Here, the hypergraph state

$$|\mathrm{HG}\rangle = \bigotimes_{i=1}^{n} \mathrm{CZ}_{\{i,i+n\}} C^{n-1}Z_{\{n+1\to 2n\}}|+\rangle^{\otimes 2n} \quad (58)$$

with the $C^{n-1}Z$ gate operating on the final n qubits.

In this way, we can directly obtain the stabilizer generators of the Choi states from the ones of the hypergraph state. For example, for the $|\Phi_{C^{n-1}Z}\rangle$, the generator related to the fourth qubit is $g_4 = X_1X_4CZ_{5,6}$. It is not hard to see that the graph is $n+1$ colorable in Fig. 3. Thus, one can verify $|\Phi_{C^{n-1}Z}\rangle$ and $|\Phi_{C^{n-1}X}\rangle$ using verification operator constructed from the stabilizers with the spectral gap $1/(n+1)$ according to the cover protocol in [36]. In a similar way as in Sec. III B, we can transfer the state protocol to the verification strategy of the unitary gates, and the verification trial number is $N \leqslant \lceil \frac{n+1}{\epsilon} \ln \delta^{-1} \rceil$. Note that one can still use local state inputs and Pauli basis measurements since the $C^{n-1}Z$ operator on n qubit can be measured with the Z basis measurement $Z^{\otimes n}$ using postprocessing.

IV. APPLICATIONS IN CHANNEL PROPERTY TESTING

In this section, we show the application of the verification protocol to the efficient test on the property of the underlying quantum channel. Here, we focus on the entanglement property of quantum channels. We believe that the following analysis could be easily generalized to other properties, such as the coherence generating power [40,41].

The entanglement property refers to whether the underlying channel is an entanglement-preserving (EP) or the entanglement-breaking (EB) one. This kind of test is essential for quantum communications, such as the quantum memory and the quantum channel in quantum networks and distributed quantum computing. An EB channel can always be described by a measurement-and-preparation channel, thus destroys any quantum correlation between the initial input state and other possible parties. In the following sections, we first discuss the verification of the entanglement property of the channel and further quantifies this kind of quantumness with an estimation of a lower bound for the (generalized) robustness of the quantum memory [26,27].

A. Entanglement property detection

As a specific type of quantum channel, a good quantum memory can preserve the quantum information to some extent. In the ideal case, the quantum memory keeps all the information contained in the states and is reversible. The perfect memory is a known unitary $\mathcal{U}$, e.g., the identity channel $\mathcal{I}$. In the following discussion, we show that the verification protocol can help us reveal whether the noisy channel is EP. Without loss of generality, here we focus on the strategies to verify $\mathcal{I}$.

It is known that a channel is EP iff the corresponding Choi state is an entangled state. The Choi state $\Phi_{\mathcal{E}}$ is entangled if the fidelity to the maximally entangled state $\mathrm{Tr}(\Phi_{\mathcal{E}}\Phi_+) > 1/d$, that is, by the violation of the following witness:

$$\mathcal{W} := \frac{\mathbb{I}}{d} - \Phi_+, \quad (59)$$

where the expectation value $\langle \mathcal{W} \rangle \geqslant 0$ for all separable states [42].

As a result, the error threshold here is taken as $\epsilon = 1 - 1/d$. From Theorem 1, we know that the optimal verification round is

$$N^{op} = \left\lceil \frac{\ln \delta^{-1}}{\ln[1-\nu(\Omega_{op})\epsilon]^{-1}} \right\rceil = \left\lceil \frac{\ln \delta^{-1}}{\ln\left(\frac{d+1}{2}\right)} \right\rceil. \quad (60)$$

Thus, EP property can be verified in a single round if $d \geqslant 2\delta^{-1} - 1$. Moreover, suppose we consider the verification protocol just with two MUBs, which is the easiest to realize in the experiment, the corresponding verification round is

$$N^{2-\mathrm{MUB}} \leqslant \left\lceil \frac{\ln \delta^{-1}}{\ln\left(1-\frac{d-1}{2d}\right)^{-1}} \right\rceil = \left\lceil \frac{\ln \delta^{-1}}{\ln\left(\frac{2d}{d+1}\right)} \right\rceil. \quad (61)$$

Thus, we can use two measurement settings, for example, X and Z base states and measurements to detect the entanglement property of the quantum channel.

B. Quantumness quantification

In this section, we further apply the verification to the quantification of quantumness. Specifically, an operational measure called the robustness of the quantum memory can be lower bounded with the verification protocol.

We first introduce the robustness of entanglement [43]

$$\mathcal{R}^s(\rho) := \min_{\sigma\in\mathcal{S}} \left\{ t \geqslant 0,\ \frac{\rho + t\sigma}{1+t} \in \mathcal{S} \right\}, \quad (62)$$

where $\mathcal{S}$ is the set of separable states. $\mathcal{R}^s(\rho)$ quantifies how much separable noise needs to be introduced to make the state separable. If one allows the noisy state σ to be any state, the definition becomes the generalized robustness $\mathcal{R}^s_G(\rho)$. By definition, $\mathcal{R}^s_G(\rho) \leqslant \mathcal{R}^s(\rho)$.

In a similar way, the robustness of quantum channel is defined as [26,27]

$$\mathcal{R}(\mathcal{E}) := \min_{\mathcal{M}\in\mathcal{F}} \left\{ t \geqslant 0,\ \frac{\mathcal{E} + t\mathcal{M}}{1+t} \in \mathcal{F} \right\}, \quad (63)$$

where $\mathcal{F}$ is the set of EB channels. If one allows the mixed channel $\mathcal{M}$ to be any channel, the definition becomes the generalized robustness $\mathcal{R}_G(\mathcal{E})$. By definition, $\mathcal{R}_G(\mathcal{E}) \leqslant \mathcal{R}(\mathcal{E})$. The (generalized) robustness measure of quantum channel owns a few of significant operational meaning, such as the amount of classical simulation cost and the advantage in state discrimination-based quantum games.

Observation 4.

$$\mathcal{R}^s(\Phi_\mathcal{E}) \leqslant \mathcal{R}(\mathcal{E}),\ \mathcal{R}^s_G(\Phi_\mathcal{E}) \leqslant \mathcal{R}_G(\mathcal{E}), \tag{64}$$

where $\Phi_\mathcal{E}$ is the Choi state of the quantum channel $\mathcal{E}$.

Proof. Here, we prove the first inequality, and the second can be proved in the same way. If we write Eq. (63) in the Choi state form, we can see that the noisy Choi state $\Phi_\mathcal{M}$ is not only a separable state, but also under the additional constraint maximally mixed on the first subsystem. However, the minimization of $\mathcal{R}^s(\Phi_\mathcal{E})$ does not need this constraint, thus serves as a lower bound. ■

From Observation 4, one has $\mathcal{R}^s_G(\Phi_\mathcal{E}) \leqslant \mathcal{R}_G(\mathcal{E}) \leqslant \mathcal{R}(\mathcal{E})$. Thus we can give a reliable lower bound of the robustness of quantum channel by estimating the corresponding measure on the Choi state. From Ref. [44], the generalized robustness of entanglement on states can be lower bounded by the witness as

$$R^s_G(\rho) \geqslant \frac{|\mathrm{Tr}(\mathcal{W}\rho)|}{\lambda_{\max}}, \tag{65}$$

where the expectation value of the witness should satisfy $\mathrm{Tr}(\mathcal{W}\rho) \leqslant 0$ and $\lambda_{\max}$ is the largest eigenvalue of the witness operator $\mathcal{W}$. Inserting the witness in Eq. (59), we have

$$R^s_G(\Phi_\mathcal{E}) \geqslant d\,\mathrm{Tr}(\Phi_\mathcal{E}\Phi_+) - 1. \tag{66}$$

As a result, to confirm $\mathcal{R}(\mathcal{E}) \geqslant r$, the entanglement infidelity should satisfy $\epsilon \leqslant \frac{d-r-1}{d}$. And we have the trial number of the optimal strategy given by

$$N^{op} = \left\lceil \frac{\ln \delta^{-1}}{\ln[1-\nu(\Omega_{op})\epsilon]^{-1}} \right\rceil = \left\lceil \frac{\ln \delta^{-1}}{\ln\left(\frac{d+1}{r+2}\right)} \right\rceil. \tag{67}$$

Note as $r = 0$, Eq. (67) becomes the result in Eq. (60) of the verification of entanglement. We can further reduce the measurement efforts by using less MUBs.

V. CONCLUSION AND OUTLOOK

In this work, we studied the verification of quantum gates. Based on the Choi representation of quantum channels, we analyze the verification strategies with local state inputs and local measurements without the assistance of extra ancillaries.

In the nonadversarial scenario, the verification performance characterized by the type-II error probability $P(\epsilon, \Omega)$ can be calculated by a semidefinite program. On account of the unitary invariance and convexity of the passing probability with respect to Ω, one can prove the optimality of a uniformly mixing strategy Ω_{op} in Eq. (19), which can be realized by a CB test with $(d+1)$ MUB when d is a prime power or other mixing strategy based on quantum state 2-design. Moreover, we show that the performance of all the Bell-diagonal strategies can be exactly evaluated.

In the adversarial scenario, the verification performance characterized by the entanglement fidelity lower bound $F(N, \delta, \Omega)$ and number of trials upper bound $N(\epsilon, \delta, \Omega)$ are in general hard to solve, while the corresponding state parameters $F_S(N, \delta, \Omega)$ and $N_S(\epsilon, \delta, \Omega)$ can provide a useful bound. We prove that, for the Bell-diagonal strategies with the form in Eq. (33), the calculation of $F(N, \delta, \Omega)$ and $N(\epsilon, \delta, \Omega)$ can be reduced to its corresponding state version $F_S(N, \delta, \Omega)$ and $N_S(\epsilon, \delta, \Omega)$. Meanwhile, we prove that, among all the Bell-supported strategies Ω defined in Sec. II C, for given trial rounds N and significant level δ, the optimal $F(N, \delta, \Omega)$ can always be achieved by the homogeneous strategies.

More specifically, we analyze the local verification strategies and their performance for some common quantum gates, such as single-qubit and qudit gates, multiqubit Clifford gates, and multiqubit controlled-Z and controlled-X gates. We also demonstrate the application of gate verification for channels' property testing. We show that gate verification can be used to test the entanglement-preserving property and further the quantification of the robustness of quantum memory.

To enhance the robustness of our work against state preparation and measurement error, we may consider the combination of channel verification with common robust methods, such as randomized benchmarking [15,17], robust tomographic information extraction [45], and gate set tomography [14]. On the other hand, it is important to make the gate verification protocol robust against a few rounds of failure tests [46].

To characterize the quantumness in a channel is currently a hot topic [26,27,47–51]. Here, we analyze the application of gate verification to quantify the robustness of quantum memory [26,27]. We believe that our method can be extended to quantify other properties of the channel, such as the coherence-generating power [40,41], magic [52], and so on.

Note added. Recently, we noticed two recent related works [53,54]. Comparing to Ref. [53], we analytically derive the optimal verification strategy for the general d-level unitary. Reference [54] develops a very general framework for the quantum gate verification with local state inputs and local measurements, which is suitable for quite a few gates, especially for the multipartite ones. Here, we focus on the preparation and measurement strategies and directly relate them to the channel's Choi representation. As a result, our performance (by the number of trials) on the multiqubit Clifford gate in Eq. (55), $N \leqslant \lceil \frac{2^{2n}-1}{2^{2n-1}}\epsilon^{-1}\ln\delta^{-1}\rceil$, is better than the one in Ref. [54], $N \leqslant \lceil 3\epsilon^{-1}\ln\delta^{-1}\rceil$. Moreover, we also consider the quantum gate verification in the adversarial scenario and its application in channel property testing.

ACKNOWLEDGMENTS

We thank X. Ma and X. Yuan for the helpful discussion on the quantumness of channels and the semidefinite programming. Y. Zhou was supported in part by the Templeton Religion Trust under Grant TRT No. 0159 and by the ARO under Contract No. W911NF1910302. This work was supported by the National Natural Science Foundation of China Grants No. 11875173 and No. 11674193, the National Key R&D Program of China Grants No. 2017YFA0303900 and No. 2017YFA0304004, and the Zhongguancun Haihua Institute for Frontier Information Technology.

APPENDIX A: HEISENBERG-WEYL OPERATORS AND GENERALIZED QUDIT BELL STATES

The Heisenberg-Weyl group is a generalization of Pauli group. For a qudit Hilbert space with computational basis

$\{|l\rangle\}_{l=0}^{d-1}$, we define

$$Z = \sum_{l=0}^{d-1} \exp\left(i\frac{2\pi}{d}l\right)|l\rangle\langle l|, \qquad X = \sum_{l=0}^{d-1} |l+1\rangle\langle l|, \tag{A1}$$

where $|l+1\rangle$ means $|(l+1) \bmod d\rangle$.

The Heisenberg-Weyl operator $W(u,v)$ is defined to be

$$W(u,v) = X^u Z^v, \tag{A2}$$

with $u, v = 0, 1, \ldots, d-1$. It is easy to verify that

$$X^d = Z^d = \mathbb{I}, \quad (X^u)^\dagger = X^{-u}, \quad (Z^v)^\dagger = Z^{-v},$$
$$X^u Z^v = \exp\left(-i\frac{2\pi}{d}uv\right) Z^v X^u,$$
$$W(u,v)W(u',v') = \exp\left(-i\frac{2\pi}{d}(uv' - vu')\right) \times W(u',v')W(u,v). \tag{A3}$$

Define $|\Phi_{0,0}\rangle = |\Phi_+\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jj\rangle$. The generalized qudit Bell states [55] are

$$|\Phi_{u,v}\rangle := \mathbb{I}\otimes W(u,v)|\Phi_+\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\exp\left(\frac{2\pi i}{d}lv\right)|l\rangle_A \otimes |l+u\rangle_B. \tag{A4}$$

Denote $\Phi_{u,v} := |\Phi_{u,v}\rangle\langle\Phi_{u,v}|$. The qudit Bell states $\{\Phi_{u,v}\}_{u,v=0}^{d-1}$ form an orthonomal basis

$$\begin{aligned}\langle\Phi_{u,v}|\Phi_{u',v'}\rangle &= \langle\Phi_+|(\mathbb{I}\otimes W(u,v)^\dagger W(u',v'))|\Phi_+\rangle \\ &= \exp\left(-i\frac{2\pi}{d}u_d v\right)\langle\Phi_+|(\mathbb{I}\otimes X^{u_d}Z^{v_d})|\Phi_+\rangle \\ &= \frac{1}{d}\exp\left(-i\frac{2\pi}{d}u_d v\right)\sum_{j=0}^{d-1}\sum_{m,l=0}^{d-1}\exp\left(i\frac{2\pi}{d}v_d l\right) \\ &\quad\times \langle j,j|m,l+u_d\rangle\langle m,l|j,j\rangle \\ &= \frac{1}{d}\delta_{u_d,0}\exp\left(-i\frac{2\pi}{d}u_d v\right)\sum_{j=0}^{d-1}\exp\left(i\frac{2\pi}{d}v_d j\right) \\ &= \delta_{u_d,0}\delta_{v_d,0},\end{aligned} \tag{A5}$$

where $u_d := u' - u$, $v_d := v' - v$.

APPENDIX B: PROOF OF LEMMA 2

Proof. The summation in Eq. (18) is a"twirling" operation on the Weyl operators, and we first prove that the twirling result is in the Bell-diagonal form. To prove this, we take out an operator element $|\Phi_{w_1}\rangle\langle\Phi_{w_2}|$ in the Bell basis with the vector $w_i = (u_i, v_i)$ and $|\Phi_{w_i}\rangle = \mathbb{I}\otimes W_i|\Phi_+\rangle$, and show that it vanishes after the twirling unless $w_1 = w_2$. For simplicity, we denote the phase factor as $a = \exp(-i\frac{2\pi}{d})$ and the symplectic inner product as $\{w, w'\} = uv' - vu'$:

$$\begin{aligned}&\sum_w \mathcal{W}^*(u,v)\otimes\mathcal{W}(u,v)(|\Phi_{w_1}\rangle\langle\Phi_{w_2}|) \\ &= \sum_w (W^*\otimes W)(|\Phi_{w_1}\rangle\langle\Phi_{w_2}|)(W^T\otimes W^\dagger) \\ &= \sum_w (W^*\otimes W)(\mathbb{I}\otimes W_1)|\Phi_+\rangle\langle\Phi_+|(\mathbb{I}\otimes W_2^\dagger)(W^T\otimes W^\dagger) \\ &= \sum_w a^{\{w,w_1\}}a^{-\{w,w_2\}}(\mathbb{I}\otimes W_1)(W^*\otimes W)|\Phi_+\rangle \\ &\quad\times\langle\Phi_+|(W^T\otimes W^\dagger)(\mathbb{I}\otimes W_2^\dagger) \\ &= \sum_w a^{\{w,w_1-w_2\}}(\mathbb{I}\otimes W_1)|\Phi_+\rangle\langle\Phi_+|(\mathbb{I}\otimes W_2^\dagger) \\ &= \sum_w a^{(w,w_1-w_2)}|\Phi_{w_1}\rangle\langle\Phi_{w_2}| \\ &= \sum_{u,v} e^{-i\frac{2\pi}{d}(u\Delta v' - v\Delta u')}|\Phi_{w_1}\rangle\langle\Phi_{w_2}| \\ &= \delta_{w_1-w_2}|\Phi_{w_1}\rangle\langle\Phi_{w_2}|,\end{aligned} \tag{B1}$$

where $(\Delta u', \Delta v') = (u_1 - u_2, v_1 - v_2) = w_1 - w_2$, and $\delta_{w_1-w_2} = 1$ iff $w_1 = w_2$. Here, Eq. (A3) is applied to show the third equality; the fourth equality is due to the invariance of the maximally entangled state $|\Phi_+\rangle$ under the operation $W^*\otimes W$.

Then, we prove the nonincreasing of the passing probability $P(\epsilon,\Omega)$. Note that the twirling operation is a mixing of d^2 verification operators $\Omega_{\{u,v\}} = \mathcal{W}^*(u,v)\otimes\mathcal{W}(u,v)(\Omega)$ with equal probability $\Omega' = 1/d^2\sum\Omega_{\{u,v\}}$. Thus, combining Observation 1 and Lemma 1, one has $P(\epsilon,\Omega') \leqslant 1/d^2\sum P(\epsilon,\Omega_{\{u,v\}}) = P(\epsilon,\Omega)$. ∎

APPENDIX C: PROOF OF LEMMA 3

Proof. For the strategy Ω, we take a group of eigenvectors $\{\Psi_{j,l}\}$ corresponding to different eigenvalues $\{\lambda_j\}$. If the rank of Π_j is larger than 1, then l denotes the index in the degenerated space. We set $\Psi_{j,0}$ to be (one of) the Bell state in Π_j if $\Pi_j\in\mathbf{S}_0(\Omega)$. Obviously, $\{\Psi_{j,l}\}$ are also the eigenvectors of Ω'. We denote the set of maximally entangled basis in it as $\Theta(\Psi_{j,l})$.

Similar to the argument in the proof of Observation 2, we now introduce the permutation-invariant basis

$$\Psi_{\mathbf{k}} = \hat{\mathbf{P}}_S\left(\bigotimes_{j,l}\Psi_{j,l}^{\otimes k_{j,l}}\right), \tag{C1}$$

where $\hat{\mathbf{P}}_S$ is the symmetrization operator, mixing all possible permutation with respect to different rounds, $k := [k_{0,0}, k_{0,1}, \ldots, k_{J-1,L-1}]$ is a sequence of non-negative integer number with $\sum_{j,l}k_{j,l} = N+1$. If k is nonzero only on the set $\Theta(\Psi_{j,l})$, the generated symmetric state $\Psi_{\mathbf{k}}$ will also be the maximally entangled state. We denote the set of such $\Psi_{\mathbf{k}}$ as the symmetric Bell basis $\Theta_{\mathbf{S}}(\Psi_{j,l}, N)$.

Since $p_{\mathcal{E}}$ and $f_{\mathcal{E}}$ in Eqs. (25) and (28) only depend on the diagonal elements of $\Phi_{\mathcal{E}}$ in the basis of Ω, without loss of generality, we may assume that the Choi state is diagonal in

the product basis of $\{\Psi_{j,l}\}$. We only need to consider the Choi state $\Phi_{\mathcal{E}}$ as the mixture of $\Psi_{\mathbf{k}}$,

$$\Phi_{\mathcal{E}}(\mathbf{c}) = \sum_{\mathbf{k}\in\mathbf{K}} c_{\mathbf{k}} \Psi_{\mathbf{k}}, \tag{C2}$$

where $\mathbf{c} = \{c_{\mathbf{k}}\}$ are the non-negative mixing coefficients with $\sum_{\mathbf{k}\in\mathbf{K}} c_{\mathbf{k}} = 1$, and $\mathbf{K}$ is the set of all possible $\mathbf{k}$. Since $\Psi_{\mathbf{k}}$ might not meet the requirement of Choi state, there is extra limitation on the coefficients:

$$\mathrm{Tr}_B[\Phi_{\mathcal{E}}(\mathbf{c})] = \left(\frac{\mathbb{I}_d}{d}\right)^{\otimes(N+1)}. \tag{C3}$$

We denote the set of legal coefficients $\mathbf{c}$ satisfying Eq. (C3) as $\mathbf{C}(\Psi_{\mathbf{k}})$, which is determined by $\{\Psi_{\mathbf{k}}\}$. Note that, due to the linearity of Eq. (C3), $\mathbf{C}(\Psi_{\mathbf{k}})$ is a convex set.

According to Eqs. (25), (28), (C1), and (C2), one has

$$\begin{aligned} p_{\mathcal{E}}(\mathbf{c}) &= \sum_{\mathbf{k}\in\mathbf{K}} c_{\mathbf{k}} \eta_{\mathbf{k}}(\vec{\lambda}), \quad \mathbf{c} \in \mathbf{C}(\Psi_{\mathbf{k}}) \\ f_{\mathcal{E}}(\mathbf{c}) &= \sum_{\mathbf{k}\in\mathbf{K}} c_{\mathbf{k}} \zeta_{\mathbf{k}}(\vec{\lambda}), \quad \mathbf{c} \in \mathbf{C}(\Psi_{\mathbf{k}}) \end{aligned} \tag{C4}$$

where $\vec{\lambda} := (\lambda_{0,0}, \lambda_{0,1}, \ldots, \lambda_{J-1,L-1})$ is the eigenvalue of Ω or Ω', and

$$\begin{aligned} \eta_{\mathbf{k}}(\vec{\lambda}) := p(\mathbf{k}) &= \sum_{i|k_i>0} \frac{k_i}{(N+1)} \lambda_i^{k_i-1} \prod_{j\neq i|k_j>0} \lambda_j^{k_j}, \\ \zeta_{\mathbf{k}}(\vec{\lambda}) := f(\mathbf{k}) &= \frac{k_0}{(N+1)} \prod_{i|k_i>0} \lambda_i^{k_i}. \end{aligned} \tag{C5}$$

Here, λ_i^0 is set to be 1, even if $\lambda_i = 0$. Due to the degeneration of $\{\lambda_{j,l}\}$, for different $\mathbf{k}$, the values of $\eta_{\mathbf{k}}(\vec{\lambda})$ and $\zeta_{\mathbf{k}}(\vec{\lambda})$ could be the same. The optimization value of $F(N, \delta, \Omega)$ is determined by the two-dimensional region of $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ with legal $\mathbf{c} \in \mathbf{C}(\Psi_{\mathbf{k}})$.

Our main idea to prove $F(N, \delta, \Omega') \geqslant F(N, \delta, \Omega)$ to show that the optimizing area of Ω' belongs to the optimizing area of Ω, that is, the point $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ by coefficients $\mathbf{c}$ with Ω' can always be achieved by the same coefficients $\mathbf{c}$ with Ω. First, for the strategy Ω', all the value of $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ with $\mathbf{c} \in \mathbf{C}(\Psi_{\mathbf{k}})$ can be achieved even if we restrict our consideration to the symmetric Bell basis $\Psi_{\mathbf{k}} \in \Theta_{\mathbf{S}}(\Psi_{j,l}, N)$. Since the symmetric Bell basis terms $\{\Psi_{\mathbf{k}}\}$ naturally satisfy Eq. (C3), the Bell coefficients $\{c_{\mathbf{k}}\}$ can then be chosen freely, without any extra requirements than non-negative and normalization. On the other hand, due to the degeneracy of eigenvalues, i.e., $\tilde{\lambda}_j \in \lambda(\mathbf{S}_0(\Omega))$, all the values of $\eta_{\mathbf{k}}(\vec{\lambda})$ and $\zeta_{\mathbf{k}}(\vec{\lambda})$ can be realized by the symmetric Bell basis set $\Theta_{\mathbf{S}}(\Psi_{j,l}, N)$. Second, if we consider a symmetric Bell state $\Phi_{\mathcal{E}}(\mathbf{c})$ with coefficients $\mathbf{c} = \{c_{\mathbf{k}}\}$, the corresponding values of $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ are the same for Ω' and Ω. This is because the values of $\eta_{\mathbf{k}}(\vec{\lambda})$ and $\zeta_{\mathbf{k}}(\vec{\lambda})$ for the symmetric Bell basis are independent of Ω and Ω'. Third, the feasible coefficients region $\mathbf{C}(\Psi_{\mathbf{k}})$ for Ω and Ω' are the same since the region only depends on the eigenbasis $\{\Psi_{\mathbf{k}}\}$.

To summarize, for any point $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ in the optimization space of Ω', it can be achieved by the a state $\Phi_{\mathcal{E}}(\mathbf{c})$ on the space of the symmetric Bell basis $\Psi_{\mathbf{k}} \in \Theta_{\mathbf{S}}(\Psi_{j,l}, N)$. The value of $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ is the same for such symmetric Bell state $\Phi_{\mathcal{E}}(\mathbf{c})$ using the strategy Ω. Therefore, any point $(p_{\mathcal{E}}(\mathbf{c}), f_{\mathcal{E}}(\mathbf{c}))$ in the optimization space of Ω' will be contained in the optimization space of Ω. ■

[1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, arXiv:1910.06343.

[2] M. Paris and J. E. Rehacek, *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649 (Springer Science & Business Media, Berlin, Heidelberg, 2007), p. 7.

[3] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).

[4] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Phys. Rev. Lett. **105**, 150401 (2010).

[5] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, New J. Phys. **14**, 095022 (2012).

[6] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. **1**, 149 (2010).

[7] T. Baumgratz, D. Gross, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **111**, 020401 (2013).

[8] B. Lanyon, C. Maier, M. Holzäpfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. Buyskikh, A. Daley, M. Cramer *et al.*, Nat. Phys. **13**, 1158 (2017).

[9] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, and H. Weinfurter, Phys. Rev. Lett. **105**, 250403 (2010).

[10] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggebaum, S. Gaile, O. Gühne, and H. Weinfurter, New J. Phys. **14**, 105001 (2012).

[11] Y. Zhou, C. Guo, and X. Ma, Phys. Rev. A **99**, 052324 (2019).

[12] S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett. **106**, 230501 (2011).

[13] S. T. Merkel, J. M. Gambetta, J. A. Smolin, S. Poletto, A. D. Córcoles, B. R. Johnson, C. A. Ryan, and M. Steffen, Phys. Rev. A **87**, 062119 (2013).

[14] R. Blume-Kohout, J. K. Gamble, E. Nielsen, J. Mizrahi, J. D. Sterk, and P. Maunz, arXiv:1310.4492.

[15] J. Emerson, R. Alicki, and K. Życzkowski, J. Opt. B: Quantum Semiclassical Opt. **7**, S347 (2005).

[16] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[17] E. Magesan, J. M. Gambetta, and J. Emerson, Phys. Rev. Lett. **106**, 180504 (2011).

[18] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[19] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[20] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2009), pp. 517–526.

[21] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[22] I. Šupić and J. Bowles, arXiv:1904.10042.

[23] S. Pallister, N. Linden, and A. Montanaro, Phys. Rev. Lett. **120**, 170502 (2018).

[24] H. Zhu and M. Hayashi, Phys. Rev. Lett. **123**, 260504 (2019).
[25] H. Zhu and M. Hayashi, Phys. Rev. A **99**, 052346 (2019).
[26] Z.-W. Liu and A. Winter, arXiv:1904.04201.
[27] X. Yuan, Y. Liu, Q. Zhao, B. Regula, J. Thompson, and M. Gu, arXiv:1907.02521.
[28] K. Wang and M. Hayashi, Phys. Rev. A **100**, 032315 (2019).
[29] Z. Li, Y.-G. Han, and H. Zhu, Phys. Rev. A **100**, 032316 (2019).
[30] X.-D. Yu, J. Shang, and O. Guhne, npj Quantum Inf. **5**, 112 (2019).
[31] H. Zhu and M. Hayashi, Phys. Rev. A **100**, 062335 (2019).
[32] M. Hayashi, K. Matsumoto, and Y. Tsuda, J. Phys. A: Math. Gen. **39**, 14427 (2006).
[33] G. ZAUNER, Int. J. Quantum. Inf. **09**, 445 (2011).
[34] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
[35] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).
[36] H. Zhu and M. Hayashi, Phys. Rev. Appl. **12**, 054047 (2019).
[37] Y. Zhou, Q. Zhao, X. Yuan, and X. Ma, npj Quantum Inf. **5**, 83 (2019).
[38] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, arXiv:quant-ph/0602096.
[39] M. Rossi, M. Huber, D. BruB, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).
[40] A. Mani and V. Karimipour, Phys. Rev. A **92**, 032331 (2015).
[41] M. G. Díaz, K. Fang, X. Wang, M. Rosati, M. Skotiniotis, J. Calsamiglia, and A. Winter, Quantum **2**, 100 (2018).
[42] O. Guhne and G. Toth, Phys. Rep. **474**, 1 (2009).
[43] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).
[44] J. Eisert, F. G. Brandao, and K. M. Audenaert, New J. Phys. **9**, 46 (2007).
[45] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, Phys. Rev. X **4**, 011050 (2014).
[46] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, npj Quantum Inf. **5**, 27 (2019).
[47] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).
[48] X. Yuan, Phys. Rev. A **99**, 032317 (2019).
[49] G. Gour and M. M. Wilde, arXiv:1808.06980 [quant-ph].
[50] G. Gour, IEEE Trans. Inf. Theory **65**, 5880 (2019).
[51] Y. Liu and X. Yuan, Phys. Rev. Res. **2**, 012035 (2020).
[52] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, New J. Phys. **16**, 013009 (2014).
[53] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, Phys. Rev. A **101**, 042315 (2020).
[54] H. Zhu and H. Zhang, Phys. Rev. A **101**, 042316 (2020).
[55] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).