Statistical Methods for Quantum State Verification and Fidelity Estimation

Xiao-Dong Yu, Jiangwei Shang,* and Otfried Gühne**

The efficient and reliable certification of quantum states is essential for various quantum information processing tasks as well as for the general progress on the implementation of quantum technologies. In the last few years several methods have been introduced which use advanced statistical methods to certify quantum states in a resource-efficient manner. In this article, a review of the recent progress in this field is presented. How the verification and fidelity estimation of a quantum state can be discussed in the language of hypothesis testing is explained first. Then, various strategies for the verification of entangled states with local measurements or measurements assisted by local operations and classical communication are explained in detail. Finally, several extensions of the problem, such as the certification of quantum channels and the verification of entanglement are discussed.

1. Introduction

A basic yet important step in quantum information processing is the efficient and reliable characterization of quantum states. This is not only important in certain information processing protocols, such as quantum teleportation,[1] quantum cryptography,[2–7] and measurement-based quantum computation,[8,9] where the state emitted by a source needs to be characterized. The problem of state certification arises also frequently in the technological design and analysis of quantum devices, where the occurring quantum states need to be identified in an efficient manner.

Originally, a standard approach is to perform quantum state tomography by fully reconstructing the density matrix.[10–12] Tomography, however, is known to be both time consuming and computationally hard due to the exponentially increasing number of parameters to be determined.[13,14] Furthermore, in order to reconstruct a valid density matrix from experimental data, approximations like the maximum-likelihood estimation or Bayesian techniques have to be used,[12,15,16] which require additional effort and may lead to problematic effects.[17]

In fact, full tomographic information is often not required, thus a lot of effort has been devoted to characterizing quantum states or processes with non-tomographic methods.[18–22] For instance, in many experiments the fidelity of the prepared quantum state with respect to some target state is used as a benchmarking parameter.[23–25] Consequently, various methods for the fidelity estimation and the determination of confidence intervals have been derived.[26–28]

In the last few years, the research on quantum state verification (QSV) has made enormous progress by using advanced statistical methods and the framework of hypothesis testing.[29–31] This not only leads to unambiguous statements on experimental data, but also results in efficient methods which require only few copies of the quantum state under investigation. The archetypical situation is depicted in **Figure 1**. A source is promised to emit some state $|\psi\rangle$. In practice, the device produces a sequence of independent states $\sigma_1, \sigma_2, \ldots, \sigma_N$. How can we decide whether $\sigma_k = |\psi\rangle\langle\psi|$ or not? What are the optimal measurement strategies for this task, especially if not all measurements are available due to physical constraints such as locality? Interestingly, for many cases these questions can be answered, and the answers are relevant also for experimental situations which are not as clean as the scenario depicted in Figure 1.

In this article we review the recent developments on quantum state verification. Our aim is to provide the reader first with a basic and pedagogical introduction into the concepts of hypothesis testing and state verification. Then, we explain the results for different scenarios in detail. These detailed protocols naturally depend on the state one wishes to verify, but also on the allowed measurement protocols, for example, the extent to which communication between the parties is allowed.

We are aware of the fact that statistical tools have found widespread applications in quantum information processing and

X.-D. Yu, O. Gühne
Naturwissenschaftlich-Technische Fakultät
Universität Siegen
Walter-Flex-Str. 3, D-57068 Siegen, Germany
E-mail: xiao-dong.yu@uni-siegen.de; otfried.guehne@uni-siegen.de

X.-D. Yu
Department of Physics
Shandong University
Jinan 250100, China

J. Shang
Key Laboratory of Advanced Optoelectronic Quantum Architecture and Measurement of Ministry of Education
School of Physics
Beijing Institute of Technology
Beijing 100081, China
E-mail: jiangwei.shang@bit.edu.cn

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202100126

DOI: 10.1002/qute.202100126

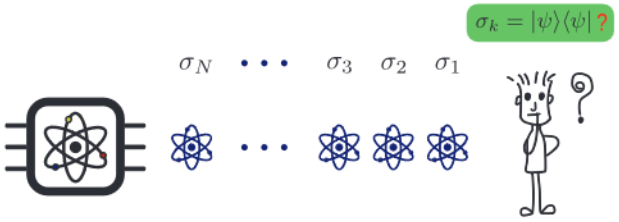


Figure 1. Schematic view on quantum state verification. One considers a quantum device which is promised to produce a specific target state $|\psi\rangle$, but in practice, the device produces a sequence of independent states $\sigma_1, \sigma_2, \ldots, \sigma_N$. The quantum state verification protocol studies how one can verify whether $\sigma_k = |\psi\rangle\langle\psi|$ or not in the language of hypothesis testing.

our article can cover only a small aspect of that. There are already excellent review articles on quantum state discrimination[32,33] and, very recently, on entanglement tests using witnesses from a statistical perspective.[34] Furthermore, we encourage the reader to consult the original literature on related topics, such as the estimation of pure or mixed quantum states,[35–38] the estimation of drift or change point detection,[39–41] sequential hypothesis testing,[42–44] the blind channel estimation,[45] and the estimation of quantum teleportation.[46,47] In addition, this review focuses on the problem of state verification in discrete-variable quantum systems. For their counterparts, continuous-variable quantum systems, the verification stands as a related but independent problem; see refs. [48, 49] for recent progresses.

This article is organized as follows. In Section 2 we give an introduction to the underlying concepts. We first explain the framework of hypothesis testing and then explain the basic scenario of quantum state verification and fidelity estimation. In Section 3 we discuss in detail the different scenarios. On the one hand, these are characterized by the pure bipartite or multipartite entangled state that should be verified. On the other hand, one can distinguish different types of available measurements and types of communication that are allowed. In Section 4 we discuss generalizations of quantum state verification, such as the verification of quantum channels and the implementation of entanglement tests based on few copies of a state. Finally, we conclude and point out some interesting questions for further investigation.

2. Preliminaries and Concepts

Before presenting the various results on QSV, we need to introduce the required concepts. First, we discuss the notion of hypothesis testing in some detail. Then, we can formalize the task of QSV as the main topic of this review. Finally, we discuss the problem of estimating the fidelity with a certain target state. Formulated as a statistical test, this task is different from QSV, but similar from a physical point of view on aims at characterizing the same physical quantity. Hence, methods known from fidelity estimation can frequently be applied to QSV.

2.1. Hypothesis Testing

Let us start by introducing the notion of hypothesis testing, which is a method used for making statistical decisions using experimental data.[50] Here, we focus on the Neyman–Pearson framework for testing hypotheses.[51] To illustrate the idea, we consider the following classical example. Suppose that we have a coin, which is either a fair coin with $P(\text{head}) = 1/2$ or a biased coin with $P(\text{head}) = 3/4$. Now, we want to decide whether the coin is fair or biased. To do this, we toss the coin 100 times. Suppose that we obtain more than 70 times of heads, then a natural guess is that the coin is biased. The main reason for this intuition is that if the coin were fair, then it would be very unlikely to observe the described data. Indeed, one can directly calculate that for a fair coin the probability of observing more than 70 times of heads from 100 tosses is $p \approx 1.61 \times 10^{-5}$, while for the biased coin it is $p \approx 0.850$, which makes this conclusion appealing.

For the general case, however, one needs a precise framework for such conclusions, and the notion of hypothesis testing is such a tool, giving answers on how to make a decision and how reliable the decision is. In this framework, the above statements that the coin is fair or biased correspond to two hypotheses. Then, how to make the decision based on the number of heads appeared corresponds to the decision rule. Finally, there are different types of errors that can be made, and these errors need to be quantified. Formally, the Neyman–Pearson framework consists of the following components:

1) Hypotheses: One has two hypotheses, namely the
   i) Null hypothesis H_0, for example, the hypothesis that the coin is fair.
   ii) Alternative hypothesis H_1, for example, the hypothesis of a specific unfair coin.
2) Decision rule: This is a rule based on the observed data to either
   i) Reject H_0. In the given example, one may use the rule to reject H_0 if say, more than 60% of the observed coin tosses give "heads".
   ii) Accept H_0. Correspondingly, one accepts the assumption of a fair coin if the fraction of "heads" is not larger than 60%, but also other rules are conceivable.
3) Errors: For the given decision rule two errors are relevant:
   i) Type I error: This is the probability of rejecting H_0 when H_0 is true, that is $P(\text{type I error}) = P(\text{reject } H_0 \mid H_0)$. For the example given above this error is $P_I \approx 1.76\%$, if the coin is tossed 100 times.
   ii) Type II error: This is the probability of accepting H_0 when H_1 is true, $P(\text{type II error}) = P(\text{accept } H_0 \mid H_1)$. For the example given above this is $P_{II} \approx 0.07\%$, if the coin is tossed 100 times.

In this framework the hypotheses are non-symmetric: one is singled out as the null hypothesis, denoted by H_0 and the other as the alternative hypothesis, denoted by H_1. Usually, H_0 is chosen as the hypothesis that one wants to disprove from the experimental data. Statistically, it may happen that one makes wrong conclusions on the accepting or rejecting, which are then characterized by the type I/II errors. The type I error is usually called the significance level of the hypothesis testing. In practice, some typical values, such as 5% or 1%, are widely used in various scientific fields.

Next, we explain the above notions with a discrimination task in quantum information processing, which is similar to the

previous example of coins, but already closely related to QSV. Suppose that we have a quantum device which is promised to always produce the same state, but it is unknown whether this state is the basis state $|0\rangle$ or the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

Now, one wishes to verify that the device is indeed producing the superposition state $|+\rangle$ instead of the basis state $|0\rangle$. The following procedure can be applied. First, let the null hypothesis be that the device produces the state $\rho_0 = |0\rangle\langle 0|$, and the alternative hypothesis be that the device produces the state $\rho_1 = |+\rangle\langle +|$. Second, let the device produce N copies of the state ρ, and performs a measurement

$$\mathcal{M} = \{\Omega, \mathbb{1} - \Omega\} \tag{1}$$

with two outcomes on each copy. Here, Ω is a positive semidefinite operator corresponding to one of the two possible measurement results. In order to discriminate the hypotheses, Ω needs to satisfy that the probabilities of the outcomes for $|0\rangle$ and $|+\rangle$ are different, that is, $p_0 = \langle 0|\Omega|0\rangle \neq p_1 := \langle +|\Omega|+\rangle$. Without loss of generality, we can assume that $p_0 < p_1$.

Then, let T denote the number of times where the result corresponding to Ω occurs out of the N measurements. A decision rule can be defined by

$$\begin{cases} \text{reject } H_0 & \text{if } T \geq t_0 \\ \text{accept } H_0 & \text{if } T < t_0 \end{cases} \tag{2}$$

Here t_0 is a constant that is specified before the experiment by the desired significance level α, as one wishes to have

$$P\left(T \geq t_0 \,\middle|\, H_0\right) \leq \alpha \tag{3}$$

In this way, one can design a test for the described device. The main task is then, of course, to design the measurement operator Ω, in such a way that the desired significance level can be reached with few copies N.

In practice, the significance level is often not fixed from the beginning. Instead, one characterizes the significance with the so-called p-value

$$\delta_t := P\left(T \geq t \,\middle|\, H_0\right) \tag{4}$$

Note that the difference between t_0 in Equation (3) and t in Equation (4) is that t_0 is a predefined value that is determined before the experiment, but t is the observed result of the actual experiment. The value $1 - \delta_t$ is usually called the confidence of the hypothesis testing. If one finds a t such that $\delta_t \leq \alpha$, then the null hypothesis is rejected.

Note that calculation of the p-value as in Equation (4) is closely connected to the so-called large deviation bounds. In these bounds one has a given probability distribution, here specified by the hypothesis H_0, and one aims to bound the probability to find a certain deviation from the mean value, if a statistical experiment is repeated N times. The archetypical bound of this type is the Hoeffding inequality,[52] which states the following. Consider N independent (but not necessarily identically distributed) random variables $X_i \in [a_i, b_i]$ with a mean value $\langle X_i\rangle$. In a statistical experiment, one may observe their sample mean, $X = (\sum_{i=1}^{N} X_i)/N$. Then, the probability that this sample mean deviates from the overall mean value $\langle X\rangle = (\sum_{i=1}^{N}\langle X_i\rangle)/N$ is bounded by

$$P\left(X - \langle X\rangle \geq \varepsilon\right) \leq \mathrm{e}^{-\frac{2\varepsilon^2 N^2}{\sum_{i=1}^{N}(b_i - a_i)^2}} \tag{5}$$

Various similar bounds exist, such as the Bernstein, Cantelli, or McDiarmid inequalities[53–55] and have been frequently used to analyze quantum experiments from a statistical point of view.[17,26,56–60]

In this article we are mainly interested in the case that the p-value is small enough to reject the null hypothesis. Thus, we will not distinguish the notions of (the probability of) the type I error, the significance level, or the p-value, unless otherwise stated. The type II error defined as

$$\beta := P\left(T < t_0 \,\middle|\, H_1\right) \tag{6}$$

characterizes the power of the hypothesis testing, that is, the smaller the type II error is the less likely that one makes a false acceptance.

Going back to the previous example on quantum state discrimination, we may choose $\Omega = |+\rangle\langle +|$ and $t_0 = N$, resulting in $p_0 = 1/2$ and $p_1 = 1$. Then the decision rule will be that we accept the null hypothesis $\rho_0 = |0\rangle\langle 0|$ unless $t = N$ and the type II error of the hypothesis is always zero. In the case that $t = N$, the null hypothesis $\rho_0 = |0\rangle\langle 0|$ is rejected in favor of the alternative hypothesis $\rho_1 = |+\rangle\langle +|$ with confidence

$$1 - \delta = 1 - \left(\langle 0|\Omega|0\rangle\right)^N = 1 - \frac{1}{2^N} \tag{7}$$

where $\delta = 1/2^N$ is the p-value. We note that the p-value measures how unlikely the given data are if H_0 is true. It is neither the probability that H_0 is false nor the probability that H_1 is true.

2.2. The Basic Task of Quantum State Verification

With the knowledge of hypothesis testing, we can describe the model for QSV by Pallister et al.[29] This is one basic model of QSV, but one should also refer to the pioneering works by Hayashi et al.[30,31] using slightly different assumptions.

Suppose that we have a quantum device which is promised to produce a specific target state $|\psi\rangle$, for instance the entangled singlet state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. In practice, the device produces a sequence of independent states $\sigma_1, \sigma_2, \ldots, \sigma_N$. The QSV protocol studies how one can verify whether $\sigma_k = |\psi\rangle\langle\psi|$ in the language of hypothesis testing; see Figure 1. To this end, we choose the alternative hypothesis as

$$H_1 : \ \sigma_k \in S := \{|\psi\rangle\langle\psi|\} \text{ for all } k \tag{8}$$

A first simple, but naive, choice of the null hypothesis could be $\sigma_k \in S^c = \{\rho \mid \rho \neq |\psi\rangle\langle\psi|\}$, where S^c denotes the complement of S. This, however, is not a good choice, because for any $\rho \in S$ there exists a $\tilde{\rho} \in S^c$ such that $\tilde{\rho}$ can be arbitrarily close to ρ. As a result,

it is impossible to reject the null hypothesis with a strictly positive confidence.

Thus, instead of choosing S^c as the null hypothesis, we choose the set of states that is ϵ-away from the target state $|\psi\rangle$, that is,

$$H_0 : \ \sigma_k \in S_\epsilon := \left\{ \rho \ \middle| \ \langle\psi|\rho|\psi\rangle \leq 1-\epsilon \right\} \text{ for all } k. \tag{9}$$

If this hypothesis H_0 is rejected, this implies that at least some of the states σ_k are close to the target state $|\psi\rangle$.

The basic QSV protocol from ref. [29] considers the idealized scenario where either H_0 is true or H_1 is true. This may sound unrealistic, but this idealized model is more convenient for theoretical studies. Moreover, the results can be directly generalized to the practically relevant estimation of fidelities described in the next subsection. We also note that in the QSV protocol, the states σ_k generated by the device are only assumed to be independent, but not necessarily to be identical, that is, arbitrary fluctuation of σ_k is allowed as long as $\sigma_{1,2,\ldots,N} = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_N$. This is relevant, as in realistic scenarios there may be some drift in the source, leading to a systematic change of the states σ_k with time. The generalization of the QSV protocols to non-independent sources, the so-called adversarial scenario, will be discussed in Section 4.

Due to the trade-off between type I and type II errors, different figures of merit for a hypothesis testing can be chosen depending on different physical or mathematical considerations. In QSV, the type II error is usually constrained to be zero, which means if the quantum device indeed produces the desired state $|\psi\rangle$, then it will always pass the test. This assumption is, however, not necessary. We will talk about possible generalizations in Section 4.

Then, it finally remains to discuss the measurements that shall be performed. In general, for each state σ_k, the verifier may apply a measurement, $\{\Omega_\ell, \mathbb{1} - \Omega_\ell\}$ randomly chosen from some set with probability p_ℓ. For instance, if the singlet state $|\psi^-\rangle$ shall be verified, he/she may perform spin measurements in correlated, but arbitrary directions, in order to observe the anti-correlations which are characteristic of the singlet state.

Thus, any QSV strategy can be expressed as an overall measurement

$$\Omega = \sum_{\ell=1}^{m} p_\ell \Omega_\ell \tag{10}$$

where $(p_1, p_2, \ldots, p_m)$ is a probability distribution, and $\{\Omega_\ell, \mathbb{1} - \Omega_\ell\}$ are allowed measurements with outcomes labeled by "pass" and "fail", respectively. An essential insight in the following discussion is that often only the properties of Ω are relevant, but not the specific forms of $\{p_\ell, \Omega_\ell\}$.

To guarantee that the type II error is zero, that is, that the target state $|\psi\rangle$ never fails the test, all Ω_ℓ are required to satisfy that

$$\langle\psi|\Omega_\ell|\psi\rangle = 1 \ \Leftrightarrow \ \Omega_\ell|\psi\rangle = |\psi\rangle \tag{11}$$

where the equivalence follows from the fact that the measurement effect Ω_ℓ cannot have eigenvalues larger than one. In a pass instance, the verifier continues to state σ_{k+1} and repeats the test, otherwise the verification ends and the verifier accepts the hypothesis H_0, that is, he/she asserts that the states were not $|\psi\rangle$. If all the N states σ_k pass the test, then the verifier rejects the hypothesis H_0 in favor of H_1, asserts that the states were indeed $|\psi\rangle$ and that the quantum device is working as intended.

To evaluate the type I error of the hypothesis testing scheme, we consider the worst-case failure probability $\max_{\langle\psi|\sigma|\psi\rangle\leq 1-\epsilon} \mathrm{Tr}(\Omega\sigma)$ of each run. Note that $\Omega|\psi\rangle = |\psi\rangle$ and the maximal eigenvalue of Ω equals one. So, one can restrict σ to be of the following form for the maximization

$$\sigma = (1-\epsilon')|\psi\rangle\langle\psi| + \epsilon'|\psi^\perp\rangle\langle\psi^\perp| \tag{12}$$

where $\epsilon' \geq \epsilon$ and $|\psi^\perp\rangle$ is orthogonal to $|\psi\rangle$. This further implies that the maximization is achieved when $\epsilon' = \epsilon$ and $|\psi^\perp\rangle$ is the eigenvector corresponding to the second largest eigenvalue of Ω. Thus, the worst-case failure probability is given by

$$\max_{\langle\psi|\sigma|\psi\rangle\leq 1-\epsilon} \mathrm{Tr}(\Omega\sigma) = 1 - \epsilon\nu(\Omega) \tag{13}$$

where $\nu(\Omega)$ represents the spectral gap between the largest ($\lambda_1 = 1$) and the second largest ($\lambda_2 = 1-\nu$) eigenvalues of Ω. In the case that H_0 is true and all the N sample states still pass the test, the type I error is bounded by

$$\delta \leq [1 - \epsilon\nu(\Omega)]^N \tag{14}$$

Thus, to achieve a given confidence $1-\delta$, it is sufficient to take

$$N = \frac{\ln(\delta)}{\ln[1-\epsilon\nu(\Omega)]} \tag{15}$$

sample states from the quantum device. In the high precision limit ($\epsilon, \delta \to 0$) this scales as

$$N \approx [\nu(\Omega)]^{-1}\epsilon^{-1}\ln(\delta^{-1}) \tag{16}$$

For the detailed construction of state verification protocols for specific states the main problem is to find the optimal Ω. Here, the optimization is typically subject to some constraints, as not all measurements are available. This will be discussed in details in the remainder of this review.

2.3. Quantum Fidelity Estimation

As we have mentioned, the QSV scenario above is an idealized model. This is because the choice of the two hypotheses in Equations (8) and (9) is impractical, in fact the hypothesis that $\sigma_k = |\psi\rangle\langle\psi|$ for all k is very unlikely to be true due to the unavoidable noise in actual experiments. Hence, a more practical model is to characterize the average fidelity of the output of the quantum device, which we refer to as quantum fidelity estimation (QFE)[61]; see also a related statistical entanglement witness method in refs. [62, 63] or Section 4.

To explain this, recall that the fidelity of some mixed quantum state ρ with a pure target state $|\psi\rangle$ is given by

$$F_\psi(\rho) = \langle\psi|\rho|\psi\rangle = \mathrm{Tr}(\rho|\psi\rangle\langle\psi|) \tag{17}$$

If ρ is a state generated in an experiment, this fidelity is a frequently used parameter to compare different

implementations.[23–25] Also, the fidelity may be used to prove that the state ρ is entangled. If the fidelity exceeds the maximal value for separable states, then the state ρ must necessarily be entangled. This approach is widely used,[20] although not all forms of entanglement can be detected with it.[64,65]

One of the main tasks for experiments is to develop methods to determine or estimate the fidelity from few measurements, without doing full state tomography of the state ρ. Indeed, for many cases, such as Bell states, cluster and graph states, or Dicke states, methods are known to be able to achieve this efficiently, that is, without using an exponentially increasing number of measurements.[27,66–69] Also known are the statistical tests based on the Hoeffding inequality of Equation (5),[17,26] which allow to compute rigorous error bars for the case that only a finite number of copies of the state ρ are available.

How can these concepts be connected with the concept of QSV? Given the output states σ_k, one can take the null and alternative hypotheses as follows

$$H_0 : \frac{1}{N}\sum_{k=1}^{N}\langle\psi|\sigma_k|\psi\rangle \leq 1-\varepsilon \tag{18}$$

$$H_1 : \frac{1}{N}\sum_{k=1}^{N}\langle\psi|\sigma_k|\psi\rangle > 1-\varepsilon \tag{19}$$

These hypotheses are essentially statements about the average fidelity of the states σ_k with the target state $|\psi\rangle$. In order to test these hypotheses, the verifier can take the same measurement strategy as in Equation (10). In this case, the verifier performs a random measurement $\{\Omega_{\ell}, \mathbb{1}-\Omega_{\ell}\}$ for each state σ_k and calculates the frequency f of the pass instances, that is,

$$f = \frac{t}{N} \tag{20}$$

where t is the number of cases where $\{\sigma_k\}_{k=1}^{N}$ pass the test. Now, the verifier may reject the null hypothesis and conclude that the average fidelity is larger than $1-\varepsilon$ if

$$f > 1-\varepsilon\nu(\Omega) \tag{21}$$

Furthermore, given the independence of σ_k, the confidence $1-\delta$ can be determined by the Chernof–Hoeffding theorem[52]

$$\delta \leq \mathrm{e}^{-D[f\|1-\varepsilon\nu(\Omega)]N} \tag{22}$$

where

$$D(x\|y) = x\ln\left(\frac{x}{y}\right) + (1-x)\ln\left(\frac{1-x}{1-y}\right) \tag{23}$$

is the Kullback–Leibler divergence. Note that the Hoeffding bound in Equation (5) can also be used for deriving the confidence, but it is weaker than Equation (22). Especially, if all the N states pass the test, that is, $f=1$, Equation (22) reduces to Equation (14), but now the physical consequences are clear. This is the confidence that the *average* fidelity of the output of the quantum device is larger than $1-\varepsilon$. Before, the rejection of the null hypothesis was interpreted as a statement on some of the states σ_k (see the discussion after Equation (9)) or, if one of the hypotheses in Equations (8, 9) is assumed to be true, as an acceptance of the hypothesis that $\sigma_k = |\psi\rangle\langle\psi|$ for all k.

A key feature of the presented QSV and QFE protocols 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 Equations (14) and (22), the performance of a verification strategy depends solely on $\nu(\Omega)$. Therefore, to achieve an optimal strategy, we need to maximize $\nu(\Omega)$ over all accessible measurements.

The previous discussions also imply that all measurement settings for QSV can be directly used for QFE. For simplicity, hereafter, we will only consider QSV strategies, but these strategies can be directly used for QFE, unless otherwise stated. Note, however, that optimality statements for a QSV strategy do not necessarily imply optimality for the QFE problem. This is because the bound in Equation (22) may not be optimal when $f<1$.

3. QSV for Entangled States

In QSV, a fundamental quantity is the spectral gap $\nu(\Omega)$. For any quantum state $|\psi\rangle$, if there is no constraint to the choice of measurements, one can easily see that the optimal verification strategy is to take $\Omega = |\psi\rangle\langle\psi|$, and correspondingly, $\nu(\Omega)=1$. If the quantum system involves many parties, it is, however, difficult or even impossible to implement the entangled measurement $\{|\psi\rangle\langle\psi|, \mathbb{1}-|\psi\rangle\langle\psi|\}$. In this case, a more realistic model is to consider local measurements or measurements assisted by local operations and classical communication (LOCC).

By a strategy with local measurements we mean that different parties perform their measurements independently, that is, no communication is needed during the measurements. For a strategy with measurements assisted by LOCC, some parties perform the measurements first, then the measurement outcomes are sent to the other parties, whose measurements depend on the received outcomes. As a result, QSV with local measurements and LOCC measurements are also called the nonadaptive and adaptive scenarios, respectively. Note that the adaptivity here does not mean that the verification strategy Ω in the kth run is changed based on the results of the previous $k-1$ tests.

3.1. QSV with Local Measurements

In ref. [29], the verification of entangled pure states with local projective measurements was introduced, as illustrated in **Figure 2**. The quantum device prepares quantum states σ_k for $k=1,2,\ldots,N$, which are promised to be an entangled state $|\psi\rangle$ between Alice and Bob. Suppose that each of the parties performs a single local projective measurements, for example, $\mathcal{M} = \{M_1, M_2, \ldots, M_{d_A}\}$ and $\mathcal{N} = \{N_1, N_2, \ldots, N_{d_B}\}$, then the entangled state $|\psi\rangle$ cannot be verified. This is because $M_a \otimes N_b$ are orthogonal projectors, and thus there exists no projector of the form

$$\Omega = \sum_{(a,b)\in\mathcal{Y}} M_a \otimes N_b \tag{24}$$

that can single out $|\psi\rangle$ as a nondegenerate eigenvector, where $\mathcal{Y}$ is any subset of the measurement outcomes. However, if we

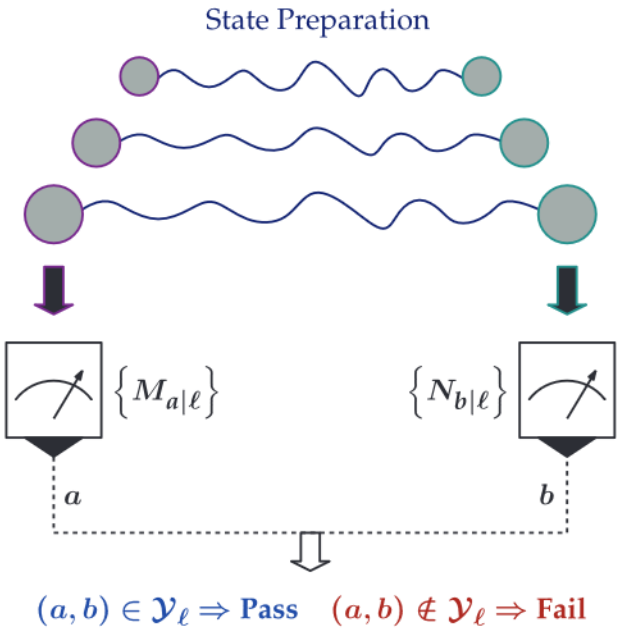


Figure 2. QSV with local measurements. In the kth run, Alice and Bob perform some random measurements $\mathcal{M}_\ell = \{M_{a|\ell}\}_{a=1}^{d_A}$ and $\mathcal{N}_\ell = \{N_{b|\ell}\}_{b=1}^{d_B}$ with probability p_ℓ using shared randomness. The state σ_k passes the test if their measurement outcomes a, b satisfy that $(a, b) \in \mathcal{Y}_\ell$. Note that classical communication is still necessary for making the decision on pass or fail.

consider randomly chosen measurements and construct different projectors Ω_ℓ, then it is possible to get a nonzero spectral gap $\nu(\Omega)$ for

$$\Omega = \sum_\ell p_\ell \Omega_\ell \tag{25}$$

Indeed, the previously mentioned example of spin correlation measurements on the singlet state illustrates already the potential advantage of randomly chosen measurements.

More formally, let Alice and Bob perform local measurements $\mathcal{M}_\ell = \{M_{1|\ell}, M_{2|\ell}, \ldots, M_{d_A|\ell}\}$ and $\mathcal{N}_\ell = \{N_{1|\ell}, N_{2|\ell}, \ldots, N_{d_B|\ell}\}$ with some probability p_ℓ, where both $M_{a|\ell}$ and $N_{b|\ell}$ add up to the identity. Let the set $\mathcal{Y}_\ell$ be defined as

$$\mathcal{Y}_\ell = \left\{ (a,b) \;\middle|\; M_{a|\ell} \otimes N_{b|\ell} |\psi\rangle \neq 0 \right\} \tag{26}$$

then Ω_ℓ may be chosen as

$$\Omega_\ell = \sum_{(a,b)\in\mathcal{Y}_\ell} M_{a|\ell} \otimes N_{b|\ell} \tag{27}$$

From the definition of $\mathcal{Y}_\ell$, it follows directly that $\Omega_\ell|\psi\rangle = |\psi\rangle$ and thus the verification defined as in Equation (25) also satisfies that $\Omega|\psi\rangle = |\psi\rangle$. In order to make Ω_ℓ nontrivial, that is, $\Omega_\ell \neq \mathbb{1}$, there must exist some $M_{a|\ell}$ and $N_{b|\ell}$ such that $M_{a|\ell} \otimes N_{b|\ell}|\psi\rangle = 0$.

Thus, finding the optimal local strategy can be written as

$$\begin{aligned} \max_{p_\ell, \Omega_\ell} \quad & \nu(\Omega) \\ \text{s.t.} \quad & \Omega = \sum_{\ell=1}^{m} p_\ell \Omega_\ell \\ & \Omega_\ell = \sum_{(a,b)\in\mathcal{Y}_\ell} M_{a|\ell} \otimes N_{b|\ell} \quad \forall\, \ell \\ & \sum_{\ell=1}^{m} p_\ell = 1, \;\; p_\ell \geq 0 \;\; \forall\, \ell \end{aligned} \tag{28}$$

Constructing the optimal verification strategy with local measurements is in general difficult, as the set of local strategies is complicated. However, efficient/optimal local strategies have been constructed for various widely-used states in quantum information processing, and in the following we will discuss these in details.

3.1.1. Bell States

As the first example, we consider the verification of Bell states

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{29}$$

In order to construct the local projectors, we take advantage of the fact that Bell states are eigenstates of local observables,

$$X \otimes X|\psi\rangle = |\psi\rangle, \;\; Y \otimes Y|\psi\rangle = -|\psi\rangle, \;\; Z \otimes Z|\psi\rangle = |\psi\rangle \tag{30}$$

where X, Y, Z are the Pauli matrices. The fact that certain pure quantum states are uniquely defined as eigenstates of such observables is described more generally in the so-called stabilizer formalism;[70] see also below.

With this relation, we can construct the verification strategy[29]

$$\Omega = \frac{1}{3}P_{XX}^{+} + \frac{1}{3}P_{YY}^{-} + \frac{1}{3}P_{ZZ}^{+} \tag{31}$$

where

$$P_{XX}^{+} = P_X^{+} \otimes P_X^{+} + P_X^{-} \otimes P_X^{-} = |+\rangle\langle+|^{\otimes 2} + |-\rangle\langle-|^{\otimes 2} \tag{32}$$

and similar for P_{YY}^{-} and P_{ZZ}^{+}.

In experiments, the verification protocol works as follows: in each run, Alice and Bob first use shared randomness to select with equal probability which measurement, $X \otimes X$, $Y \otimes Y$, or $Z \otimes Z$, they wish to perform. Second, they perform the corresponding measurements independently and share the measurement outcomes with classical communication. The result of this run is then decided by comparing their outcomes. For the $Y \otimes Y$ ($X \otimes X$ or $Z \otimes Z$) measurement, if their outcomes are different (the same), the outcome is labeled as pass, otherwise labeled as fail. At last, the frequency of the pass instances can be calculated after all the N runs.

From Equation (31), one can easily verify that the spectral gap is

$$\nu(\Omega) = \frac{2}{3} \tag{33}$$

As proved in ref. [29], this is the largest spectral gap achievable with projective local measurements. Moreover, as proved in refs. [61, 71], this is also optimal even if LOCC measurements are considered.

3.1.2. Maximally Entangled Two-Party States

The verification of Bell states can be directly generalized to the two-qudit maximally entangled states. For the two-qudit maximally entangled state

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{\alpha=1}^{d} |\alpha\alpha\rangle \tag{34}$$

an important symmetry[30,31] that can be used for constructing the verification strategy is that

$$U \otimes U^* |\psi\rangle = |\psi\rangle \tag{35}$$

where $U \in SU(d)$ and U^* is the complex conjugate of U in the computational basis $\{|\alpha\rangle\}_{\alpha=1}^{d}$. Let

$$P_{ZZ} = \sum_{\alpha=1}^{d} |\alpha\rangle\langle\alpha| \otimes |\alpha\rangle\langle\alpha| \tag{36}$$

then $P_{ZZ}|\psi\rangle = |\psi\rangle$ and a verification strategy with a continuous family of measurements can be written as

$$\Omega = \int_U U \otimes U^* P_{ZZ} U^\dagger \otimes U^T \mathrm{d}U = \frac{\mathbb{1} \otimes \mathbb{1} + d|\psi\rangle\langle\psi|}{d+1} \tag{37}$$

where the integral is with respect to the Haar measure. An easy way to see the second equality in Equation (37) is that the partial transpose of Ω is a Werner state.[72] The spectral gap of this strategy is given by

$$\nu(\Omega) = \frac{d}{d+1} \tag{38}$$

As proved in ref. [73], this strategy is optimal not only over all local measurements, but also over all LOCC measurements.

Equation (37) needs a continuous family of measurements, but it also admits a representation with finite number of measurements. This can be seen as follows. As Ω belongs to the convex hull of $\{U \otimes U^* P_{ZZ} U^\dagger \otimes U^T\}_U$ and the underlying space is finite-dimensional, the well-known Minkowski–Carathéodory theorem[74] implies that there exists a finite set $\{U_\ell\}_{\ell=1}^{m}$ such that

$$\Omega = \sum_{\ell=1}^{m} p_\ell U_\ell \otimes U_\ell^* P_{ZZ} U_\ell^\dagger \otimes U_\ell^T \tag{39}$$

for some probability distribution $(p_1, p_2, \ldots, p_m)$. An explicit construction of Equation (39) based on mutually unbiased bases[75] or weighted complex projective 2-designs[76,77] can be found in ref. [73]. An alternative construction based on measurements in the computational and Fourier bases accompanied with random local phase gates is presented in the next subsection.

3.1.3. GHZ States

The QSV protocol is also applicable to multi-party entangled states. We take the Greenberger–Horne–Zeilinger (GHZ) states, which are among the most widely used states in quantum information processing, as examples to illustrate this. The n-qubit GHZ state is defined as

$$|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) \tag{40}$$

It is well-known that the n-qubit GHZ state is identified by

$$X \otimes X \otimes \cdots \otimes X |\mathrm{GHZ}_n\rangle = |\mathrm{GHZ}_n\rangle \tag{41}$$

$$Z \otimes \mathbb{1}^{\otimes k} \otimes Z \otimes \mathbb{1}^{\otimes(n-k-2)} |\mathrm{GHZ}_n\rangle = |\mathrm{GHZ}_n\rangle \tag{42}$$

for $k = 0, 1, 2, \ldots, n-2$. In the language of the stabilizer formalism,[70] the n operators involved in Equations (41) and (42) are called generators of the stabilizer group, which consists of the elements (besides arbitrary permutations)

$$Z^{\otimes 2k} \otimes \mathbb{1}^{\otimes(n-2k)} \tag{43}$$

$$(-1)^k Y^{\otimes 2k} \otimes X^{\otimes(n-2k)} \tag{44}$$

for $k = 0, 1, 2, \ldots, \lfloor n/2 \rfloor$. The group is called the stabilizer group for $|\mathrm{GHZ}_n\rangle$ because all its 2^n elements g satisfy that $g|\mathrm{GHZ}_n\rangle = |\mathrm{GHZ}_n\rangle$. The elements of the stabilizer group play an outstanding role in the construction of quantum error-correcting code,[78] Bell inequalities,[79,80] and entanglement detection.[67]

For the verification of GHZ states different problems arise. Besides asking for the optimal verification strategy one may ask for efficient strategies, in the sense that these do not require many measurements. Concerning the latter point and in analogy to the results on entanglement witnesses,[66] Zhu and Hayashi showed that any n-qubit GHZ stated can be verified with two measurement settings,[81]

$$X \otimes X \otimes \cdots \otimes X, \quad Z \otimes Z \otimes \cdots \otimes Z \tag{45}$$

The key observation is that if the prepared state is indeed the GHZ state $|\mathrm{GHZ}_n\rangle$ and the n parties perform the measurement $Z^{\otimes n}$, then either all the n parties get the outcome +1 or all of them get the outcome −1. This will actually force the possible states to be within the subspace spanned by $\{|0\rangle^{\otimes n}, |1\rangle^{\otimes n}\}$. Then, the measurement $X^{\otimes n}$ can distinguish the two states $(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$ and $(|0\rangle^{\otimes n} - |1\rangle^{\otimes n})/\sqrt{2}$. Correspondingly, the verification operator can be written as

$$\Omega = \frac{1}{2} P_{Z^{\otimes n}} + \frac{1}{2} P^+_{X^{\otimes n}} \tag{46}$$

where

$$P_{Z^{\otimes n}} = |0\rangle\langle 0|^{\otimes n} + |1\rangle\langle 1|^{\otimes n} \tag{47}$$

$$P^{+}_{X^{\otimes n}} = \frac{\mathbb{1} + X^{\otimes n}}{2} \tag{48}$$

Physically, $P^{+}_{X^{\otimes n}}$ means that the test is passed when the product of the measurement outcomes of the n different parties is one. The spectral gap is

$$\nu(\Omega) = \frac{1}{2} \tag{49}$$

In the previous verification strategy, only the Pauli X and Z measurements are involved, but it is not optimal. In ref. [82], Li et al. showed that the optimal strategy can be achieved by considering all the stabilizers in Equation (44). By choosing the measurement settings (besides the permutations)

$$Z^{\otimes n}, \quad Y^{\otimes 2k} \otimes X^{\otimes n-2k}, \quad k = 0, 1, \ldots, \lfloor n/2 \rfloor \tag{50}$$

The optimal strategy can be achieved by

$$\Omega = \frac{1}{3}\left(P_{Z^{\otimes n}} + \frac{1}{2^{n-2}} \sum_{g \in S_{XY}} P^{+}_{g}\right) \tag{51}$$

where $P_{Z^{\otimes n}}$ is defined by Equation (47), S_{XY} is the set of all the 2^{n-1} stabilizers of the form in Equation (44), and

$$P^{+}_{g} = \frac{\mathbb{1} + g}{2} \tag{52}$$

means that the product of the measurement outcomes of the n different parties is one. The spectral gap

$$\nu(\Omega) = \frac{2}{3} \tag{53}$$

is optimal not only over all local measurements but also over all LOCC measurements. The above strategy can also be generalized to the n-qudit GHZ state with the optimal spectral gap $\nu(\Omega) = d/(d+1)$.[82]

At last, we would like to mention that it is also possible to verify GHZ states in the presence of dishonest parties. See a pioneering work by Pappa et al.,[83] a recent result by Han et al.,[84] and also a completely device-independent treatment by Dimić et al.[85]

3.1.4. Graph and Hypergraph States

The verification of GHZ states can be generalized to a class of widely-used entangled states in quantum information, the so-called stabilizer states.[78] Without loss of generality, we only need to consider the family of graph states,[86,87] as any stabilizer state is equivalent to a graph state up to a local Clifford (LC) operation.[88–90] Here, local Clifford operations are local unitary transformations, which leave the set of Pauli matrices up to some signs invariant.

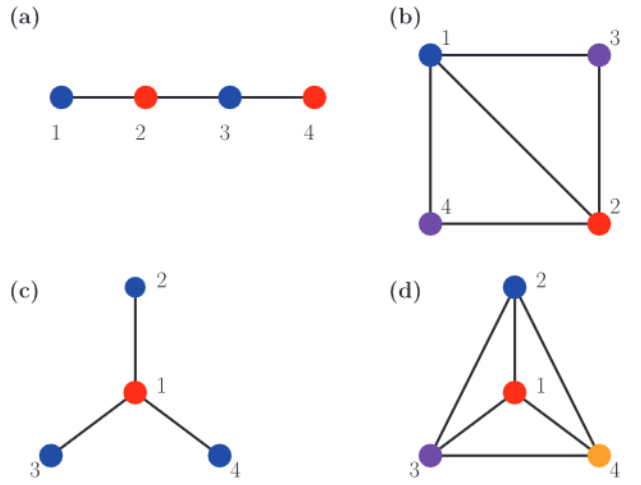


Figure 3. Some graphs and their optimal coloring. Graphs (a) and (b) have equivalent corresponding graph states (up to an LC operation), but their chromatic numbers are different. So are graphs (c) and (d), and moreover they are equivalent to the 4-qubit GHZ state.

Graph states are defined as follows: First, one considers a graph $G = (V, E)$, that is, an object with $n := |V|$ vertices and $|E|$ edges connecting some pairs of the vertices; see some examples in **Figure 3**. We can associate to each vertex $i \in V$ an operator

$$g_i = X_i \otimes \bigotimes_{\{i,j\} \in E} Z_j \tag{54}$$

that is, g_i consists of a Pauli X observable on the qubit i and a Pauli Z observable on all qubits in the neighborhood. The graph state $|G\rangle$ corresponding to the graph G is then defined as the unique state that satisfies the eigenvalue relations

$$g_i|G\rangle = |G\rangle \tag{55}$$

for all $i \in V$. The mutually commuting operators g_i generate the stabilizer group

$$\mathcal{S} = \left\{ g_1^{b_1} g_2^{b_2} \ldots g_n^{b_n} \;\middle|\; b_i = 0, 1 \right\} \tag{56}$$

for $|G\rangle$. Alternatively, an explicit expression of the graph state $|G\rangle$ is

$$|G\rangle = \prod_{\{i,j\} \in E} \mathrm{CZ}_{ij} |+\rangle^{\otimes n} \tag{57}$$

where the two-qubit control-Z gates CZ_{ij}, defined as

$$\begin{aligned} \mathrm{CZ}_{ij} &= |0\rangle\langle 0|_i \otimes \mathbb{1}_j + |1\rangle\langle 1|_i \otimes Z_j \\ &= |0\rangle\langle 0|_j \otimes \mathbb{1}_i + |1\rangle\langle 1|_j \otimes Z_i \\ &= \mathbb{1}_i \otimes \mathbb{1}_j - 2|1\rangle\langle 1|_i \otimes |1\rangle\langle 1|_j \end{aligned} \tag{58}$$

are mutually commuting. Finally, it should be noted that Bell states and GHZ states are, up to a local change of the basis, also graph states.

In ref. [29], the verification of graph states is considered as a direct generalization for the verification of Bell states. Let S be the stabilizer group of $|G\rangle$, then one can construct a verification strategy

$$\Omega = \frac{1}{2^n - 1} \sum_{g \in S, g \neq \mathbb{1}} P_g^+ \tag{59}$$

As in Equation (40), $P_g^+ = (\mathbb{1}^{\otimes n} + g)/2$ means that the product of the measurement outcomes of the n different parties is one. The definition of the graph state implies the relation

$$|G\rangle\langle G| = \prod_{i=1}^{n} \frac{\mathbb{1} + g_i}{2} = \frac{1}{2^n} \sum_{g \in S} g \tag{60}$$

from which one obtains that

$$\Omega = \frac{2^{n-1}}{2^n - 1} |G\rangle\langle G| + \frac{2^{n-1} - 1}{2^n - 1} \mathbb{1} \tag{61}$$

Thus, the spectral gap is given by

$$\nu(\Omega) = \frac{2^{n-1}}{2^n - 1} = \frac{1}{2} + \frac{1}{2^{n+1} - 2} \tag{62}$$

Unlike the case of Bell states, this strategy is no longer optimal for the general graph states. One example was already shown for the case of GHZ states. The spectral gap in Equation (59) is slightly better than the verification strategy with two measurement settings in Equation (46), but less efficient than the optimal strategy in Equation (51).

In ref. [81], Zhu and Hayashi put forward another efficient method for verifying graph states. This method is closely related to the coloring problem of the corresponding graphs, which also plays a central role for efficient entanglement witnesses.[67] A (proper) coloring of a graph is a labeling of the graph's vertices with colors such that no two adjacent vertices have the same color. A graph G is called m-colorable if there exists a coloring with m colors and the smallest number of colors needed for coloring G is called the chromatic number $\chi(G)$; some examples are shown in Figure 3.

Now, we can explain the coloring strategy for verifying graph states. Let $c : V \to \{1, 2, \ldots, m\}$ be an m-coloring of a graph G. Then, the following m measurement settings are taken

$$\bigotimes_{c(i)=\ell} X_i \otimes \bigotimes_{c(i)\neq\ell} Z_i \quad \text{for } \ell = 1, 2, \ldots, m \tag{63}$$

For example, for the colored graph in Figure 3a, the measurement settings read

$$X \otimes Z \otimes X \otimes Z, \quad Z \otimes X \otimes Z \otimes X \tag{64}$$

The reason for choosing the measurement settings in Equation (63) is that all the measurement outcomes of the generators g_i in Equation (54), or more precisely, $\{P_{g_i}^+, \mathbb{1} - P_{g_i}^+\}$, can be inferred from the outcomes. Indeed, the measurement outcome of $\{\Omega_\ell, \mathbb{1} - \Omega_\ell\}$ with

$$\Omega_\ell = \prod_{c(i)=\ell} \frac{1 + g_i}{2} \tag{65}$$

can be inferred from the ℓth measurement setting in Equation (63). Then, by choosing

$$\Omega = \frac{1}{m} \sum_{\ell=1}^{m} \Omega_\ell \tag{66}$$

one can achieve the spectral gap

$$\nu(\Omega) = \frac{1}{m} \tag{67}$$

With the coloring strategy, the largest spectral gap that can be achieved is $1/\chi(G)$, where $\chi(G)$ is the chromatic number of the graph G. But still, there exist some possible improvements and generalizations of the coloring strategy.

First, efficiency of the coloring strategy can be improved by the LC operations,[88] which do not change the entanglement properties of the graph state, but they change the graph and hence the chromatic number. In this way, the graph state can be transformed to a local unitary equivalent graph state, which however may have a smaller chromatic number. For example, the graph states in Figure 3b,d are equivalent to those in Figure 3a,c, respectively, but the chromatic numbers are reduced from $3 \to 2$ and $4 \to 2$, respectively. This reduction can not only simplify the measurement settings, but also improve the verification efficiency.

Second, another way to improve the verification efficiency is to take advantage of the so-called fractional coloring. The corresponding strategy is called the fractional coloring strategy (or cover strategy).[81] In the fractional coloring strategy, arbitrary independent sets instead of disjoint independent sets are taken, and the largest achievable spectral gap is $1/\chi_f(G)$, where $\chi_f(G) \leq \chi(G)$ is called the fractional chromatic number.[91]

Third, as also shown in ref. [81], both the coloring and fractional coloring strategies can be directly generalized to the family of so-called hypergraph states.[92–94] Although the stabilizer operators for hypergraph states are non-local as they contain multi-qubit control-Z operators, they can still be revealed by local measurements. This is because the measurement outcome of the n-qubit control-Z operator $C^{n-1}Z$ can be revealed by the local measurement $Z^{\otimes n}$, mathematically speaking

$$\frac{\mathbb{1}^{\otimes n} - C^{n-1}Z}{2} = \bigotimes_{i=1}^{n} \frac{\mathbb{1} - Z_i}{2} \tag{68}$$

The coloring and fractional coloring of hypergraphs are also defined similarly,[91] from which the coloring and fractional coloring strategies can be naturally generalized to the hypergraph states.

Recently, Dangniam et al. put forward an algorithm for finding the optimal verification strategies for graph states with Pauli measurements.[95] The optimal verification strategies are based on the so-called canonical test operators, and finding the optimal strategy can be written as a linear program. Surprisingly, for all

the graph states numerically tested in ref. [95], including all states with no more than seven qubits, the maximal spectral gap is

$$\nu(\Omega) = \frac{2}{3} \tag{69}$$

which is also optimal over all local or LOCC measurements. This motivates the authors to conjecture that the upper bound $\nu(\Omega) = \frac{2}{3}$ can be achieved for all graph states with Pauli measurements.

In addition, we would like to point out that there are also plenty of other statistical methods for verifying graphs and hypergraph states[26,96–99]; see ref. [81] for a detailed comparison of these methods.

3.1.5. General Pure Two-Qubit States

All the above strategies are related to the stabilizer formalism. For general states, it is however difficult to construct an optimal verification strategy. The only known optimal result is for two-qubit pure states with local projective measurements. Without loss of generality, we can assume that the general (not separable or maximally entangled) pure quantum state is of the form

$$|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \tag{70}$$

where $0 < \theta < \pi/4$.

In ref. [29], Pallister et al. showed that the optimal strategy for verifying the state in Equation (70) is

$$\Omega = \alpha(\theta) P_{ZZ}^{+} + \frac{1-\alpha(\theta)}{3} \sum_{\ell=1}^{3} (\mathbb{1} - |u_\ell\rangle\langle u_\ell| \otimes |v_\ell\rangle\langle v_\ell|) \tag{71}$$

where $\alpha(\theta) = \frac{2-\sin(2\theta)}{4+\sin(2\theta)}$ and $|u_\ell\rangle|v_\ell\rangle$ are some states such that $\langle u_\ell|\langle v_\ell|\psi\rangle = 0$. The optimal spectral gap is given by

$$\nu(\Omega) = \frac{1}{2 + \sin\theta\cos\theta} \tag{72}$$

As shown in **Figure 4**, the optimal spectral gap is not continuous at $\theta = \pi/4$, which suggests that there may exist methods to improve the verification efficiency. Indeed, unlike in the case of Bell states, the strategy in Equation (71) is no longer optimal if local POVMs are considered, at least for some $0 < \theta < \pi/4$. An easy way to see this is to perform a local filtering to make the state maximally entangled and then perform the optimal verification for the resulted state. In this way, the verification efficiency will be continuous at $\theta = \pi/4$. However, finding the optimal strategy with local POVMs is still an open problem, even for two-qubit states. Another method for improving the verification efficiency is to take advantage of LOCC measurements, which is the main topic of the next subsection.

The first experimental implementation of QSV on two-qubit entangled photonic states with local measurements was reported in ref. [100]. Considering the robustness to practical imperfections, the actual realization was relying on the Chernof–Hoeffding bound in Equation (22). The inverse proportionality between the estimated infidelity and the number of samples was clearly demonstrated by all the tested states. For the estimated infidelity of, say $\epsilon = 0.01$, the confidence level rapidly approaches near-unity within 1000 number of samples. Moreover, to show the scalability of the QSV methodology, a four-qubit GHZ state was also verified.

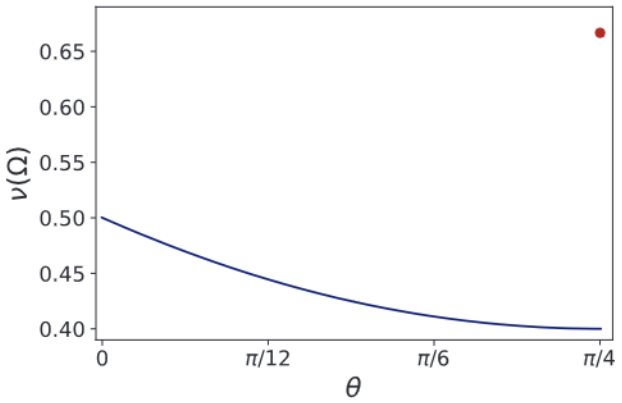


Figure 4. Optimal verification of $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with local projective measurements. When $0 < \theta < \pi/4$, the spectral gap is shown in Equation (72), which satisfies that $\lim_{\theta\to\pi/4} \nu(\Omega) = 2/5$. However, when $\theta = \pi/4$, the optimal gap is 2/3, as shown in Equation (33).

3.2. QSV with LOCC Measurements

QSV with LOCC measurements was proposed independently in refs. [61, 71, 101]. LOCC is a method in quantum information theory where the local operations are assisted by classical communication between the parties.[102] The set of general LOCC measurements is complicated due to the unbounded number of communication rounds.[103,104] As a result, most of the works on QSV with LOCC measurements focus on the simplified scenario of one-round communication.

We start with the analysis of the one-way LOCC strategy for two parties, Alice and Bob, as illustrated in **Figure 5**. In this case, Alice first performs a random measurement $\mathcal{M}_\ell = \{M_{a|\ell}\}_a$ with probability p_ℓ on her subsystem, and sends to Bob the measurement setting ℓ and the outcome a, based on which Bob performs a measurement $\{N_{a|\ell}, \mathbb{1} - N_{a|\ell}\}$ on his subsystem. The state σ_k passes the test if and only if Bob obtains the outcome corresponding to $N_{a|\ell}$. Thus, the one-way LOCC strategy $\Omega^{\rightarrow}$ is of the form

$$\Omega^{\rightarrow} = \sum_{\ell=1}^{n} p_\ell \Omega_\ell^{\rightarrow}, \quad \Omega_\ell^{\rightarrow} = \sum_a M_{a|\ell} \otimes N_{a|\ell} \tag{73}$$

Without loss of generality, one can assume that the measurement operators $M_{a|\ell}$ are rank-one. If this is not the case, one can always perform a finer measurement by measuring the spectral decomposition. Then, Alice's measurement $\mathcal{M}_\ell$ would cause Bob's subsystem to collapse to the pure state

$$P_{a|\ell} = \frac{\mathrm{Tr}_A\left[(M_{a|\ell} \otimes \mathbb{1})|\psi\rangle\langle\psi|\right]}{\mathrm{Tr}\left[(M_{a|\ell} \otimes \mathbb{1})|\psi\rangle\langle\psi|\right]} \tag{74}$$

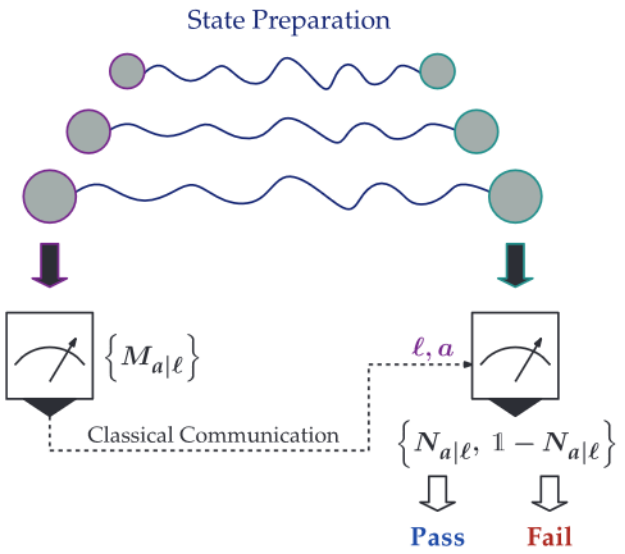


Figure 5. QSV with one-way LOCC measurements. In the kth run, Alice randomly chooses a measurement $\mathcal{M}_\ell$ with probability p_ℓ. After performing the measurement $\mathcal{M}_\ell$, Alice tells Bob via classical communication the measurement setting ℓ and the outcome a, based on which Bob performs the pass or fail test $\{N_{a|\ell}, \mathbb{1} - N_{a|\ell}\}$.

where a is the corresponding measurement outcome. For a fixed $\mathcal{M}_\ell$, the optimal strategy for Bob is to take

$$N_{a|\ell} = P_{a|\ell} \tag{75}$$

Thus, a strategy of this form is called semi-optimal, as it is optimal concerning Bob's side. From the definition, one can easily prove the following necessary conditions for $\Omega^{\rightarrow}$ being semi-optimal

$$\Omega^{\rightarrow} \in \mathrm{SEP}, \quad \mathrm{Tr}_B(\Omega^{\rightarrow}) = \mathbb{1}, \quad \langle\psi|\Omega^{\rightarrow}|\psi\rangle = 1 \tag{76}$$

where SEP is the set of unnormalized separable states, that is,

$$\mathrm{SEP} := \left\{ \sum_i X_i^A \otimes Y_i^B \;\middle|\; X_i^A \geq 0,\ Y_i^B \geq 0 \right\} \tag{77}$$

On the other hand, if $\Omega^{\rightarrow}$ is of the form in Equation (76), one can also verify that it has a decomposition of the form in Equation (73).[61] Thus, constructing the optimal one-way LOCC strategy can be written as the following convex optimization problem

$$\begin{aligned} \max_{\Omega^{\rightarrow}} \quad & \nu(\Omega^{\rightarrow}) \\ \text{s.t.} \quad & \Omega^{\rightarrow} \in \mathrm{SEP} \\ & \mathrm{Tr}_B(\Omega^{\rightarrow}) = \mathbb{1} \\ & \langle\psi|\Omega^{\rightarrow}|\psi\rangle = 1 \end{aligned} \tag{78}$$

Let us continue to discuss the case of one-round two-way LOCC strategies. In this case, Alice and Bob use shared randomness to decide who first performs the measurement. After the measurement, the measurement outcome is sent to the other party. The receiver then performs the pass or fail test according to the received measurement outcome. Further, up to some local unitary operation, a general bipartite pure state can be written in the Schmidt decomposition

$$|\psi\rangle = \sum_{\alpha=1}^{d} \lambda_\alpha |\alpha\alpha\rangle \tag{79}$$

where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d \geq 0$.

Thanks to the permutation symmetry of $|\psi\rangle$ in Equation (79), the optimization in this setting can be easily simplified. Let V be the SWAP operator, that is,

$$V|\alpha\rangle|\beta\rangle = |\beta\rangle|\alpha\rangle \quad \text{for all } \alpha, \beta = 1, 2, \ldots, d \tag{80}$$

then we have $V|\psi\rangle = |\psi\rangle$. This indicates that, if Ω is a two-way LOCC strategy, so is $(\Omega + V\Omega V^\dagger)/2$. Furthermore, one can easily show that

$$\nu\left[\tfrac{1}{2}(\Omega + V\Omega V^\dagger)\right] \geq \tfrac{1}{2}\left[\nu(\Omega) + \nu(V\Omega V^\dagger)\right] = \nu(\Omega) \tag{81}$$

Hence, one can focus on the two-way LOCC strategies that are invariant under the SWAP operation. When restricted to the one-round case, constructing the optimal strategy $\Omega^{\leftrightarrow}$ can be written as

$$\begin{aligned} \max_{\Omega^{\rightarrow}} \quad & \nu\left[\tfrac{1}{2}(\Omega^{\rightarrow} + \Omega^{\leftarrow})\right] \\ \text{s.t.} \quad & \Omega^{\rightarrow} \in \mathrm{SEP}, \\ & \mathrm{Tr}_B(\Omega^{\rightarrow}) = \mathbb{1}, \\ & \langle\psi|\Omega^{\rightarrow}|\psi\rangle = 1 \end{aligned} \tag{82}$$

where $\Omega^{\rightarrow}$ is a one-way LOCC strategy, $\Omega^{\leftarrow} = V\Omega^{\rightarrow}V^\dagger$, and the constraints are from Equation (78).

At last, we note that it is possible to further improve the verification efficiency by considering many-round communication; see **Figure 6**. A concrete example will be shown for two-qubit pure states below.

3.2.1. General Two-Qubit Pure States

As in Equation (70), we write the general two-qubit entangled pure state as $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $0 < \theta \leq \pi/4$. Then the optimization problems in Equations (78) and (82) are directly solvable because the positive partial transpose (PPT) criterion provides a necessary and sufficient condition for the separability problem.[105,106] Indeed, the optimization problems can be solved analytically by taking advantage of the symmetry.

Contrary to the maximally entangled state, a general bipartite pure state has no longer the $U \otimes U^*$ symmetry as in Equation (35). However, a restricted symmetry still holds where the U are constrained to be the diagonal unitary matrices.[29] This is also equivalent to the discrete group $\mathcal{G}$ generated by the following phase gate

$$g_0 = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -\mathrm{i} \end{bmatrix} \tag{83}$$

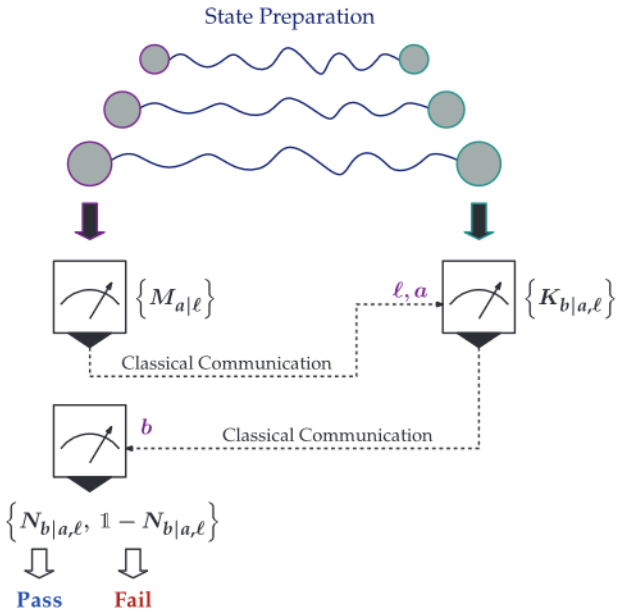


Figure 6. QSV with many-round LOCC measurements. In the protocol, nondestructive measurements are performed and many-round communication is involved between Alice and Bob.

which also plays an important role in constructing the optimal verification strategy.[61] One can easily verify that $\mathcal{G} = \{\mathbb{1}, g_0, g_0^2, g_0^3\}$ and

$$\nu\left(\sum_{g\in\mathcal{G}} g\Omega g^\dagger\right) \geq \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \nu\left(g\Omega g^\dagger\right) = \nu(\Omega) \tag{84}$$

Thus, without loss of generality, one can assume that the optimal Ω is invariant under $\mathcal{G}$. Then, by taking advantage of the PPT criterion, one obtains the optimal verification strategy by solving the optimization in Equation (78), and the spectral gap is given by

$$\max_{\Omega^{\rightarrow}} \nu(\Omega^{\rightarrow}) = \frac{1}{1+\cos^2\theta} \tag{85}$$

As shown in refs. [61, 71, 101], this optimal spectral gap can be achieved already with the following projective measurements

$$\Omega^{\rightarrow} = \frac{1}{(1+\cos^2\theta)}\left[(\cos^2\theta)P^{+}_{ZZ} + \frac{1}{2}X^{\rightarrow}_{\psi} + \frac{1}{2}Y^{\rightarrow}_{\psi}\right] \tag{86}$$

where

$$\begin{aligned} P^{+}_{ZZ} &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|, \\ X^{\rightarrow}_{\psi} &= |\varphi_0\rangle\langle\varphi_0| + |\varphi_2\rangle\langle\varphi_2|, \\ Y^{\rightarrow}_{\psi} &= |\varphi_1\rangle\langle\varphi_1| + |\varphi_3\rangle\langle\varphi_3| \end{aligned} \tag{87}$$

with $|\varphi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)$ and $|\varphi_k\rangle = g_0^k|\varphi_0\rangle$ for $k = 1, 2, 3$.

Similarly, for the case of one-round two-way LOCC measurements, the optimal spectral gap, that is, the solution of the optimization in Equation (82), is given by

$$\max_{\Omega^{\leftrightarrow}} \nu(\Omega^{\leftrightarrow}) = \frac{2}{3} \tag{88}$$

which can also be achieved by projective measurements[61,71,101]

$$\Omega^{\leftrightarrow} = \frac{1}{3}P^{+}_{ZZ} + \frac{1}{6}X^{\rightarrow}_{\psi} + \frac{1}{6}X^{\leftarrow}_{\psi} + \frac{1}{6}Y^{\rightarrow}_{\psi} + \frac{1}{6}Y^{\leftarrow}_{\psi} \tag{89}$$

where P^{+}_{ZZ}, $X^{\rightarrow}_{\psi}$, and $Y^{\rightarrow}_{\psi}$ are defined as in Equation (87), and $X^{\leftarrow}_{\psi} = VX^{\rightarrow}_{\psi}V^\dagger$ and $Y^{\leftarrow}_{\psi} = VY^{\rightarrow}_{\psi}V^\dagger$, with V being the SWAP operator.

In addition, it is also possible to improve the verification efficiency further by taking advantage of many-round communication.[71] The building block $\{X^{A\Leftrightarrow B}_{\psi,\eta}, \mathbb{1} - X^{A\Leftrightarrow B}_{\psi,\eta}\}$ is the following measurement procedure:

1) Alice first performs a nondestructive POVM $\{M_0 := \eta|0\rangle\langle 0|, M_1 := \mathbb{1} - \eta|0\rangle\langle 0|\}$ and sends the measurement outcome 0 or 1 to Bob.
2) If the measurement outcome of Alice is zero, Bob performs the measurement Z on his subsystem and accepts (rejects) the test if he obtains the outcome +1 (−1). If the measurement outcome of Alice is one, Bob performs the measurement X on his subsystem and sends the measurement outcome +1 or −1 back to Alice.
3) Based on the measurement outcome of Bob, Alice performs the corresponding test to check whether the subsystem is in the post-measurement state $|\nu_+\rangle\langle\nu_+|$ or $|\nu_-\rangle\langle\nu_-|$, which is defined similarly as the in semi-optimal strategy in Equations (74) and (75).

Mathematically, this procedure (for the pass instances) can be written as

$$\begin{aligned} \rho \rightarrow &\left[\sqrt{M_0}\otimes|0\rangle\langle 0|\right]\rho\left[\sqrt{M_0}\otimes|0\rangle\langle 0|\right] \\ &+ \left[\left(|\nu_+\rangle\langle\nu_+|\sqrt{M_1}\right)\otimes|+\rangle\langle +|\right]\rho\left[\left(\sqrt{M_1}|\nu_+\rangle\langle\nu_+|\right)\otimes|+\rangle\langle +|\right] \\ &+ \left[\left(|\nu_-\rangle\langle\nu_-|\sqrt{M_1}\right)\otimes|-\rangle\langle -|\right]\rho\left[\left(\sqrt{M_1}|\nu_-\rangle\langle\nu_-|\right)\otimes|-\rangle\langle -|\right] \end{aligned} \tag{90}$$

where

$$|\nu_\pm\rangle\langle\nu_\pm| = \frac{\mathrm{Tr}_B\left[\left(\sqrt{M_1}\otimes|\pm\rangle\langle\pm|\right)|\psi\rangle\langle\psi|\left(\sqrt{M_1}\otimes|\pm\rangle\langle\pm|\right)\right]}{\mathrm{Tr}\left[\left(\sqrt{M_1}\otimes|\pm\rangle\langle\pm|\right)|\psi\rangle\langle\psi|\left(\sqrt{M_1}\otimes|\pm\rangle\langle\pm|\right)\right]} \tag{91}$$

Accordingly, $X^{A\Leftrightarrow B}_{\psi,\eta}$ reads

$$\begin{aligned} X^{A\Leftrightarrow B}_{\psi,\eta} = M_0\otimes|0\rangle\langle 0| &+ \left(\sqrt{M_1}|\nu_+\rangle\langle\nu_+|\sqrt{M_1}\right)\otimes|+\rangle\langle +| \\ &+ \left(\sqrt{M_1}|\nu_-\rangle\langle\nu_-|\sqrt{M_1}\right)\otimes|-\rangle\langle -| \end{aligned} \tag{92}$$

By taking advantage of the symmetry, one can construct similar procedures $Y^{A\Leftrightarrow B}_{\psi,\eta}$, in which the measurement X is replaced

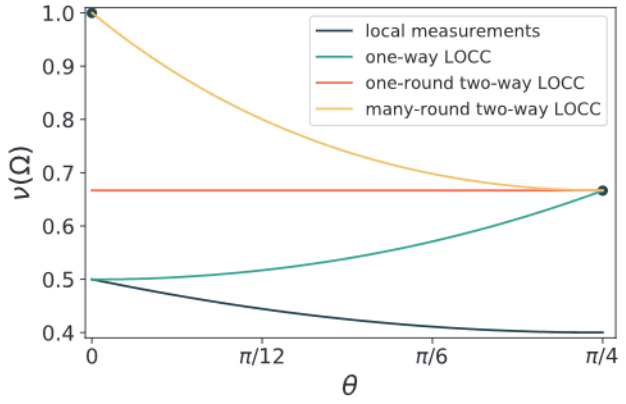


Figure 7. Optimal values of $\nu(\Omega)$ with different verification strategies for the two-qubit entangled pure state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $0 \le \theta \le \pi/4$. Note that when $\theta = 0$ or $\theta = \pi/4$, all strategies give the same optimal spectral gap $\nu(\Omega) = 1$ or $\nu(\Omega) = 2/3$.

by Y, as well as $X^{\mathrm{B}\Leftrightarrow\mathrm{A}}_{\psi,\eta}$ and $Y^{\mathrm{B}\Leftrightarrow\mathrm{A}}_{\psi,\eta}$, in which Bob, instead of Alice, starts the measurement. In ref. [71], Wang and Hayashi proved that the optimal verification strategy with many-round communication can be achieved by

$$\Omega^{\Leftrightarrow} = pP^{+}_{ZZ} + \frac{1-p}{4}\left(X^{\mathrm{A}\Leftrightarrow\mathrm{B}}_{\psi,\eta} + X^{\mathrm{B}\Leftrightarrow\mathrm{A}}_{\psi,\eta} + Y^{\mathrm{A}\Leftrightarrow\mathrm{B}}_{\psi,\eta} + Y^{\mathrm{B}\Leftrightarrow\mathrm{A}}_{\psi,\eta}\right) \tag{93}$$

where $\eta = 1 - \tan\theta$ and $p = (\sin^2\theta)/(1 + \sin\theta\cos\theta)$. The optimal spectral gap is

$$\nu(\Omega^{\Leftrightarrow}) = \frac{1}{1 + \sin\theta\cos\theta} \tag{94}$$

Remarkably, this strategy is also optimal for the case that infinite rounds of classical communication are allowed. The comparison of the verification efficiency (spectral gap) of different local and LOCC strategies is illustrated in **Figure 7**.

Using photonic systems, both the experiments reported in refs. [107, 108] have successfully demonstrated the enhanced QSV strategies using classical communication. For instance, it was shown in ref. [108] that only 60% of the measurements are required to achieve a certain value of precision as compared to the optimal strategy with local projective measurements. Hence, the experimental results clearly indicate that classical communication can significantly enhance the performance of QSV, and lead to an efficiency that further approaches the globally optimal bound.

3.2.2. General Bipartite Pure States

We move on to discuss the verification of general bipartite pure states with LOCC measurements. As in Equation (79), we write the bipartite pure state as $|\psi\rangle = \sum_{\alpha=1}^{d} \lambda_\alpha |\alpha\alpha\rangle$, where $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_d$.

To construct the optimal LOCC strategy, a crucial ingredient is the group $\mathcal{G}$ generated by

$$g_\alpha = \Phi_\alpha \otimes \Phi_\alpha^{\dagger}, \quad \alpha = 1, 2, \ldots, d \tag{95}$$

$$\Phi_\alpha|\beta\rangle = \begin{cases} \mathrm{i}|\beta\rangle & \text{when } \alpha = \beta, \\ |\beta\rangle & \text{when } \alpha \ne \beta \end{cases} \tag{96}$$

which generalizes Equation (83) to the two-qudit case. Similar to Equation (84), we can also assume the optimal Ω is invariant under $\mathcal{G}$.

The main difference between two-qudit and two-qubit states is that the PPT criterion is no longer sufficient for characterizing the separability when $d \ge 3$.[106] Hence, by replacing $\Omega^{\rightarrow} \in \mathrm{SEP}$ with $\Omega^{\rightarrow} \ge 0$ and $(\Omega^{\rightarrow})^{T_B} \ge 0$, Equations (78) and (82) only give us relaxations of the original optimization problems, and the solutions of the relaxed problems only result in upper bounds of the optimal $\nu(\Omega^{\rightarrow})$ and $\nu(\Omega^{\leftrightarrow})$.

For the one-way LOCC strategy, the relaxed optimization problem can be solved analytically,[61] which gives the upper bound

$$\max_{\Omega^{\rightarrow}} \nu(\Omega^{\rightarrow}) \le \frac{1}{1 + \lambda_1^2} \tag{97}$$

for all $d \ge 2$. Fortunately, this upper bound can be achieved with one-way LOCC measurements, or even with projective ones. The corresponding verification strategy reads

$$\Omega^{\rightarrow} = \omega P_{ZZ} + \frac{1-\omega}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} g X^{\rightarrow}_{\psi} g^{\dagger} \tag{98}$$

where

$$P_{ZZ} = \sum_{\alpha=1}^{d} |\alpha\rangle\langle\alpha| \otimes |\alpha\rangle\langle\alpha|, \; X^{\rightarrow}_{\psi} = \sum_{\alpha=1}^{d} |f_\alpha\rangle\langle f_\alpha| \otimes |\phi_\alpha\rangle\langle\phi_\alpha|$$
$$|f_\alpha\rangle = \frac{1}{\sqrt{d}}\sum_{\beta=1}^{d} \zeta_d^{\alpha\beta}|\beta\rangle, \quad |\phi_\alpha\rangle = \sum_{\beta=1}^{d} \zeta_d^{-\alpha\beta}\lambda_\beta|\beta\rangle \tag{99}$$

with $\zeta_d = \mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}$ and $\omega = \lambda_1^2/(1 + \lambda_1^2)$. In experiments, the above strategy can be easily implemented with the random measurement in the computational basis $\{|\alpha\rangle\}_{\alpha=1}^{d}$ or in the Fourier basis $\{|f_\alpha\rangle\}_{\alpha=1}^{d}$ accompanied by random phase shifts from $\mathcal{G}$. Especially, when $|\psi\rangle$ is maximally entangled, $\{|\phi_\alpha\rangle\}_{\alpha=1}^{d}$ forms an orthogonal basis. Hence, Equation (99) gives an alternative optimal strategy for verifying maximally entangled states with local projective measurements.

For one-round two-way LOCC strategies, the verification efficiency can also be improved by averaging $\Omega^{\rightarrow}$ and its swap $\Omega^{\leftarrow}$. Specifically, one can achieve the spectral gap

$$\nu(\Omega^{\leftrightarrow}) = \nu\left[\tfrac{1}{2}(\Omega^{\rightarrow} + \Omega^{\leftarrow})\right] = \frac{1}{1 + \lambda^2} \tag{100}$$

when $\Omega^{\rightarrow}$ is of the form in Equation (98) with

$$\omega = \frac{\lambda^2}{1 + \lambda^2}, \quad \lambda^2 = \frac{1}{2}\left(\lambda_1^2 + \lambda_2^2\right) \tag{101}$$

Unlike the two-qubit case, this one-round two-way LOCC strategy is only nearly optimal for general bipartite states.[61]

Remarkably, as shown in ref. [101], the optimal and near-optimal spectral gap in Equations (97) and (100) can also be

achieved by taking advantage of the complete set of MUBs or with 2-designs, which are essentially different implementations (decompositions) of the same verification operators $\Omega^{\rightarrow}$ or $\Omega^{\leftrightarrow}$ in Equations (98) and (100).

3.2.3. W States and Dicke States

The LOCC strategies can be easily generalized for verifying multi-party states. Especially, the first verification strategy for non-stabilizer states was constructed by Liu et al., in ref. [109] for W states and Dicke states.

We take W states to illustrate the idea for verifying multi-party states with LOCC measurements. The n-qubit W state[13,110] is defined as

$$|W_n\rangle = \frac{1}{\sqrt{n}}(|10\ldots0\rangle + |01\ldots0\rangle + \cdots + |00\ldots1\rangle) \tag{102}$$

The verification strategy for $|W_n\rangle$ is based on the following two observations (which have also been used to derive non-locality arguments[111]): First, the state $|W_n\rangle$ is symmetric under permutations. Second, if the verifier performs the measurement $Z^{\otimes(n-2)}$ on the first $n-2$ qubits, then outcome 1 can appear at most once; otherwise, the original state cannot be $|W_n\rangle$. If outcome 1 appears, then the post-measurement state of parties $n-1$ and n will be $|00\rangle$, which can be verified easily by $Z\otimes Z$ measurement on these two qubits; if outcome 1 does not appear, then the post-measurement state will be the Bell state $(|01\rangle + |10\rangle)/\sqrt{2}$, which can be verified with local measurements as shown in Equation (31). By taking advantage of the permutation symmetry, it can be shown that the tests based on $Y\otimes Y$ and $Z\otimes Z$ measurements in Equation (31) can be dropped. More precisely, $|W_n\rangle$ can be verified efficiently using the strategy

$$\Omega^{\leftrightarrow} = \frac{2}{n(n-1)}\sum_{i<j}\Omega^{\rightarrow}_{i,j} \tag{103}$$

with

$$\Omega^{\rightarrow}_{i,j} = \bar{\mathcal{Z}}^1_{i,j}(Z^+_iZ^+_j) + \bar{\mathcal{Z}}^0_{i,j}(XX)^+_{i,j} \tag{104}$$

where $\bar{\mathcal{Z}}^k_{i,j}$ denotes that exactly k excitations are detected when the measurement $Z^{\otimes(n-2)}$ is performed on all but the ith and jth qubits; see **Figure 8**. The corresponding spectral gap reads

$$\nu(\Omega^{\leftrightarrow}) = \begin{cases} \frac{1}{3} & \text{for } n=3,\\ \frac{1}{n-1} & \text{for } n\geq 4 \end{cases} \tag{105}$$

Further, the LOCC verification strategy in Equation (103) also inspires an efficient local verification strategy without communication. The basic idea is to replace the LOCC test $\Omega^{\rightarrow}_{i,j}$ with two local tests, performed randomly with equal probability. In the test

$$\mathcal{Z}^1 = \sum_{i=1}^{n}|0\rangle\langle0|^{\otimes(i-1)}\otimes|1\rangle\langle1|\otimes|0\rangle\langle0|^{\otimes(n-i)} \tag{106}$$

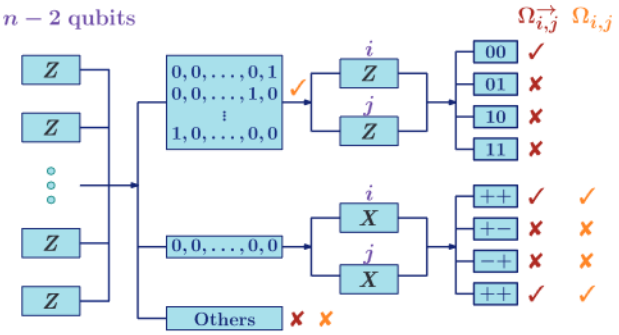


Figure 8. $\Omega^{\rightarrow}_{i,j}$ and $\Omega_{i,j}$ for the verification of $|W_n\rangle$. For both $\Omega^{\rightarrow}_{i,j}$ and $\Omega_{i,j}$, the measurement $Z^{\otimes(n-2)}$ is performed on all but the ith and jth qubits. The difference is that for $\Omega_{i,j}$ the measurement on the ith and jth qubits is always $X\otimes X$, but for $\Omega^{\rightarrow}_{i,j}$ the measurement on the ith and jth qubits depends on the measurement outcome on the previous $n-2$ qubits.

measurement $Z^{\otimes n}$ is performed; the test is passed if the excitation is detected exactly once. In the test

$$\Omega_{i,j} = \bar{\mathcal{Z}}^1_{i,j}(\mathbb{1}\mathbb{1})_{ij} + \bar{\mathcal{Z}}^0_{i,j}(XX)^+_{i,j} \tag{107}$$

measurement $X\otimes X$ is performed on the ith and jth qubit, and measurement $Z^{\otimes(n-2)}$ is performed on the other $n-2$ qubits; the test is passed if one excitation is detected for measurement $Z^{\otimes(n-2)}$, or no excitation is detected and the outcomes for the ith and jth qubits coincide; see Figure 8. The resulting local verification operator reads

$$\Omega = \frac{1}{2}\mathcal{Z}^1 + \frac{1}{n(n-1)}\sum_{i<j}\Omega_{i,j} \tag{108}$$

and the spectral gap reads

$$\nu(\Omega) = \begin{cases} \frac{1}{4} & \text{for } n=3,\\ \frac{1}{2(n-1)} & \text{for } n\geq 4 \end{cases} \tag{109}$$

which is at most two times worse than the corresponding LOCC strategy. Remarkably, any one-round LOCC verification strategy can be transformed to a local strategy, in which the efficiency loss depends on the so-called branch number.[109]

The verification strategy in Equation (103) can be directly generalized for verifying Dicke states[112]

$$|D^k_n\rangle = \binom{n}{k}^{-\frac{1}{2}}\sum_j \mathcal{P}_j\left\{|1\rangle^{\otimes k}\otimes|0\rangle^{\otimes(n-k)}\right\} \tag{110}$$

where $\sum_j \mathcal{P}_j\{\cdot\}$ denotes the sum over all possible permutations. Remarkably, the verification efficiency for Dicke states ($k\neq 0$ or n) is equal to that for W states, which is independent of the number of excitations k. This makes the protocol much more efficient than the previously known methods.

In ref. [113], Li et al. proposed an alternative LOCC verification strategy for W states, which consists of measuring $Z^{\otimes(n-1)}$ or $X^{\otimes(n-1)}$ on the first $n-1$ qubits and verifying the

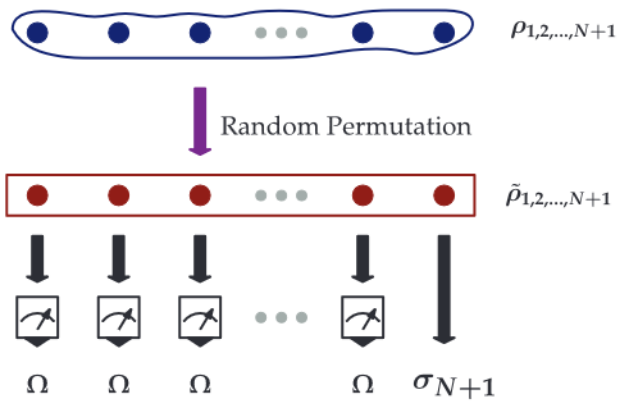


Figure 9. In an adversarial scenario, the device is controlled by a potentially malicious adversary and can produce an arbitrarily correlated or even entangled state $\rho_{1,2,\ldots,N+1}$ on $\mathcal{H}^{\otimes(N+1)}$. The verifier first performs a random permutation to make the state permutation-invariant, that is, $\tilde{\rho}_{1,2,\ldots,N+1} = \frac{1}{(N+1)!}\sum_{\pi\in S_{N+1}} \rho_{\pi(1,2,\ldots,N+1)}$, where S_{N+1} is the symmetric group. Then, the QSV strategy Ω is performed on each of the first N subsystems and the goal is to estimate the fidelity of the post-measurement state on the $(N+1)$th subsystem σ_{N+1}, given that all the first N subsystems pass the test.

post-measurement state on the nth qubit. An advantage of this strategy is that when $n \gg 1$

$$\nu(\Omega^{\rightarrow}) \approx \begin{cases} \frac{0.342}{\sqrt{n}} & \text{for } n \text{ is odd,} \\ \frac{0.287}{\sqrt{n}} & \text{for } n \text{ is even} \end{cases} \tag{111}$$

which is of $\mathcal{O}(1/\sqrt{n})$ and asymptotically better than Equation (105). The efficiency can also be further improved by about four times when some symmetrization process is employed.[113]

4. Generalizations and Related Protocols

4.1. The Adversarial Scenario

In the previous sections, the states $\sigma_1, \sigma_2, \ldots, \sigma_N$ generated by the quantum devices are always assumed to be independent. In refs. [114, 115], Zhu and Hayashi proposed an adversarial scenario, which makes QSV also applicable to the case of nonindependent sources.

In the adversarial scenario, the device is controlled by a potentially malicious adversary and can produce an arbitrarily correlated or even entangled state ρ on $\mathcal{H}^{\otimes(N+1)}$, as illustrated in **Figure 9**. To verify the state produced in a certain run, the verifier randomly chooses N subsystems from $\mathcal{H}^{\otimes(N+1)}$ to perform the tests. This is also equivalent to assume that ρ is permutation-invariant on $\mathcal{H}^{\otimes(N+1)}$ and the first N subsystems are chosen. For convenience, we will employ the latter description in the following. Now, the QSV strategy Ω is performed on each of the first N subsystems and the goal is to estimate the fidelity of the (averaged) post-measurement state on the $(N+1)$th subsystem, given that all the first N subsystems pass the test. That is the fidelity of the state

$$\sigma_{N+1} = \frac{1}{p_\rho}\mathrm{Tr}_{1,2,\ldots,N}\left[\left(\Omega^{\otimes N}\otimes \mathbb{1}\right)\rho\right] \tag{112}$$

with respect to the target state $|\psi\rangle$, where

$$p_\rho = \mathrm{Tr}\left[\left(\Omega^{\otimes N}\otimes \mathbb{1}\right)\rho\right] \tag{113}$$

is the probability that the tests are passed. Then, the figure of merit is defined as

$$F(N,\delta,\Omega) := \min_\rho\left\{\langle\psi|\sigma_{N+1}|\psi\rangle \;\middle|\; p_\rho \geq \delta\right\} \tag{114}$$

which represents the minimum fidelity with the confidence $1-\delta$. More precisely, the null hypothesis, $\langle\psi|\sigma_{N+1}|\psi\rangle < F(N,\delta,\Omega)$, is rejected with the confidence $1-\delta$, given that all the first N subsystems pass the test. Correspondingly, to achieve a confidence $1-\delta$, the number of tests needed is

$$N(\varepsilon,\delta,\Omega) = \min\left\{N \geq 1 \;\middle|\; F(N,\delta,\Omega) \geq 1-\varepsilon\right\} \tag{115}$$

In the adversarial scenario, the so-called homogeneous strategy plays a crucial role, as it is the most efficient among all verification strategies with a given spectral gap. A verification strategy Ω is called homogeneous if it is of the form

$$\Omega = |\psi\rangle\langle\psi| + \lambda\left(\mathbb{1} - |\psi\rangle\langle\psi|\right) \tag{116}$$

where $|\psi\rangle$ is the target state. The spectral gap is $\nu(\Omega) = 1-\lambda$ for the homogeneous strategy. The rigorous analysis of $F(N,\delta,\Omega)$ and $N(\varepsilon,\delta,\Omega)$ is complicated even for the homogeneous strategies. An important difference between the adversarial and nonadversarial scenario is that the optimal strategy is not achieved when $\lambda = 0$. In particular, in the high precision limit $(\varepsilon,\delta \to 0)$,

$$N(\varepsilon,\delta,\Omega) \approx \left(\lambda\ln\lambda^{-1}\right)^{-1}\varepsilon^{-1}\ln\delta^{-1} \tag{117}$$

which is of the same scaling with respect to ε and δ as the nonadversarial scenario in Equation (16). However, the minimum number of tests needed is achieved when $\lambda = 1/\mathrm{e}$.

For the general verification strategy Ω, the efficiency of the adversarial scenario depends not only on the second largest eigenvalue λ, but also the smallest eigenvalue τ of Ω. In the high precision limit $(\varepsilon,\delta \to 0)$,

$$N(\varepsilon,\delta,\Omega) \approx h\varepsilon^{-1}\ln\delta^{-1} \tag{118}$$

where the overhead h reads

$$h = \max\left\{\left(\lambda\ln\lambda^{-1}\right)^{-1}, \left(\tau\ln\tau^{-1}\right)^{-1}\right\} \tag{119}$$

When the smallest eigenvalue τ is equal or close to zero, the adversarial QSV is not efficient in general. Thus, additional methods are proposed to improve the efficiency by adding the trivial test[114,115] or other extra terms[101] to Ω.

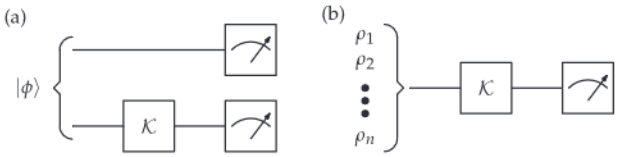


Figure 10. There are two methods for verifying the quantum process $\mathcal{K}$. a) Ancilla-assisted QPV: by taking advantage of the Choi–Jamiołkowski isomorphism, the verification of K is transformed to the verification of the Choi state $\rho_{\mathcal{K}}$; b) Prepare-and-measure QPV: the verifier randomly chooses an input state ρ_ℓ and tests the output state with a corresponding measurement $\{N_\ell, \mathbb{1} - N_\ell\}$.

At last, we would like to note that for the adversarial scenario only the unit frequency, that is, all the previous N states pass the test, has been considered. How to generalize the problem to the non-unit frequency, like in the case of QFE, is still an open problem. This is also of vital importance for the practical applications of the adversarial scenario.

4.2. Quantum Process Verification

There are two main strategies for quantum process verification (QPV); see **Figure 10**. The first one is based on the Choi–Jamiołkowski isomorphism[116–118] between processes and states, which allows to relate QPV with QSV. The second strategy is a prepare-and-measure scheme, where certain input states are subjected to the process and then verified.

We start our discussion with the first class of strategies.[119–121] Consider the (unnormalized) maximally entangled bipartite state $|\phi\rangle = \sum_{\alpha=1}^{d} |\alpha\rangle_A |\alpha\rangle_S$ between a quantum system $\mathcal{H}_S$ and an ancilla system $\mathcal{H}_A$. The Choi-Jamiołkowski isomorphism J is defined as

$$J(\mathcal{E}) := \mathrm{id} \otimes \mathcal{E}\big(|\phi\rangle\langle\phi|\big) = \sum_{\alpha,\beta=1}^{d} |\alpha\rangle\langle\beta| \otimes \mathcal{E}\big(|\alpha\rangle\langle\beta|\big) \tag{120}$$

where $\mathcal{E} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is a map (quantum process) on the system $\mathcal{H}_S$ only, and $J(\mathcal{E}) \in \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is usually called the Choi matrix of the process $\mathcal{E}$. Conversely, $\mathcal{E}$ can also be obtained from $J(\mathcal{E})$ as

$$\mathcal{E}(\rho) = \mathrm{Tr}_A\Big[\Big(\rho^T \otimes \mathbb{1}\Big) J(\mathcal{E})\Big] \tag{121}$$

Tomographically, Equation (121) implies that once the Choi matrix $J(\mathcal{E})$ is determined, all the information of the process $\mathcal{E}$ is known. Thus, one can verify a quantum process $\mathcal{K}$ indirectly by verifying the corresponding Choi state

$$\rho_{\mathcal{K}} := \frac{J(\mathcal{K})}{\mathrm{Tr}[J(\mathcal{K})]} \tag{122}$$

instead. Especially, when $\rho_{\mathcal{K}}$ is pure (e.g., if $\mathcal{E}$ is unitary), one can apply the QSV protocols for verifying $\mathcal{K}$.

For simplicity, we only consider the case when $\mathcal{K}$ is a unitary gate U, that is, the verification of quantum gates or quantum circuits. In general, $\mathcal{E}$ is not necessary to be trace-preserving, which makes it possible to deal with post-selection or particle losses.[119]

Suppose that a quantum device is promised to perform a unitary gate U, but a quantum process $\mathcal{E}$ is performed in practice. We want to use the hypothesis testing method to verify this claim with high confidence. The entanglement gate fidelity

$$F_e(\mathcal{E}, U) := F(\rho_{\mathcal{E}}, \rho_U) = \mathrm{Tr}(\rho_{\mathcal{E}} \rho_U) \tag{123}$$

is employed as a benchmark, which is only different from the average gate fidelity by an affine function.[122]

Due to the Choi–Jamiołkowski isomorphism, one can transform the verification of U to the verification of the pure Choi state $\rho_U = |\psi_U\rangle\langle\psi_U|$, where

$$|\psi_U\rangle = \frac{1}{\sqrt{d}} \sum_{\alpha=1}^{d} |\alpha\rangle \otimes U|\alpha\rangle \tag{124}$$

This method is called the ancilla-assisted QPV. As ρ_U is maximally entangled, one can verify ρ_U with the spectral gap $\nu(\Omega) = d/(d+1)$ as shown in Equation (38). In actual experiments, one usually has more restrictions to the allowed measurements, for example, each party should be measured locally for verifying the multi-qubit gates. In general, the worst-case failure probability in each run is always bounded by

$$\max_{F(\rho_{\mathcal{E}}, \rho_U) \le 1-\epsilon} \mathrm{Tr}(\Omega \rho_{\mathcal{E}}) \le 1 - \epsilon\nu(\Omega) \tag{125}$$

Correspondingly, the confidence $1 - \delta$ is still bounded by Equation (14) or Equation (22).

The second class of strategies is the prepare-and-measure QPV, which does not require an additional ancilla system or maximally entangled input states. In the prepare-and-measure QPV, the verifier randomly chooses an input state ρ_ℓ with probability p_ℓ and test the output state with the measurement $\{N_\ell, \mathbb{1} - N_\ell\}$. If the measurement outcome is N_ℓ, then we say the channel $\mathcal{E}$ passes the test; otherwise we say $\mathcal{E}$ fails the test. Similar to QSV, we require that the target gate U always passes the test, that is,

$$\mathrm{Tr}(U \rho_\ell U^\dagger N_\ell) = 1 \tag{126}$$

For convenience, we denote the prepare-and-measure strategy as

$$\Xi = \sum_\ell p_\ell \rho_\ell^T \otimes N_\ell \tag{127}$$

Then in each run the worst-case failure probability is given by

$$\max_{F_e(\mathcal{E}, U) \le 1-\epsilon} \sum_\ell p_\ell \,\mathrm{Tr}[\mathcal{E}(\rho_\ell) N_\ell] = \max_{F_e(\mathcal{E}, U) \le 1-\epsilon} \mathrm{Tr}[\Xi J(\mathcal{E})] \tag{128}$$

A remarkable result on QPV is that every one-way LOCC QSV strategy for the Choi state ρ_U can be transformed to a prepare-and-measure QPV strategy.[119] According to Equation (73), the one-way adaptive QSV strategy takes on the general form

$$\Omega^{\rightarrow} = \sum_\ell M_\ell \otimes N_\ell \tag{129}$$

such that $\{M_\ell\}_\ell$ is a POVM on the ancilla system $\mathcal{H}_A$ and $\{N_\ell, \mathbb{1} - N_\ell\}$ is a pass or fail test on the system $\mathcal{H}_S$ which depends on the measurement outcome of $\{M_\ell\}_\ell$. Now, $\Omega^{\rightarrow}$ can be converted to a

prepare-and-measure QPV strategy of the form in Equation (127) by letting

$$p_\ell = \frac{\mathrm{Tr}(M_\ell)}{d},\ \rho_\ell = \frac{M_\ell^T}{\mathrm{Tr}(M_\ell)},\ N_\ell = N_\ell \tag{130}$$

and the failure probability defined in Equation (128) is bounded by

$$\max_{F_e(\mathcal{E},U)\le 1-\varepsilon} \mathrm{Tr}[\Xi J(\mathcal{E})] \le 1 - \varepsilon\nu(\Omega^{\to}) \tag{131}$$

Again, the confidence $1-\delta$ is bounded by Equation (14) or Equation (22). By taking advantage of the corresponding QSV strategies in Section 3, many widely-used quantum gates can be efficiently verified, including general single qubit and qudit gates, Clifford gates, $C^{(n-1)}Z$ and $C^{(n-1)}X$ gates, as well as CSWAP gates.[119–121] The adversarial scenario for quantum gate verification was also considered in ref. [121].

Using photonic platforms, the first experimental verification of quantum gates including a two-qubit controlled-not gate and a three-qubit Toffoli gate using only local state preparations and measurements was reported in ref. [123]. The experimental results show that, by using only 1600 and 2600 measurements on average, a 95% confidence can be drawn that the implemented controlled-not gate and Toffoli gate have fidelities at least 99% and 97%, respectively. This is substantially more efficient than quantum process tomography, thus successfully demonstrated the superior low sample complexity and experimental feasibility of quantum process verification. See also ref. [124] for a proof-of-principle optical demonstration of quantum gate verification of two general single-qubit gates.

4.3. Quantum Entanglement Verification

The QSV protocol, more precisely, the QFE protocol is also closely related to the statistical entanglement verification method proposed by Dimić and Dakić and by Saggio et al. in refs. [62, 63]; see also the very recent review paper.[34] In their method, the verifier also perform a set of random pass or fail tests $\{\Omega_\ell, \mathbb{1}-\Omega_\ell\}$, such that no separable state can pass the test with probability higher than q_s. Similar to Equation (22), if in actual experiments the frequency of pass instances f is larger than q_s, the verifier can conclude the state is entangled with the confidence $1-\delta$, where

$$\delta \le \mathrm{e}^{-D[f\|q_s]N} \tag{132}$$

and $D[\cdot\|\cdot]$ is the Kullback–Leibler divergence.

To see the connection to QFE, let us consider the fidelity-based entanglement witness[20] for bipartite states. This is a limited class of witness operators[64,65] but widely used in real experiments. According to ref. [65], we can just consider the witness operator

$$W = \frac{1}{d}\mathbb{1}\otimes\mathbb{1} - |\psi\rangle\langle\psi| \tag{133}$$

where $|\psi\rangle$ is some maximally entangled state. This implies that for a quantum state σ

$$\sigma \in \mathrm{SEP} \quad \Rightarrow \quad \langle\psi|\sigma|\psi\rangle \le \frac{1}{d} \tag{134}$$

which essentially transforms an entanglement witness problem to a fidelity estimation problem. Now, suppose that we use the optimal QSV strategy Ω in Equation (37) or (39) for the maximally entangled state, where the spectral gap is $\nu(\Omega) = d/(d+1)$. Then, Equations (13) and (134) imply that

$$\max_{\sigma\in\mathrm{SEP}} \mathrm{Tr}(\Omega\sigma) \le 1 - \left(1-\frac{1}{d}\right)\nu(\Omega) = \frac{2}{d+1} \tag{135}$$

Similar to Equation (22), the null hypothesis that all the produced states $\sigma_1, \sigma_2, \ldots, \sigma_N$ are separable can be rejected with the confidence $1-\delta$[62,63] with

$$\delta \le \mathrm{e}^{-D\left[f\left\|\frac{2}{d+1}\right.\right]N} \tag{136}$$

where f is the frequency of the pass instances. Actually, the value $1-\delta$ can also be interpreted as the confidence of the presence of entanglement in the averaged state

$$\bar{\sigma} = \frac{1}{N}\sum_{k=1}^{N}\sigma_k \tag{137}$$

The method can be directly generalized to detect (genuine) multi-partite entanglement,[62,63] as the fidelity-based entanglement witness of the form in Equation (134) also exists for multipartite states.[20]

More generally, in ref. [63], Saggio et al. also showed that this method can in principle go beyond the fidelity-based entanglement witness. The basic idea is that any entanglement witness can be decomposed into local operators, which can then be measured probabilistically. This leads to a general method for transforming any entanglement witness operator to a statistical entanglement verification strategy.

Then, the experimental verification of entanglement in a photonic six-qubit cluster state was presented in ref. [63]. It showed that the presence of entanglement can be certified with at least 99.74% confidence by using 20 copies of the quantum state. Additionally, genuine six-qubit entanglement can be verified with at least 99% confidence by using 112 copies of the state. These results make it possible to apply the method to verify large-scale quantum devices.

4.4. Emerging Research Directions

Apart from the aforementioned generalizations there are also other emerging research directions that further extend the applicability and efficiency of QSV protocols. Here, we mention only a few of them.

As proved in ref. [29], the QSV strategy satisfying Equation (11), that is, the zero type II error, is optimal in the asymptotic

limit. Roughly speaking, this is because the Kullback–Leibler divergence satisfies that

$$D(f\|f-\varepsilon)=\begin{cases}\mathcal{O}(\varepsilon) & f=1,\\ \mathcal{O}(\varepsilon^2) & 0<f<1\end{cases} \tag{138}$$

when $\varepsilon \to 0$, and Equation (11) is necessary to ensure that the frequency of pass instances is $f = 1$. This advantage, however, is not robust as it exists only in the idealized situation when the fidelity of the produced states is exactly one. Thus, in practice, it is interesting to study whether the efficiency of the QFE protocol can be improved by relaxing the constraint in Equation (11). In ref. [125], the authors investigate a related problem under the QSV framework, that is, with the hypotheses in Equations (8) and (9).[126] Instead of choosing zero Type II error $\langle\psi|\Omega|\psi\rangle = 1$, the authors consider the bounded Type II error,

$$\langle\psi|\Omega|\psi\rangle = 1-\beta_0 \tag{139}$$

under which the minimization of type I error is studied.

In ref. [127], an alternative implementation of the QSV protocol is proposed by using so-called quantum nondemolition (QND) measurements, which are the type of measurements that leave the post-measurement quantum states undestroyed, thus allowing repeated or sequential measurements. The protocol fully explores the use of sequentially constructed QND measurements for state verification instead of the probabilistic construction in standard QSV strategies. Under such a design, not only the target states can be preserved, but also the protocol turns to be equivalent to the optimal global strategy in terms of the verification efficiency. Moreover, the protocol is robust in the sense that the order of the sequential measurements can be arbitrarily constructed which is rather friendly to experimental implementations. Very recently, Miguel-Ramiro et al. showed with collective local measurements, one can also significantly reduce the destruction of the verified states.[128]

In ref. [85], the authors generalize QSV to the device-independent scenario. Their method is based on the self-testing properties of entangled quantum states.[129,130] It is shown that a quantum state can be device-independently verified if there exists a robust self-testing protocol for it. Moreover, a systematic method is proposed to construct device-independent QSV protocols and the confidence is derived from the robustness of the corresponding self-testing protocol. In the same paper, the authors also consider the device-independent adversarial scenario. Compared with the device-dependent adversarial scenario in Section 4, their method has the advantage that more than one remaining state can be certified, while the disadvantage is that the method is only applicable to independent copies.

5. Conclusions and Outlooks

The framework of hypothesis testing is powerful and allows to analyze experimental data in an efficient manner. The methods for quantum state verification described in this review article are therefore important to analyze current and future experiments, where only a limited amount of data is available. Even more, although the considered situation may seem artificial at first sight, the insights from optimal quantum state verification protocols also turn out to be useful for other tasks, such as fidelity estimation or entanglement verification in a realistic scenario. Consequently, there are several open problems where the presented results may be useful or may be extended:

1) So far, we considered only discrete systems, mainly multi-qubit systems. It is highly desirable to develop a similar theory also for continuous-variable systems or hybrid systems, where some parties are finite-dimensional, while others are not. While finishing this review, first results in this direction have been published.[48,49]
2) The current approach to QSV is designed for the verification of pure states. For more realistic scenarios an extension to the case of mixed states is needed. For instance, how can one estimate mixed state fidelities in an optimized manner? The known results show that this problem is complicated even if entangled measurements are allowed.[131,132]
3) The scheme of QSV can be seen as a characterization of a quantum source, where one asks whether the source produces always the same quantum state. For characterizing sources, however, many other questions may be asked, for example, concerning the stability of the source or potential drifts.[41] Developing a full theory for these effects from a rigorous statistical viewpoint is highly desirable.
4) In the current literature on QSV one typically considers the number of copies N to be fixed. In a realistic experiment one may, however, keep it flexible, and abort an experiment if a desired confidence has been reached. This leads to the notion of sequential tests, which have recently been attracted some interest in the quantum information community.[43,44]
5) The presented protocols of QSV bear some similarity with other protocols for quantum information processing. For instance, the fact that the desired objects pass with certainty some test also arises in entanglement distillation protocols[133] and Hardy-type tests of non-locality.[134] It may be fruitful to formalize this similarity.
6) Finally, recently the notion of quantum algorithmic measurements has been introduced,[135] where the measuring party has coherent access to a quantum computer. This extended notion of measurements has the potential to lead to radically novel and enhanced strategies for QSV.

In summary, we believe that the topic of quantum state verification is just emerging and is likely to have a fruitful impact on other topics in quantum information processing in the future.

Acknowledgements

The authors thank Geng Chen, Rui Han, Yun-Guang Han, Masahito Hayashi, Qiongyi He, Zhibo Hou, Martin Kliesch, Yinfei Li, Zihao Li, Ye-Chao Liu, Ramon Muñoz Tapia, Gael Sentís, Géza Tóth, Kun Wang, Guo-Yong Xiang, Rui-Qi Zhang, Xiangdong Zhang, and Huangjun Zhu for discussions on quantum state verification. This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, project numbers 447948357 and 440958198), the Sino-German Center for Research Promotion (Project M-0294), and the ERC (Consolidator Grant 683107/TempoQ). J.S. acknowledges support by the National Natural Science Foundation of China (Grants No. 12175014 and No. 11805010).

Open Access funding enabled and organized by Projekt DEAL.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

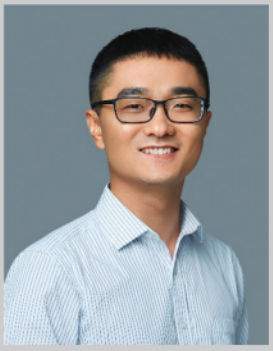
fidelity estimation, hypothesis testing, quantum certification and benchmarking, quantum state verification

Received: September 29, 2021
Revised: January 22, 2022
Published online: March 18, 2022

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, *Phys. Rev. Lett.* **1993**, *70*, 1895.
[2] C. H. Bennett, G. Brassard, in *Proc. IEEE Int. Conf. Comp., Syst. Signal Proc.*, IEEE, Piscataway, NJ **1984**, pp. 175–179.
[3] A. K. Ekert, *Phys. Rev. Lett.* **1991**, *67*, 661.
[4] A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, *Acta Phys. Pol., A* **2002**, *101*, 357.
[5] G. L. Long, X. S. Liu, *Phys. Rev. A* **2002**, *65*, 032302.
[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, *Adv. Opt. Photonics* **2020**, *12*, 1012.
[7] X.-F. Wang, X.-J. Sun, Y.-X. Liu, W. Wang, B.-X. Kan, P. Dong, L.-L. Zhao, *Quantum Eng.* **2021**, *3*, e73.
[8] R. Raussendorf, H. J. Briegel, *Phys. Rev. Lett.* **2001**, *86*, 5188.
[9] R. Raussendorf, D. E. Browne, H. J. Briegel, *Phys. Rev. A* **2003**, *68*, 022312.
[10] D. T. Smithey, M. Beck, M. G. Raymer, A. Faridani, *Phys. Rev. Lett.* **1993**, *70*, 1244.
[11] D. F. V. James, P. G. Kwiat, W. J. Munro, A. G. White, *Phys. Rev. A* **2001**, *64*, 052312.
[12] *Quantum State Estimation*, *Lecture Notes in Physics* (Eds: M. Paris, J. Řeháček), Vol. *649*, Springer, Heidelberg **2004**.
[13] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, R. Blatt, *Nature* **2005**, *438*, 643.
[14] J. Shang, Z. Zhang, H. K. Ng, *Phys. Rev. A* **2017**, *95*, 062336.
[15] R. Blume-Kohout, *New J. Phys.* **2010**, *12*, 043034.
[16] J. Shang, H. K. Ng, A. Sehrawat, X. Li, B.-G. Englert, *New J. Phys.* **2013**, *15*, 123026.
[17] C. Schwemmer, L. Knips, D. Richart, H. Weinfurter, T. Moroder, M. Kleinmann, O. Gühne, *Phys. Rev. Lett.* **2015**, *114*, 080403.
[18] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, E. Kashefi, *Nat. Rev. Phys.* **2020**, *2*, 382.
[19] M. Kliesch, I. Roth, *PRX Quantum* **2021**, *2*, 010201.
[20] O. Gühne, G. Tóth, *Phys. Rep.* **2009**, *474*, 1.
[21] N. Friis, G. Vitagliano, M. Malik, M. Huber, *Nat. Rev. Phys.* **2019**, *1*, 72.
[22] G. Chen, W.-H. Zhang, P. Yin, C.-F. Li, G.-C. Guo, *Fundam. Res.* **2021**, *1*, 27.
[23] N. Kiesel, C. Schmid, G. Tóth, E. Solano, H. Weinfurter, *Phys. Rev. Lett.* **2007**, *98*, 063604.
[24] C. Kurz, M. Schug, P. Eich, J. Huwer, P. Müller, J. Eschner, *Nat. Commun.* **2014**, *5*, 5527.
[25] C. Song, K. Xu, W. Liu, C.-P. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, J.-W. Pan, *Phys. Rev. Lett.* **2017**, *119*, 180511.
[26] S. T. Flammia, Y.-K. Liu, *Phys. Rev. Lett.* **2011**, *106*, 230501.
[27] O. Gühne, C.-Y. Lu, W.-B. Gao, J.-W. Pan, *Phys. Rev. A* **2007**, *76*, 030305.
[28] A. Seshadri, M. Ringbauer, R. Blatt, T. Monz, S. Becker, arXiv:2112.07925, **2021**.
[29] S. Pallister, N. Linden, A. Montanaro, *Phys. Rev. Lett.* **2018**, *120*, 170502.
[30] M. Hayashi, K. Matsumoto, Y. Tsuda, *J. Phys. A: Math. Gen.* **2006**, *39*, 14427.
[31] M. Hayashi, *New J. Phys.* **2009**, *11*, 043028.
[32] S. M. Barnett, S. Croke, *Adv. Opt. Photonics* **2009**, *1*, 238.
[33] J. Bae, L.-C. Kwek, *J. Phys. A: Math. Theor.* **2015**, *48*, 083001.
[34] J. Morris, V. Saggio, A. Gocanin, B. Dakić, arXiv:2109.03860, **2021**.
[35] E. Bagan, M. Baig, R. Muñoz Tapia, *Phys. Rev. Lett.* **2002**, *89*, 277904.
[36] J. Audretsch, L. Diósi, T. Konrad, *Phys. Rev. A* **2003**, *68*, 034302.
[37] E. Bagan, M. Baig, R. Muñoz Tapia, A. Rodriguez, *Phys. Rev. A* **2004**, *69*, 010304.
[38] J. I. de Vicente, J. Calsamiglia, R. Muñoz Tapia, E. Bagan, *Phys. Rev. A* **2010**, *81*, 012332.
[39] C. Ferrie, R. Blume-Kohout, *AIP Conf. Proc.* **2012**, *1443*, 14.
[40] G. Sentís, E. Bagan, J. Calsamiglia, G. Chiribella, R. Muñoz Tapia, *Phys. Rev. Lett.* **2016**, *117*, 150502.
[41] T. Proctor, M. Revelle, E. Nielsen, K. Rudinger, D. Lobser, P. Maunz, R. Blume-Kohout, K. Young, *Nat. Commun.* **2020**, *11*, 5396.
[42] W. Laskowski, C. Schwemmer, D. Richart, L. Knips, T. Paterek, H. Weinfurter, *Phys. Rev. A* **2013**, *88*, 022327.
[43] N. Milazzo, D. Braun, O. Giraud, *Phys. Rev. A* **2019**, *100*, 012328.
[44] E. Martínez Vargas, C. Hirche, G. Sentís, M. Skotiniotis, M. Carrizo, R. Muñoz Tapia, J. Calsamiglia, *Phys. Rev. Lett.* **2021**, *126*, 180502.
[45] G. Chai, D. Li, Z. Cao, M. Zhang, P. Huang, G. Zeng, *Quantum Eng.* **2020**, *2*, e37.
[46] X.-M. Hu, C. Zhang, C.-J. Zhang, B.-H. Liu, Y.-F. Huang, Y.-J. Han, C.-F. Li, G.-C. Guo, *Quantum Eng.* **2019**, *1*, e13.
[47] D. Cavalcanti, P. Skrzypczyk, I. Šupić, *Phys. Rev. Lett.* **2017**, *119*, 110501.
[48] Y.-D. Wu, G. Bai, G. Chiribella, N. Liu, *Phys. Rev. Lett.* **2021**, *126*, 240503.
[49] Y.-C. Liu, J. Shang, X. Zhang, *Phys. Rev. Res.* **2021**, *3*, L042004.
[50] J. A. Rice, *Mathematical Statistics and Data Analysis*, Cengage Learning, Boston, MA **2006**.
[51] J. Neyman, E. S. Pearson, *Philos. Trans. R. Soc. A* **1933**, *231*, 289.
[52] W. Hoeffding, *J. Am. Stat. Assoc.* **1963**, *58*, 13.
[53] S. Bernstein, *Ann. Sci. Inst. Sav. Ukraine, Sect. Math* **1924**, *1*, 38.
[54] F. P. Cantelli, in *Atti del Congresso Internazionale dei Matematici: Bologna del 3 al 10 de settembre di 1928*. **1929**, 47–60.
[55] C. McDiarmid, *Surveys in Combinatorics*, Cambridge University Press, Cambridge **1989**, p. 148.
[56] T. Moroder, M. Kleinmann, P. Schindler, T. Monz, O. Gühne, R. Blatt, *Phys. Rev. Lett.* **2013**, *110*, 180401.
[57] T. Sugiyama, P. S. Turner, M. Murao, *Phys. Rev. Lett.* **2013**, *111*, 160406.
[58] L. Knips, C. Schwemmer, N. Klein, J. Reuter, G. Tóth, H. Weinfurter, How long does it take to obtain a physical density matrix?, arXiv:1512.06866, **2015**.
[59] T. Sugiyama, *Phys. Rev. A* **2015**, *91*, 042126.
[60] A. Ketterer, S. Imai, N. Wyderka, O. Gühne, arXiv:2012.12176, **2021**.
[61] X.-D. Yu, J. Shang, O. Gühne, *npj Quantum Inf.* **2019**, *5*, 112.
[62] A. Dimić, B. Dakić, *npj Quantum Inf.* **2018**, *4*, 11.
[63] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, *Nat. Phys.* **2019**, *15*, 935.
[64] M. Weilenmann, B. Dive, D. Trillo, E. A. Aguilar, M. Navascués, *Phys. Rev. Lett.* **2020**, *124*, 200502, Erratum: *Phys. Rev. Lett.* **2020**, *125*, 159903(E).
[65] O. Gühne, Y. Mao, X.-D. Yu, *Phys. Rev. Lett.* **2021**, *126*, 140503.
[66] G. Tóth, O. Gühne, *Phys. Rev. Lett.* **2005**, *94*, 060501.

[67] G. Tóth, O. Gühne, *Phys. Rev. A* **2005**, *72*, 022340.
[68] G. Tóth, *J. Opt. Soc. Am. B* **2007**, *24*, 275.
[69] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, H. Weinfurter, *Phys. Rev. Lett.* **2010**, *105*, 250403.
[70] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge **2000**.
[71] K. Wang, M. Hayashi, *Phys. Rev. A* **2019**, *100*, 032315.
[72] R. F. Werner, *Phys. Rev. A* **1989**, *40*, 4277.
[73] H. Zhu, M. Hayashi, *Phys. Rev. A* **2019**, *99*, 052346.
[74] B. Simon, *Convexity: An Analytic Viewpoint*, Cambridge University Press, Cambridge **2011**.
[75] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, *Int. J. Quantum Inf.* **2010**, *08*, 535.
[76] G. Zauner, *Int. J. Quantum Inf.* **2011**, *09*, 445.
[77] A. Roy, A. J. Scott, *J. Math. Phys.* **2007**, *48*, 072110.
[78] D. Gottesman, arXiv:quant-ph/9705052, **1997**.
[79] N. D. Mermin, *Phys. Rev. Lett.* **1990**, *65*, 1838.
[80] O. Gühne, G. Tóth, P. Hyllus, H. J. Briegel, *Phys. Rev. Lett.* **2005**, *95*, 120405.
[81] H. Zhu, M. Hayashi, *Phys. Rev. Appl.* **2019**, *12*, 054047.
[82] Z. Li, Y.-G. Han, H. Zhu, *Phys. Rev. Appl.* **2020**, *13*, 054002.
[83] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, I. Kerenidis, *Phys. Rev. Lett.* **2012**, *108*, 260502.
[84] Y.-G. Han, Z. Li, Y. Wang, H. Zhu, *npj Quantum Inf.* **2021**, *7*, 164.
[85] A. Gocanin, I. Šupić, B. Dakić, *PRX Quantum* **2022**, *3*, 010317.
[86] W. Dür, H.-J. Briegel, *Phys. Rev. Lett.* **2004**, *92*, 180403.
[87] M. Hein, J. Eisert, H. J. Briegel, *Phys. Rev. A* **2004**, *69*, 062311.
[88] M. Van den Nest, J. Dehaene, B. De Moor, *Phys. Rev. A* **2004**, *69*, 022316.
[89] M. Grassl, A. Klappenecker, M. Rotteler, in *Proc. IEEE Int. Symp. Information Theory*, IEEE, Piscataway, NJ **2002**, p. 45.
[90] D. Schlingemann, *Quantum Inf. Comput.* **2002**, *2*, 307.
[91] E. R. Scheinerman, D. H. Ullman, *Fractional Graph Theory: A Rational Approach to the Theory of Graphs*, Wiley, New York **1997**.
[92] R. Qu, J. Wang, Z.-S. Li, Y.-R. Bao, *Phys. Rev. A* **2013**, *87*, 022311.
[93] M. Rossi, M. Huber, D. Bruß, C. Macchiavello, *New J. Phys.* **2013**, *15*, 113022.
[94] O. Gühne, M. Cuquet, F. E. S. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, C. Macchiavello, *J. Phys. A: Math. Theor.* **2014**, *47*, 335303.
[95] N. Dangniam, Y.-G. Han, H. Zhu, *Phys. Rev. Res.* **2020**, *2*, 043323.
[96] T. Morimae, Y. Takeuchi, M. Hayashi, *Phys. Rev. A* **2017**, *96*, 062321.
[97] M. Hayashi, M. Hajdušek, *Phys. Rev. A* **2018**, *97*, 052308.
[98] Y. Takeuchi, T. Morimae, *Phys. Rev. X* **2018**, *8*, 021060.
[99] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, J. F. Fitzsimons, *npj Quantum Inf.* **2019**, *5*, 27.
[100] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, G. Chen, C.-F. Li, G.-C. Guo, *Phys. Rev. Lett.* **2020**, *125*, 030506.
[101] Z. Li, Y.-G. Han, H. Zhu, *Phys. Rev. A* **2019**, *100*, 032316.
[102] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* **2009**, *81*, 865.
[103] M. Kleinmann, H. Kampermann, D. Bruß, *Phys. Rev. A* **2011**, *84*, 042326.
[104] E. Chitambar, *Phys. Rev. Lett.* **2011**, *107*, 190502.
[105] A. Peres, *Phys. Rev. Lett.* **1996**, *77*, 1413.
[106] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **1996**, *223*, 1.
[107] X. Jiang, K. Wang, K. Qian, Z. Chen, Z. Chen, L. Lu, L. Xia, F. Song, S. Zhu, X. Ma, *npj Quantum Inf.* **2020**, *6*, 90.
[108] W.-H. Zhang, X. Liu, P. Yin, X.-X. Peng, G.-C. Li, X.-Y. Xu, S. Yu, Z.-B. Hou, Y.-J. Han, J.-S. Xu, Z.-Q. Zhou, G. Chen, C.-F. Li, G.-C. Guo, *npj Quantum Inf.* **2020**, *6*, 103.
[109] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, X. Zhang, *Phys. Rev. Applied* **2019**, *12*, 044020.
[110] W. Dür, G. Vidal, J. I. Cirac, *Phys. Rev. A* **2000**, *62*, 062314.
[111] L. Heaney, A. Cabello, M. F. Santos, V. Vedral, *New J. Phys.* **2011**, *13*, 053054.
[112] R. H. Dicke, *Phys. Rev.* **1954**, *93*, 99.
[113] Z. Li, Y.-G. Han, H.-F. Sun, J. Shang, H. Zhu, *Phys. Rev. A* **2021**, *103*, 022601.
[114] H. Zhu, M. Hayashi, *Phys. Rev. Lett.* **2019**, *123*, 260504.
[115] H. Zhu, M. Hayashi, *Phys. Rev. A* **2019**, *100*, 062335.
[116] M.-D. Choi, *Linear Algebra Appl.* **1975**, *10*, 285.
[117] A. Jamiołkowski, *Rep. Math. Phys.* **1972**, *3*, 275.
[118] J. de Pillis, *Pacific J. Math.* **1967**, *23*, 129.
[119] Y.-C. Liu, J. Shang, X.-D. Yu, X. Zhang, *Phys. Rev. A* **2020**, *101*, 042315.
[120] H. Zhu, H. Zhang, *Phys. Rev. A* **2020**, *101*, 042316.
[121] P. Zeng, Y. Zhou, Z. Liu, *Phys. Rev. Research* **2020**, *2*, 023306.
[122] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **1999**, *60*, 1888.
[123] R.-Q. Zhang, Z. Hou, J.-F. Tang, J. Shang, H. Zhu, G.-Y. Xiang, C.-F. Li, G.-C. Guo, *Phys. Rev. Lett.* **2022**, *128*, 020502.
[124] M. Luo, X. Zhang, X. Zhou, *Phys. Rev. A* **2022**, *105*, 012614.
[125] L. P. Thinh, M. Dall'Arno, V. Scarani, *Quantum* **2020**, *4*, 320.
[126] Note that the choices of null and alternative hypotheses are the opposite in ref. [125], with Equation (8) being the null hypothesis and Equation (9) being the alternative hypothesis.
[127] Y.-C. Liu, J. Shang, R. Han, X. Zhang, *Phys. Rev. Lett.* **2021**, *126*, 090504.
[128] J. Miguel-Ramiro, F. Riera-Sàbat, W. Dür, arXiv:2201.01782 [quant-ph], **2021**.
[129] D. Mayers, A. Yao, *Quantum Inf. Comput.* **2004**, *4*, 273.
[130] I. Šupić, J. Bowles, *Quantum* **2020**, *4*, 337.
[131] C. Bădescu, R. O'Donnell, J. Wright, arXiv:1708.06002, **2017**.
[132] S. Chen, J. Li, R. O'Donnell, arXiv:2102.13098, **2021**.
[133] W. Dür, H. J. Briegel, *Rep. Prog. Phys.* **2007**, *70*, 1381.
[134] L. Hardy, *Phys. Rev. Lett.* **1992**, *68*, 2981.
[135] D. Aharonov, J. Cotler, X.-L. Qi, arXiv:2101.04634, **2021**.

Xiao-Dong Yu is currently a professor at Shandong University, China. He obtained his Ph.D. in theoretical physics from Shandong University, China and subsequently worked as a postdoctoral researcher at Universität Siegen, Germany. He is interested in various fundamental aspects of quantum information processing.



Jiangwei Shang is currently an associate professor in School of Physics at Beijing Institute of Technology, China. He received his B.Sc. (first class honours) in physics and mathematics in 2010 from National University of Singapore (NUS), then his Ph.D. in 2014 from the Centre for Quantum Technologies, NUS. His research interests include various aspects in quantum information and foundations of quantum mechanics.

Otfried Gühne is currently professor for theoretical physics at the University of Siegen in Germany. He obtained his Ph.D. from the University of Hannover, Germany, in 2004. After that, he moved to Innsbruck in Austria, first as a postdoc and, since 2008, as a leader of a junior research group. His research interests are the theory of multiparticle entanglement and the foundations of quantum mechanics.