Non-Destructive Verification of Entangled States via Fidelity Witnessing

Ferran Riera-Sàbat,* Jorge Miguel-Ramiro,* and Wolfgang Dür
Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, 6020 Innsbruck, Austria
(Dated: September 16, 2022)

Assessing the quality of an ensemble of noisy entangled states is a central task in quantum information processing. Usually this is done by measuring and hence destroying multiple copies, from which state tomography or fidelity estimation can be employed to characterize states. Here we propose several methods to directly distinguish between two different sets of states, e.g. if their fidelity is above or below a certain threshold value. This turns out to be significantly more efficient, and importantly keeps the verified states intact. We make use of auxiliary entanglement or an ensemble of larger size, where we operate on the whole ensemble, but measure only a small fraction where information has been concentrated. For certain state families, we demonstrate that such an approach can even outperform optimal methods that collectively measure directly a fixed fraction of the ensemble.

I. INTRODUCTION

Quantum entanglement is the key resource for multiple applications in quantum technology, including quantum communication and cryptography [1, 2], quantum networks [3–5], distributed computation [6–8] and distributed sensing [9–11]. However, in any realistic scenario channels and devices are imperfect, and resulting states will be noisy. Assessing whether the quality of produced or maintained entangled states is sufficient for the desired application is hence a central task for all these applications.

The typical approach to determine the quality of an ensemble of mixed states is to perform local measurements on some individual copies, from which features of the states can be assessed. Multiple strategies for certifying entangled states have been proposed [12–16]. The approaches differ on the amount of information learnt from the states, which is general related with the amount of resources spent in the process. The existing strategies range from a complete characterization of the states via state tomography [17, 18], to the learning of some specific property such as the fidelity as in fidelity estimation [19]. In this work we consider a still less demanding information-demanding problem, consisting in determining whether the fidelity of an entangled state is above or below certain threshold value, a natural and realistic extension of the state verification problem [20–25]. We denote this decision problem as fidelity witnessing, which can be relevant in multiple scenarios, whenever it suffices to know if the quality of the states of an ensemble is large enough to perform the desired task. For instance, in a communication scenario the fidelity directly indicates the error rate of transmitted quantum information via teleportation, but also if the states can be used to expand a secure secret key. The main advantage of such an approach lies in the reduced required resources as compared to schemes that acquire more information.

Here, in contrast to many previous approaches [16, 25], we assume that we have access to the whole ensemble, and not just individual copies that are processed locally and individually, and also consider entanglement-assisted protocols. While this poses additional experimental challenges, we find that these approaches have significant advantages: First, they are more efficient and can lead to up to exponential enhancements as compared to previous schemes, even outperforming optimal, non-local methods that measure all states from on an ensemble of fixed size. Second, certified states are not destroyed - the remaining states are directly certified, without the necessity to assume a tensor product structure of the initial ensemble. The key element is an information transfer from multiple copies of the states in the ensemble to a certain subset, or to some auxiliary entangled states, where only these few copies are subsequently measured and hence destroyed. In this way a much larger fraction of an ensemble can be left intact, while still deciding if the remaining states are suitable for the desired application. We also take care of properly accounting for additional entanglement resources, by relating auxiliary entanglement to the required number of noisy copies.

We introduce three different protocols, which are compared with the typically considered case of sequential measurements of single copies of identical, noisy entangled states $\rho^\otimes n$. We propose strategies that rely on collective operations which allow us to transfer information about the noise of several copies into few auxiliary state(s), in the spirit of [26, 27]. By partially or completely measuring the auxiliary system(s), one can access the information of the accumulated noise with increased efficiency, in such a way that the copies that are certified are not consumed in the process. We make use of this powerful tool and introduce several approaches, each of which works better in specific situations. To this aim we consider different state families, including noisy ensembles that result from maximally entangled states affected by decay noise, phase-flip noise or depolarizing noise, mimicking relevant situations such as distributing entanglement through noisy channels, or storing entangled states for some time in an imperfect quantum memory. The main findings can be summarized as follows:

• We introduce three different protocols for the decision problem of distinguishing between two state families of noisy entangled states w.r.t. their fidelity.

* These two authors contributed equally.
II. BACKGROUND

We discuss here the basic notions and operations we make use of throughout this work.

A. Maximally entangled states

Bell states.— Bell states are maximally entangled quantum states shared by two qubits. The set of Bell states form a basis of $\mathbb{C}_2^A \otimes \mathbb{C}_2^B$ given by the elements

$$|\Psi_{ij}\rangle_{AB} \equiv 1 \otimes \sigma_x^i \sigma_z^j \left(\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}\right),$$  

where $\sigma_i$ is the $i$th Pauli operator. These states are a fundamental resource for multiple applications such as e.g. super-dense coding [28], quantum teleportation [29, 30], QKD [1, 2] or distributed quantum computation [6, 7].

Higher dimensional maximally entangled states.— Qudits are natural extensions of qubit systems for $d-$dimensional systems. A bipartite system of qudits is associated with the Hilbert space $\mathcal{H}_{AB} = \mathbb{C}_d^A \otimes \mathbb{C}_d^B$, where we can define an orthonormal basis of maximally entangled states of the form [29]

$$|\Psi_{mn}\rangle_{AB} \equiv \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{i2\pi km/d} |k\rangle_A |k \oplus n\rangle_B,$$  

where $m, n \in \mathbb{Z}_d$ are called the phase and amplitude index of the state respectively, and where $k \oplus n \equiv (k - n)\text{mod } d$ and $d$ is the dimension of the qudit systems.

B. Fidelity of quantum states

The fidelity of two quantum states $\rho, \sigma$ is a measure of how close the two states are, with respect to the probability of identifying one as the other with an optimal measurement. Formally, it is defined as

$$F = \left(\text{tr}\sqrt{\rho \sigma} \sqrt{\rho}\right)^2.$$  

We use the fidelity as a natural figure of merit to measure the amount of noise affecting a quantum state. Since we mainly deal with maximally entangled states, the fidelity in our case mostly refers to the distance between some state $\rho$ and the corresponding maximally entangled –pure– state $|\Psi\rangle$, such that Eq. (3) reduces to $F \equiv \langle \Psi | \rho | \Psi \rangle$.

C. Families of states

We introduce here the different families of states we make use of throughout this work as probe state to be verified or witnessed. All of them correspond to dominant noise processes relevant in many physical scenarios.

1. Bell diagonal states

Any arbitrary bipartite mixed state $\rho$ can be always depolarized into a state diagonal in the Bell basis with local operations. This is achieved by implementing a quantum map with Kraus operators $\mathcal{D}_{\text{BD}} = \{\frac{1}{2} \sigma_i \otimes \sigma_i\}_{i=0}^{3}$, i.e.,

$$\mathcal{D}_{\text{BD}}: \rho = \sum_{i_1,j_1,i_2,j_2} \alpha_{i_1,j_1,i_2,j_2} |\Psi_{i_1,j_1}\rangle \langle \Psi_{i_2,j_2}| \mapsto \rho_{\text{BD}} = \sum_{i,j} \alpha_{ij} |\Psi_{ij}\rangle \langle \Psi_{ij}|.$$  

Note that the fidelity of the state remains unchanged.

2. Werner states

Further depolarization is possible by making all but one of the diagonal elements equal and transforming the state into a Werner state [31], i.e.,

$$\rho_{\text{w}} = q |\Psi_{00}\rangle \langle \Psi_{00}| + \frac{1-q}{4} 1_4,$$  

while keeping the fidelity $F = (3q + 1)/4$ unchanged. This is accomplished by suitable twirling techniques (see e.g. [32]), i.e.,

$$\mathcal{D}_{\text{w}}: \rho \mapsto \int \langle U \otimes U \rangle \rho (U \otimes U)^\dagger \ dU = \rho_{\text{w}},$$  

where $dU$ is the Haar measure. Depolarization can also be achieved using only local operations drawn from a discrete set [33]. Werner state can be conceived as worst case in terms of the noise of the states, where with some probability no information of the state is left.
3. Dephasing type states

A less general family of states is given by rank-2 Bell diagonal states. These states are local unitary (LU) equivalent to a Bell state, where one of the parts is affected by a bit flip noise, i.e.,

$$\mathbb{I} \otimes N_F: |\psi_{00}\rangle \langle \psi_{00}| \rightarrow \rho_d = F|\psi_{00}\rangle \langle \psi_{00}| + (1 - F)|\psi_{01}\rangle \langle \psi_{01}|,$$ \hfill (7)

where $N_F = \sqrt{p\mathbb{I} \otimes (1 - p)Z}$. Notice that states resulting from local dephasing noise are formally equivalent, where both qubits may be affected by Pauli $\sigma_z$ noise. This kind of noise is relevant e.g. when there are fluctuating fields or phase references.

4. Amplitude damping type states

A different class of states corresponds to amplitude damping-type. These states are the result of sending a perfect Bell state $|\psi_{10}\rangle$ through an amplitude damping channel with Kraus operators $\mathcal{A}_d = \{ |0\rangle\langle 0| + \sqrt{p} |1\rangle\langle 1|, \sqrt{1 - p}|0\rangle\langle 0| \}$ \cite{34}, i.e.,

$$\mathbb{I} \otimes \mathcal{A}_d: |\psi_{10}\rangle \langle \psi_{10}| \rightarrow \rho = F|\psi_{10}\rangle \langle \psi_{10}| + (1 - F)|00\rangle\langle 00|,$$ \hfill (8)

where the state is LU equivalent to

$$\rho_u = F|\psi_{00}\rangle \langle \psi_{00}| + (1 - F)|01\rangle\langle 01|.$$ \hfill (9)

This kind of states are relevant in scenarios where one describes decay processes of e.g. atoms in a quantum memory.

D. The counter gate

In several of the strategies introduced in this work we make use of a quantum gate introduced in \cite{26,35} which allows us to transfer information from an ensemble of entangled qubit states into a higher dimensional entangled state by means of local operations. The so-called counter gate \cite{26,35} is a bilateral qubit-qudit controlled operation that takes a 2-dimensional entangled state as control and a $d$-dimensional entangled state as target. Given a target system consisting of a maximally entangled state with phase index zero, see Eq. (2), its action is given by

$$b\text{CX}^{\text{d}}_{1 \rightarrow 2} |mn\rangle |0\rangle |\Phi^d_{0j}\rangle \rightarrow |mn\rangle |0\rangle |\Phi^d_{0j+m\otimes n/2}\rangle,$$ \hfill (10)

where $|mn\rangle$ are the computational basis states, $b\text{CX}^{\text{d}}_{1 \rightarrow 2} = \text{CX}^{A_1A_2} \otimes \text{CX}^{B_1B_2}$, and

$$\text{CX}_{1 \rightarrow 2} = |0\rangle\langle 0| \otimes \mathbb{I}_d + |1\rangle\langle 1| \otimes X_d$$ \hfill (11)

is the hybrid controlled-$X$ gate \cite{36}. We denote as type-1, type-2 and type-3 error states, the states corresponding to $|01\rangle$, $|10\rangle$ and $|\psi_{10}\rangle$ respectively. The action of the counter gate taking a type-1(2) error state acting as control leads to an amplitude index value of the auxiliary state increased(decreased) by one, whereas it is left invariant for the type-3 error state.

We denote the operation consisting in applying the counter gate, Eq. (10), from each of the states of an ensemble of $n$ copies into a $d$-dimensional auxiliary state, as Error Number Gate (ENG), i.e.,

$$\text{ENG} = \prod_{k=1}^n b\text{CX}^{\text{d}}_{k \rightarrow \text{aux}}.$$ \hfill (12)

The name is motivated by the action of the gate on ensembles with only $|01\rangle$ error states, where the number of error states in the ensemble can be determined in this way.

E. Entanglement cost and relation to resources

In this work, we consider entanglement assisted protocols that make use of (small) amounts of extra entanglement. In order to make a comparison with protocols that only measure states directly, we need to relate these entangled states with the states of the noisy ensemble. First we point out that the amount of entanglement that is contained in a noiseless Bell state constitutes the basic unit of bipartite entanglement, usually denoted as ebit of entanglement. The number of ebits contained in a maximally entangled state of dimension $d$ is given by $E\left(|\psi_{BD}_{0}\rangle\right) = \log_2 d$. Therefore, in an ensemble of $n$ maximally entangled states the number of ebits is given by $E\left(|\psi_{BD}_{0}\rangle^\otimes n\right) = n \log_2 d$.

The evaluation of the amount entanglement, in terms of the number of ebits, contained in mixed states is however not clear. The distillable entanglement $E_D$ \cite{37}, i.e. the fraction of maximally entanglement states that can be distilled from many noisy copies by means of local operations and classical communication, is a suitable entanglement measure in this context. It tells us that from $m$ noisy copies of the state $\rho$, one can generate $mE_D$ ebits of entanglement. This provides the desired relation between noisy copies and ebits. However, $E_D$ is hard to compute in general, and only some upper bounds \cite{38,39} and lower bounds \cite{40} are known. Here we make use of reachable lower bounds provided by entanglement purification protocols \cite{33,39,41,42}. We compute the yield $Y$ of a combination of the recurrence protocol \cite{41} and hashing \cite{39}, i.e. the fraction maximally entangled states over initial noisy states, which is a lower bound for $E_D$ \cite{43}. While the recurrence protocol allows one to increase the fidelity of remaining pairs, hashing is only applicable for sufficiently high fidelities, but has a non-zero yield. Both protocols operate on states diagonal in the Bell basis, where any state can be transformed to such form as discussed above. The yield of the hashing protocols for Bell diagonal states $\rho_{BD}$ is given by $[1 - S(\rho_{BD})]$, and one can obtain a smooth curve as a function of the initial fidelity $F$ by mixing strategies, i.e. consider a mixture of states resulting from a certain number of rounds of the recurrence protocol, and apply Hashing to the resulting one.

So whenever auxiliary entanglement of $m$ ebits is required, we assume that it is generated from the noisy
ensemble by consuming \( \lceil m/Y \rceil \) states from the ensemble, where \( Y \) is the yield of the entanglement purification protocol. Notice that we do not optimize over entanglement purification protocols, so we provide a conservative bound, thereby underestimating the operational advantage of entanglement-assisted protocols.

### III. PROBLEM SETTING

Quantum state certification and verification has been studied and analyzed in different directions, ranging from learning more information about a state, as in state tomography, to less information as in fidelity estimation. The problems we study here are closely related to quantum state verification of entangled states [12, 14, 16, 27, 44], where the task is to verify whether some ensemble of entangled states consisting of \( n \) identical copies is indeed maximally entangled. In terms of the fidelity of the states, state verification solves the problem of deciding whether the fidelity of the states is \( F = \langle \Psi_{00} | \rho | \Psi_{00} \rangle = 1 \) or not (i.e. \( F \leq 1 - \epsilon \)).

The problems we analyze enclose more realistic situations [12, 14, 16, 25], where a certain level of noise is in general unavoidable, and therefore entangled states cannot be strictly verified with previous methods. The task reduces to a decision problem of determining whether the fidelity of an entangled state is above or below some threshold value, or correspond to one out of two possible values. We define and analyze these two closely related problems, denoted as fidelity witnessing and fidelity discrimination (see Fig. 1).

Notice that it is not required to learn the actual value of \( F \) to solve the underlying decision problem which essentially requires only to learn one bit of information. This learning of minimum amount of information can be enough and useful in many contexts and applications, for which the parties sharing the entanglement just require a minimum fidelity of the states to operate. In contrast to other methods as e.g. fidelity estimation or state tomography, fidelity witnessing and fidelity discrimination has the benefit of significant reduction in the amount of consumed resources.

### IV. FIDELITY WITNESSING STRATEGIES

We propose different approaches to solve the fidelity witnessing and discrimination problems for ensembles of identical bipartite entangled states. While the most direct approach, a direct extension of strategies applied in fidelity estimation and verification [19, 44], relies on copy-by-copy measurement of certain part of the ensemble, the remaining approaches make use of...
different tools in order to transfer information about
the noise of the ensemble into auxiliary registers with-
out destroying the original copies. The auxiliary reg-
isters are subsequently manipulated to extract the re-
quired information and solve the decision problems.

We remark that the protocols we introduce are
suited for different state families. While protocol P0
(individual measurements) and P3 (blocking strate-
gies) are suitable for all families, the error counting
protocol P1 and the coarse graining protocol P2, are
especially only applicable to states of the from ρa re-
sulting from decay or amplitude damping.

A. Protocol P0: Individual measurements

Ref. [25] discusses how to perform fidelity witnessing
by extending the strategy for verification of Bell
states.

In state verification [20–25], an arbitrary noisy en-
semble ρ⊗n is given and one aims to distinguish be-
tween either states being perfect, i.e., ρ = |Ψ(0)|Ω(Ψ(0)|,
or being noisy up to some fidelity, i.e., ⟨Ψ(0)|ρ|Ψ(0)| ≤ 1 − ε = F. The optimal solution in this case con-
sists in performing random copy-by-copy and local
two-outcome measurements, see Fig. 2a, given by

\[ \Omega_i |Ψ(0)⟩ = |Ψ(0)⟩, \]

where the label “pass” (“fail”) is assigned to the out-
come corresponding to Ω_i (1 − Ω_i). The measurement
can then be described by

\[ Ω = \sum_j p_j Ω_j \]

where \( p_j \) is a probability distribution. The probabil-
ity that one state pass the measurement test is given by

\[ p = 1 − ϵ ν(Ω), \]

where ν(Ω) is the spectral gap between the largest and the second largest eigenvalues of Ω. Therefore, for
an unknown state ρ the optimal strategy is such that
maximizes ν(Ω). For Bell states |Ψ(0)| it is shown [44]
that max_Ω ν(Ω) = 2/3 and hence \( p_{max} = (1 + 2F)/3 \).

After measuring \( n \) copies, the probability of finding
j states that “fail” the test and \( n−j \) states “pass” it
is given by

\[ \text{Pr}(j|F) = \binom{n}{j} p^{n−j} (1−p)^j, \]

where F is the fidelity of the states. Thus, the value of
j is related to the actual fidelity of the ensemble. We
exploit this property by suitably acquiring and pro-
cessing information about the value of j in order to
tackle the fidelity witnessing and discrimination prob-
lems. We detail later in this section the strategy based
on single copy measurements for these two problems.
Before, we particularize the previous properties for
two type of states that we make use of throughout
the manuscript.

Amplitude damping noise ensemble.– Consider the
states of the ensemble to be amplitude damping type,
Eq. (9), with some unknown fidelity F. By measur-
ing the state on the \( Z_A ⊗ Z_B \) basis, we consider the
state “pass” the measurement test is this two outcomes
coincide. This is given by

\[ p = F < p_{max}. \]

Since we can distinguish with total certainty between
the two eigenvectors (with no-null eigenvalue) of ρ,
and this measurement is equivalent to a measurement
with ν = 1, what has been shown to be optimal for
the verification problem [44].

Werner-type states.– Consider now the case where
the states of the ensemble are given by Werner states,
see Eq. (5). Note that this corresponds to depolar-
izing noise acting on the states. In particular, any
state can be brought to a Werner-type form by depo-
larization means [31], and hence this case represents
a completely general situation.

The optimal measurement in this case also corre-
sponds to locally measure the states in the computa-
tional basis, i.e. with respect to the observable \( Z_A \)
and \( Z_B \), considering that the state “pass” the mea-
surement test if the two outcomes coincide. However,
the probability of a state with fidelity F passing the
measurement is now given by \( p = (1 + 2F)/3 \), what
is equivalent to perform the optimal measurement for
an unknown state. Note that the process is analogous
to first depolarize the state to its Werner form and
then performed the described measurement.

Fidelity witnessing.– Given an ensemble of en-
tangled states with fidelity F and some threshold fi-
delity \( F_0 \), the expected value of j (see above) is given by

\[ ⟨j⟩ = n [1 − ν(Ω)(1 − F)]. \]

This allows us to extend this strategy to perform fi-
delity witnessing. After performing the measurement
\( \{Ω, 1 − Ω\} \) on \( n \) copies, we can conclude that the fi-
delity lies on one or another regime, i.e.

\[ \begin{cases} F > F_0 & \text{if } j > n [1 − ν(Ω)(1 − F_0)], \\ F < F_0 & \text{if } j < n [1 − ν(Ω)(1 − F_0)]. \end{cases} \]

Since the ensemble is in a tensor product structure,
the success probability \( P_s \) of solving the witnessing
problem based on Eq. (19), can be determined by the
Chernoff–Hoeffding theorem [45]

\[ P_s ≥ 1 − e^{D(j||np)}, \]

where

\[ D(S||Q) = \sum_x S(x) \log \left( \frac{S(x)}{Q(x)} \right) \]

is the Kullback–Leibler divergence (see [25]).

The criterion given by Eq. (19) can be extended
by defining a subset Σ which contains some of the
possible values of j, i.e., the ones for which we conclude
that the fidelity is above the threshold \( F_0 \). The values
of \( j \) contained in \( \Sigma \) are given in such a way that a certain fraction \( \delta \) of the area under the curve \( \Pr(j|F) \) contained in \( F \in [0,1] \), is above \( F_0 \). Formally, the subset \( \Sigma \) is defined as

\[
\Sigma : \left\{ j \left| \int_{F_0}^1 \Pr(j|F) \, dF > \delta \int_0^1 \Pr(j|F) \, dF \right. \right\},
\]  

(22)

where \( \delta \) can be freely chosen.

Given the fixed threshold fidelity \( F_0 \), the probability of deciding that \( F > F_0 \) is hence given by the probability of obtaining certain \( j \) from \( \Sigma \), i.e.,

\[
\Pr(F > F_0) = \sum_{j \in \Sigma} \Pr(j|F).
\]

(23)

The success probability, i.e. the probability of deciding that the fidelity is above (or below) the threshold and being right, is given by

\[
P_s(F) = \begin{cases} 
1 - \Pr(F > F_0) & \text{for } F < F_0 \\
\Pr(F > F_0) & \text{for } F > F_0.
\end{cases}
\]

(24)

The value of \( \delta \) can be tuned in order to optimize the performance in certain regimes. Observe that, by appropriately choosing the value of \( \delta \) in Eq. (22), one can increase or decrease the success probability \( P_s \) of the protocol within some of the regimes discussed in Sec. III, i.e. either enhance the success probability to correctly certify states with \( F > F_0 \), or correctly reject states with \( F < F_0 \). We analyze the performance of this protocol in detail in the following sections, comparing it with the other strategies we propose.

**Fidelity discrimination.**—The information learning process is analogous for fidelity discrimination, where one learns the number \( j \) of states that “fail” the measurement test \( \{\Omega, \mathbb{I} - \Omega\} \). Once a particular value of \( j \) is obtained, one simply concludes that the fidelity of the ensemble is \( F_1 \) in case \( \Pr(j|F_1) > \Pr(j|F_2) \).

Similar as before, We can separate all the possible values of \( j \) in two sets \( \Sigma_1 \) and \( \Sigma_2 \), such that

\[
\begin{align*}
\Sigma_1 &= \{ j \mid \Pr(j|F_1) > \Pr(j|F_2) \}, \\
\Sigma_2 &= \{ j \mid \Pr(j|F_2) > \Pr(j|F_1) \}.
\end{align*}
\]

(25)

In case fidelity \( F_1 \) is then given with probability \( \eta_1 \), the success probability reads

\[
P_s = \eta_1 \sum_{j \in \Sigma_1} \Pr(j|F_1) + \eta_2 \sum_{j \in \Sigma_2} \Pr(j|F_2).
\]

(26)

If the two fidelities are given with the prior probability \( \eta_1 = \eta_2 \), the success probability \( P_s \) is then bounded by

\[
P_s \leq \frac{1}{2} \left[ 1 + T\left( \rho_1^{\otimes n}, \rho_2^{\otimes n} \right) \right],
\]

(27)

where \( \rho_1 = \rho(F_1) \), and \( T(\rho, \sigma) \) is the trace distance between states \( \rho \) and \( \sigma \) [34]. In particular, for amplitude damping noise (see above), the success probability when performing fidelity discrimination reaches the optimal values, i.e., it saturates the trace distance between the two ensembles Eq. (27).

![Individual measurements (P0) and Error counting (P1)](image)

**B. Protocol P1: Error counting**

The first protocol we propose is an extension of the approach for quantum state verification we introduced in [27]. In the following we will consider states of the form \( \rho_a \) resulting from amplitude damping. In general, given an ensemble of \( n \) identical copies of states \( \rho_a \), the protocol consists in applying the ENG gate, Eq. (12), between \( n \) copies of the ensemble and an auxiliary \( d \)-level system of the form \( |\Phi_{00}^d\rangle \), see Eq. (2). The ENG transfers information about the number of type-1 and type-2 errors in the ensemble into the auxiliary system (see Fig. 2b) by changing its amplitude index. By subsequently measuring this auxiliary state we can learn its amplitude index \( j \), revealing information about the number of errors—and therefore the fidelity—of the ensemble. Crucially, the remaining ensemble that is witnessed is not destroyed in the process. Notice, though, that the state of the ensemble changes, and is no longer of tensor product structure, i.e. the copies are not independent. However, the fidelity of individual reduced states is known, and above the threshold value \( F_0 \) in case of successful certification. We detail in the following these steps for the different cases depending on the kind of noise affecting the ensemble copies.

**Fidelity witnessing.**—Consider first that the noise affecting the states of the ensemble is amplitude damping type Eq. (9). An ensemble of \( n \) copies of states of the form Eq. (9) is given. Note that one can also interpret an ensemble of \( n \) states of this form as an unknown distribution of pure states where each state corresponds either to \( |\Psi_{00}\rangle \) or \( |01\rangle \). The joint state of the ensemble can then be written as

\[
\rho^{\otimes n} = \sum_{j=0}^{n} \binom{n}{j} F^j (1 - F)^{n-j} \Gamma_j,
\]

(28)

where \( \Gamma_j \) is a density operator corresponding to all permutations of \( \{|\Psi_{00}\rangle^{(n-j)} |01\rangle^j\}^d \).

Information about the noise of the ensemble can be transferred and accumulated in a single \( d \)-level state.
For that end, a maximally entangled state of dimension $d = n + 1$ is prepared, $|\Phi_{00}^d\rangle$ (see Eq. (2)). The ENG gate, Eq. (12), is applied between the states of the ensemble and the auxiliary $d$-dimensional state, such that

$$\text{ENG}: \rho^{\otimes n} \otimes |\Phi_{00}^d\rangle\langle\Phi_{00}^d| \mapsto \sum_{j=0}^n \binom{n}{j} F^{n-j} (1-F)^j \Gamma_j \otimes |\Phi_{0j}^d\rangle\langle\Phi_{0j}^d|.$$  

(29)

Observe that, given the nature of the noise and the effect of the ENG gate, the amplitude index of the auxiliary state $j$ encodes very specific information about the number of errors contained in the ensemble, that directly relates with the fidelity of the copies.

By simply measuring the auxiliary state locally by parties $A$ and $B$ in the generalized $Z$ basis, and subtracting their outcomes, one learns the value of the amplitude index $j$, from which one can infer the number of errors in the ensemble. Each $j$ value can be found with probability

$$\text{Pr}(j|F) = \binom{n}{j} F^{n-j} (1-F)^j.$$  

(30)

Note that this corresponds to the same distribution obtained with protocol P0, see Eq. (16), with $p = F$. Due to this close, but probabilistic, dependence, one can solve the decision problem by determining whether the measured value of $j$ is above or below certain value $j_0 = n(1 - F_0)$, which also depends on the threshold problem fidelity $F_0$. Note that the same statistical analysis performed in protocol P0 can be applied here, and hence, the two protocols exhibit the same success probability, see Fig. 3. However, while in protocol P0 the whole ensemble is consumed, here we just destroy an auxiliary maximally entangled state of dimension $d = n + 1$, providing an exponential improvement in the amount of consumed resources. Importantly, the states that are witnessed or verified are not destroyed in the process, in opposition to protocol P0 and previous approaches. Notice, however, that the remaining ensemble is no longer of tensor product structure, but corresponds to $\Gamma_j$ when obtaining the outcome $j$. The fidelity of reduced states, i.e. tracing out all but one copy, is given by $F = (n - j)/n$, which can be larger than the initial fidelity $F$.

The protocol can equivalently be applied to Werner states of the form Eq. (5). The steps of the protocol are identical as before. However, the ensemble can now contain the three different kinds of errors, and hence, the value of $j$ after the application of the ENG does not encode the number of errors in the ensemble. Instead, it provides information about the difference between type-1 and type-2 error states. In this case, the probability of obtaining $j$ for a given $F$, corresponds to the sum of all configurations with a difference of $j$ errors, i.e.,

$$\text{Pr}(j|F) = \sum_{i,k,l=0}^n \frac{n!}{i!k!l!} A^i (1-A)^{k+l}$$  

(31)

where $A \equiv (1 + 2F)/3$.

Note that, due to the different effect of the counter gate in this case (Sec. II D), we can now obtain $2n + 1$ different values of $j$, i.e. $j \in \{-n, \ldots, n\}$. In order to differentiate between all these possible values of $j$, we require an auxiliary state of dimension $d = 2n + 1$. We remark, though, that we did not succeed in using this to obtain an efficient protocol for witnessing Werner states, i.e. a protocol that outperforms P0.

**Fidelity discrimination.**- The error counting protocol can be directly applied for solving the fidelity discrimination problem. This is accomplished by simply processing the information learnt about the value of $j$ as in the protocol P0 case, see Eqs. (25)-(27), finding comparable efficiency.

### C. Protocol P2: Coarse graining

In the strategies introduced above, i.e. the single copy measurement and the error counting protocols, the information obtained about the ensemble is unnecessarily excessive. Instead of learning information...
about whether the number of errors in the ensemble is above or below some value, we –indirectly– also obtain information about the concrete number of errors in the ensemble. This implies that the protocols likely spends more resources than the ones required to just solve the witnessing and discrimination problems.

We propose here a modified protocol that tries to minimize the amount of obtained information, therefore reducing the amount of resources spent during the process. The strategy relies on the application of coarse-grained techniques that allow us to locally access to partial information about the amplitude index \( j \) of previous protocol, without destroying the auxiliary state nor the ensemble copies.

**Fidelity witnessing.** We restrict to the amplitude damping noise case for simplicity, i.e. states of the form \( \rho_d \). The first steps of the protocol are identical as in the error counting approach. A \( d \)-dimensional auxiliary state \( A_1 B_1 \) is prepared in the state \( \Phi^d_{\phi_0} \) with \( d = n + 1 \), and the ENG operation is applied from \( n \) states of the ensemble to the auxiliary, such that the information of the number of errors of the ensemble gets accumulated in the amplitude index \( j \) of the auxiliary state, i.e. \( \Phi^d_{\phi_j} \). Here however we do not measure the auxiliary state to learn the value of \( j \). In fact, as shown later, the auxiliary state is kept unchanged (and the entanglement is not consumed).

We introduce an additional two-system register \( A_2 B_2 \), that we denote as extra register, of dimension \( m \leq d \). For simplicity, we assume that \( m \) divides \( d \), i.e., \( d/m \in \mathbb{N} \), however this assumption can be lifted. The extra register is initially prepared in the \( |00\rangle_{A_2 B_2} \) state locally by parties \( A \) an \( B \). A bilateral local operation \( U_{A_1 A_2} \otimes U_{B_1 B_2} \) is applied from the auxiliary to the extra register such that

\[
U_{12} = \sum_{k=0}^{d-1} |k\rangle\langle k| \otimes X_2^\pm, \quad (32)
\]

which transfers information of the amplitude index into the extra register in a coarse graining way (see Fig. 4).

**Protocol P2: Coarse graining**

*Input:* Ensemble of \( n \) identical noisy Bell states and auxiliary \( n+1 \)-level maximally entangled state.

1. Apply the ENG between the ensemble and the auxiliary state. The information of the noise is accumulated in its amplitude index \( j \).
2. Apply the coarse grained operation Eq. (33) from the auxiliary into an additional extra register.
3. Measure the extra register to learn information about where \( j \) lies.
4. Apply the decorrelation process to recover the auxiliary state untouched.

*Output:* The witnessing decision problem is solved, i.e., the fidelity of the ensemble states is determined to be above or below some threshold up to some failure probability.

The effect of this operation reads

\[
U_{A_1 A_2} \otimes U_{B_1 B_2} \frac{\Phi^d_{\phi_j}}{\sqrt{d}}_{A_1 B_1} |00\rangle_{A_2 B_2} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle \frac{1}{d/m} \sum_{l=0}^{d/m} |k \oplus j\rangle \frac{1}{d/m} |k \oplus j\rangle_{A_2 B_2} . \quad (33)
\]

The different \( j \) values get grouped into different sets of certain size and the group or interval \( \delta_0 \) is identified as the interval containing the threshold \( j_0 \) value, where \( j_0 \) is the most likely value of the distribution \( \Pr(j|\phi_0) \).

The qubit of the extra register that belongs to party \( A \) is subsequently teleported to party \( B \) --by consuming \( \log_2 m \) ebits of entanglement-- such that the global state becomes

\[
|\psi\rangle_{A_1 A_2 B_1 B_2 B_3} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_{A_1} \otimes |k \oplus j\rangle_{B_1 B_2} \frac{1}{d/m} \sum_{l=0}^{d/m} |l\rangle_{B_1 B_2} . \quad (34)
\]

where we have relabelled qubit \( A_2 \rightarrow B_3 \). Finally, party \( B \) performs a two outcome POVM measurement defined by the projectors \( \{M, 1-M\} \) on the extra register qubits \( B_2, B_3 \), i.e.,

\[
M = \sum_{\delta=0}^{\Delta_0} \sum_{l=0}^{m-1} |l\rangle \otimes |l \oplus \delta, l\rangle , \quad (35)
\]
The performance of the protocol can be directly analyzed given the previous reasoning and given the probability distribution of the \( j \) value as a function of the state fidelity. Fig. 6 shows the efficiency for different settings and ensemble sizes. Observe how for the witnessing problem of determining whether the value of the fidelity is \( F > F_0 \) or \( F < F_0 \), the success probability of the protocol can approach 1 for relatively small additive error \( \lambda \).

Once the decision problem is solved, the last step of the protocol entails the recuperation of the auxiliary state, which has been entangled with the extra register during the process. The following steps are required to disentangle the extra register and leave the auxiliary state—and the entanglement associated—untouched. First, the operation \( U_{B_{1}B_{2}} \), Eq. (32), is undone on the remaining measured state Eq. (34), i.e.

\[
U_{B_{1}B_{2}}^\dagger \langle \psi \rangle_{A_{1}B_{1}B_{2}B_{3}}.
\]

Then, qubit \( B_3 \) is measured in the generalized Fourier basis, given by the basis elements \( \{ |\alpha_l\rangle = \sum_{q} \exp(-2\pi i q/m) |q\rangle \} \), leading to a state

\[
\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i \frac{k}{m} l} |k, k \oplus j, 0, \frac{k}{d/m}\rangle |A_{1}B_{1}B_{2}B_{3} \},
\]

where \( l \) refers to the outcome \( |\alpha_l\rangle \) obtained. By simply applying a phase gate on party \( A \) of the from

\[
U_{A_{1}} = \sum_{k=0}^{d-1} e^{-2\pi i \frac{k}{m} l/m} |k\rangle \langle k|,
\]

the initial auxiliary state is recovered.

**Fidelity discrimination.**– The coarse graining strategy is also directly applicable for fidelity discrimination. In this case, to enhance its performance, the dimension of the extra register should be chosen depending on the possible fidelity values \( F_1, F_2 \). Performance is comparable as the efficiency for the witnessing problem.

### D. Protocol P3: Ensemble blocking

We finally consider a strategy based on parity measurements of subsets or blocks of the ensemble. In contrast to the previously discussed protocols P1 and P2, this approach is not limited to states \( \rho_\psi \) resulting from amplitude damping, but also to other state families such as Werner states \( \rho_\sigma \).

where the projector act on the \( \mathcal{H}_{B_{2}} \otimes \mathcal{H}_{B_{3}} \) Hilbert space.

In case the outcome \( M(\mathbb{I} - M) \) is found, we conclude that the fidelity of the probe ensemble states is above (below) the threshold \( F_0 \), up to certain failure probability. Importantly, the process only consumes the entanglement required to teleport qubit \( A_2 \) to party \( B \). We consider the number of ebits required by the process (see Sec. 11E) to evaluate the protocol performance. From a practical perspective, the entanglement required for the teleportation can be obtained by entanglement distillation means (see e.g. [26, 35]) of the ensemble copies directly.

In order to properly understand the effect of the measurement \( \{ M, \mathbb{I} - M \} \), we can classify the values of \( j \) in four sets (see Fig. 5):

\[
\begin{align*}
\Lambda_1 &= \{ 0, \ldots, (d_0 - 1)d \} \\
\Lambda_2 &= \{ (d_0 - 1)d + 1, \ldots, d_0d - 1 \} \\
\Lambda_3 &= \{ d_0d, \ldots, (m - 1)d \} \\
\Lambda_4 &= \{ (m - 1)d + 1, \ldots, d - 1 \},
\end{align*}
\]

where \( d = d/m \). The measurement given by Eq. (35) can deterministically distinguish between sets \( \Lambda_1 \) and \( \Lambda_3 \), such that in case \( j \) lies either in \( \Lambda_1 \) or \( \Lambda_3 \), the decision problem is solved deterministically and the auxiliary state is recovered untouched (see below). This is however not the case for the set \( \Lambda_2 \), for which certain overlapping exists that has to be taken into account. In summary, depending on where the actual set where \( j \) lies, the success probability of the witnessing problem reads

\[
\begin{cases}
\Pr(M) = 1 & \text{if } j \in \Lambda_1 \\
\Pr(M) = 0 & \text{if } j \in \Lambda_3 \\
0 < \Pr(M) < 1 & \text{if } j \in \Lambda_2 \cup \Lambda_4.
\end{cases}
\]

The performance of the protocol can be directly analyzed given the previous reasoning and given the probability distribution of the \( j \) value as a function of the state fidelity. Fig. 6 shows the efficiency for different settings and ensemble sizes. Observe how for the witnessing problem of determining whether the value of the fidelity is \( F > F_0 + \Delta \) or \( F < F_0 - \Delta \), the success probability of the protocol can approach 1 for relatively small additive error \( \lambda \).

Once the decision problem is solved, the last step of the protocol entails the recuperation of the auxiliary state, which has been entangled with the extra register during the process. The following steps are required to disentangle the extra register and leave the auxiliary state—and the entanglement associated—untouched. First, the operation \( U_{B_{1}B_{2}} \), Eq. (32), is undone on the remaining measured state Eq. (34), i.e.

\[
\begin{align*}
U_{B_{1}B_{2}}^\dagger \langle \psi \rangle_{A_{1}B_{1}B_{2}B_{3}} \\
&= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i \frac{k}{m} l} |k, k \oplus j, 0, \frac{k}{d/m}\rangle |A_{1}B_{1}B_{2}B_{3} \},
\end{align*}
\]

Then, qubit \( B_3 \) is measured in the generalized Fourier basis, given by the basis elements \( \{ |\alpha_l\rangle = \sum_{q} \exp(-2\pi i q/m) |q\rangle \} \), leading to a state

\[
\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i \frac{k}{m} l} |k, k \oplus j, 0, \frac{k}{d/m}\rangle |A_{1}B_{1}B_{2}B_{3} \},
\]

where \( l \) refers to the outcome \( |\alpha_l\rangle \) obtained. By simply applying a phase gate on party \( A \) of the from

\[
U_{A_{1}} = \sum_{k=0}^{d-1} e^{-2\pi i \frac{k}{m} l/m} |k\rangle \langle k|,
\]

the initial auxiliary state is recovered.

**Fidelity discrimination.**– The coarse graining strategy is also directly applicable for fidelity discrimination. In this case, to enhance its performance, the dimension of the extra register should be chosen depending on the possible fidelity values \( F_1, F_2 \). Performance is comparable as the efficiency for the witnessing problem.

### D. Protocol P3: Ensemble blocking

We finally consider a strategy based on parity measurements of subsets or blocks of the ensemble. In contrast to the previously discussed protocols P1 and P2, this approach is not limited to states \( \rho_\psi \) resulting from amplitude damping, but also to other state families such as Werner states \( \rho_\sigma \).
**Fidelity witnessing.**—Given an ensemble of $N$ unknown states we first depolarize them into a Werner state form, i.e., $\rho^{\otimes N} \mapsto \tilde{\rho}^{\otimes N}$, see Sec. II C. Then, we divide the ensemble in $n$ blocks of $r$ states each. Making use of bilateral CNOT gates, in analogy to purification hashing techniques [39], which act locally from the states of each block into one of the states, we can learn the parity of each block (see Fig. 7), i.e.,

$$\text{CNOT}_{1 \rightarrow 2} \otimes \text{CNOT}_{1 \rightarrow 2} |\Psi_{ij}\rangle A_i B_i |\Psi_{kl}\rangle A_k B_k = |\Psi_{ij(k,j)}\rangle A_i B_i |\Psi_{kl(i,j)}\rangle A_k B_k \quad (41)$$

Note that maximally entangled copies are not required since the parity can be encoded in one of the states of the block. We denote as $\kappa$ the number of even parities obtained, whose probability follows a binomial distribution of the form

$$\text{Pr}(\kappa|\rho) = \binom{n}{\kappa} [\pi_0(\rho^{\otimes r})]^{n-\kappa} [1 - \pi_0(\rho^{\otimes r})]^{\kappa}, \quad (42)$$

where the probability of measuring even parity in a block of size $r$ is

$$\pi_0(\rho^{\otimes r}) = \sum_{k=0}^{\lfloor r/2 \rfloor} \left( \frac{r}{2k} \right) A^{r-2k} (1 - A)^{2k}, \quad (43)$$

where $A \equiv (1 + 2F^*)/3$.

Since $\kappa$ is given by a binomial distribution, we can then repeat the same analysis performed for Protocol P0 (see Sec. IV A), but using $\text{Pr}(\kappa|\rho)$ instead of $\text{Pr}(j|F)$. Observe how, despite $N$ states are involved in the protocol, only $n$ are destroyed and the remaining $(r-1)n$ states are now correlated. After the first parity round is complete, the fidelity of the remaining states is changed depending on the value of the parity obtained. Due to the back-action effect of the bilateral control gate, see Eq. (41), the expected value of the local fidelity is given by

$$F' = F^2 + F \left(1 - \frac{F}{3}\right) + 2 \left(1 - \frac{F}{3}\right)^2. \quad (44)$$

The performance of the protocol can be further enhanced in case the initial states of the ensembles are of certain form. One case of particular interest involves states affected by dephasing type noise, Eq. (7), for which the first depolarization step is not required. For these kind of states, there is no back-action effect from the bilateral CNOT gate, and hence the average fidelity remains unchanged, i.e., $F' = F$.

Additionally, one can implement a second round of parity measurements for further enhancing the performance. This is accomplished by simply learning again the parity of the blocks where an even parity was found, leading to a recursive improvement on the protocol efficiency.

From the value of $\kappa$ we can again solve the fidelity witnessing problem following an analogous analysis as the one described for protocol P0, Sec. IV A, by including the block size $r$ as an extra parameter to consider, such that the success probability can be optimized by simply defining a block size $r^*$ that maximizes it i.e.,

$$\int_0^1 P_s(r, F) \, dF = \max_r \int_0^1 P_s(r, F) \, dF. \quad (45)$$

**Protocol P3:** Ensemble blocking

**Input:** Ensemble of $n$ identical noisy Bell states.
1. Depolarize the ensemble to the form of Eq. (5).
2. Apply bilateral CNOT gates Eq. (41) from ensemble blocks to some target ensemble states.
3. Learn the parity of each block by measuring the target states.
4. If $\kappa \in \sigma$ assume $F > F_0$, where $\kappa$ is the number of even parities.

**Output:** The fidelity of the initial ensemble was above or below $F_0$ with some success probability $P_s$.

---

*Fig. 7.* Schematic representation of the blocking strategy (P3). The initial ensemble of $n$ Bell diagonal states is divided in several blocks of size $r$. Then, the parity of each block is encoded in one of the states which later is measured reveling the actual parity value of the block. From the number of obtained “even” parities we can determine if the initial fidelity $F$ was above or below the threshold $F_0$ with some success probability.

**Fidelity discrimination.**—The value of even parities $\kappa$ can be also used to solve the discrimination problem. In this case, the optimal $r^*$ is such that the difference of obtaining an even parity is maximum, i.e.,

$$\pi_0(\rho_1^{\otimes r^*}) - \pi_0(\rho_2^{\otimes r^*}) = \max_r \left( \pi_0(\rho_1^{\otimes r}) - \pi_0(\rho_2^{\otimes r}) \right), \quad (46)$$

where the larger the difference, the more distinguishable the two probability distributions are. Importantly, the blocking strategy allows us to overcome the optimal success probability for fidelity discrimination by involving the whole ensemble in the process but only partially consuming it.

Figures 8a and 8b show the performance of the blocking strategy, compared with protocol P0 based on individual measurements. Observe how the blocking strategy provides significant performance enhancement with respect to the individual measurements strategy (P0).

**V. COMPARISON OF APPROACHES**

In order to compare different protocols, we use the number of required resources $R$ to obtain a certain success probability $P_s$ as measure. We demand that the success probability for a fixed fidelity is the same for all protocols. We use the success probability of
the single-copy approach P0 as a reference value, and adjust the parameters of the other protocols to guarantee that they lead to the same or a larger success probability. The resources are the number of copies that are measured and hence destroyed. Notice that for the error counting and coarse graining protocols, P1 and P2, we also take the cost for used maximally entangled auxiliary states into account. In order to do so, we assume that these auxiliary states are generated from noisy states of the ensemble, e.g., via entanglement purification, where the yield \( Y \) of the entanglement purification protocol (a combination of the recurrence protocol of [41] and hashing [39]) determines how many noisy copies correspond to a perfect ebit. For an entangled auxiliary register of dimension \( d \), \( \log_2(d)/Y \) states of the ensemble are required.

An overview over the applicability and strengths of the different protocols is given in Table V. All protocols are applicable for states of the form \( \rho_\eta \) resulting from amplitude damping, where both P1 and P2 give an (up-to) exponential advantage as compared to the standard approach P0. Notice that the error counting and coarse graining protocols P1 and P2 are not efficient for Werner states. However, the blocking protocol P3 still outperforms the standard approach P0 also in this case, as is shown in figures 8a and 8a.

In Fig. V we compare the different protocols (see also Table I), and plot the required resources \( r \) as a function of the fidelity of the initial states in the ensemble for the fidelity witnessing problem, i.e., to decide if the state has a fidelity larger or smaller than \( F_0 \). One clearly observes that P1 and P2 offer a large improvement for fidelities that are close to the threshold fidelity \( F_0 \), though they work even better if one excludes a small interval around \( F_0 \), i.e. considers the promise problem that \( F \geq F_0 + \lambda/2 \) or \( F < F_0 - \lambda/2 \). Similarly, for the fidelity discrimination problem one obtains an even larger improvement for P1 and P2.

VI. CONCLUSIONS AND OUTLOOK

In this work we have considered verification of noisy entangled states, with the aim to decide if the quality of states in a (large) ensemble is sufficient to use them for some desired application. We introduced methods to distinguish between two sets of entangled states by means of local operations and classical communication, eventually assisted by entanglement. We have concentrated on specific state families and the fidelity as central feature. Specifically, we introduced protocols to solve the decision problems of determining if the ensemble consists of states with fidelity \( F_1 \) or \( F_2 \) (discrete sets), or if the fidelity of the states is above or below a certain threshold value \( F_0 \), possibly excluding a small interval around \( F_0 \). The nature of the problem that we called fidelity witnessing requires as output only one bit of information, in contrast to well-studied problems such as state tomography or fidelity estimation, where a significantly larger amount of in-
Table I. General comparison between protocols. We use the required resources $R$ to obtain a certain success probability $P_s$ as a figure of merit to assess the performance of the different protocols, where we denote by $R_0$ the required resources of the reference protocol P0 to achieve $P_s$, and we demand the same or larger success probability for the other protocols. The resources depends on the problem setting (threshold fidelity $F_0$ in witnessing and $F_1, F_2$ in discrimination) and the required success probability. $\alpha(n)$ and $\beta(F_0)$ are factors that depends on the ensemble size or the threshold fidelity respectively, and which are typically smaller than 1, i.e. they indicate an improvement over P0. Efficient variants of the P1 and P2 protocols that offer an exponential improvement over P0 are not known for dephasing and Werner type states.

![Protocol efficiency: required resources R](image)

formation needs to be determined. As a first result, we have found that this practically relevant decision problem can for some state families, e.g. resulting from imperfect storage with decay as dominant noise source, be solved more efficiently than using fidelity estimation or full state tomography.

Perhaps more importantly, we demonstrate that using a larger ensemble while measuring and hence consuming only a small subset of states, provides a significant advantage. This is similarly in spirit as utilized in [26, 27] in the context of entanglement purification or state certification, but generalizes and extends these ideas in a non-trivial way and makes them applicable to new problems. This in fact leads to an up-to exponential improvement as compared to methods, extensions of state verification [20–25], that operate on ensembles of fixed size where all states are measured. Some protocols we introduce in this context operate on states of the ensemble directly (protocol P3), without any extra resources, where blocks of certain size are locally manipulated by collective operations and only few states are measured. The rest of the ensemble remains intact and can be used for the desired application after successful verification. Other approaches we introduce, such as protocols P1 and P2, require auxiliary entangled states to write in and read out relevant information of the whole ensemble. While in protocol P1 this auxiliary register is measured and hence destroyed, in protocol P2 the information is first coarse-grained, and most of the auxiliary entanglement is preserved and can be recovered. Only the read-out of a small amount of coarse-grained information is required, and little entanglement is consumed to access this (non-local) information with local operations only. It is in fact the latter protocol that yields a provable exponential advantage as compared to strategies that operate on fixed-size ensembles that are fully measured. Notice that consumed auxiliary entanglement can be directly related to the number of copies of states in the ensemble that need to be measured. One may either actually use noisy states from the ensemble as auxiliary states, or first produce e.g. by means of entanglement purification high fidelity or even perfect auxiliary entangled states from noisy copies. The conversion rate is given by the performance of entanglement purification, where reachable bounds are known. One can hence translate also protocols using auxiliary entanglement into schemes that only use noisy states from the ensemble, and find the total number of consumed states. This allows one to compare the different strategies, and assess performance (e.g. success probability) for a given number of consumed copies - or the required number of copies to reach a certain accuracy.

We remark that the ideas and tools we present here are not limited to the specific state classes we consider, but may be more broadly applicable. For instance, we believe that a generalization to multipartite entangled state such as GHZ states or certain graph states is straightforward, and will be presented elsewhere. Also the idea of using a larger ensemble, concentrating information and measuring only a small fraction might be useful for other related problems, such as e.g. for improving fidelity estimation.

**ACKNOWLEDGMENTS**

This work was supported by the Austrian Science Fund (FWF) through projects No. P30937-N27 and No. P36009-N.

---

[1] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[2] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics 8, 595 (2014).
[3] S. Wehner, D. Elkouss, and R. Hanson, Science 362 (2018), 10.1126/science.aam9288.
[4] A. Pirker and W. Dür, New Journal of Physics 21, 033003 (2019).
[5] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, AVS Quantum Science 3, 014101 (2021).
[6] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A 59, 4249 (1999).
[7] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, IEEE Network 34, 137 (2020).

---
