Improving Optimal Quantum State Verification

Jorge Miguel-Ramiro, Ferran Riera-Sàbat and Wolfgang Dür
Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, 6020 Innsbruck, Austria

Maximally entangled states are a key resource in many quantum communication and computation tasks, and their certification is a crucial element to guarantee the desired functionality. We introduce collective strategies for the efficient, local verification of ensembles of Bell pairs that make use of an initial information and noise transfer to few copies prior to their measurement. In this way the number of entangled pairs that need to be measured and hence destroyed is significantly reduced as compared to previous, even optimal, approaches that operate on individual copies. We show that our tools can be extended to other problems and larger classes of multipartite states.

Introduction.—With the emergence of quantum technologies, certification and verification of quantum devices and states becomes a necessary requirement for viable quantum communication and computation tasks, such as e.g. quantum teleportation, quantum key distribution, and distributed or blind quantum computation. In particular, certification of maximally entangled states by local operations is a crucial ingredient for a feasible implementation of bottom-up and entanglement-based quantum networks, where entanglement is a key resource to enable e.g. long-distance communication, various security applications or connecting distributed quantum processors. However, local measurements destroy entanglement, making the verification of entangled states costly.

Different approaches for certifying quantum states exist. Some of them, as state tomography, are however very inefficient as all elements of the density matrix need to be determined by means of destructive measurements. A protocol called Quantum State Verification was introduced in, in order to efficiently verify quantum states with local measurements, with just a constant overhead with respect to optimal global strategies. Several extensions have been proposed, and were implemented experimentally. These approaches rely in general on suitable sequential pass-or-fail measurements applied on individual quantum states. However, the improved control of quantum systems makes also more advanced, collective strategies that operate jointly on multiple copies feasible.

Here we show that such a collective but local strategy can significantly improve the efficiency of previous, even global and optimal, strategies based on sequential measurements of single copies. Our approach operates on multiple copies of entangled states, where only few of these states are designated for certifying the whole ensemble. This is achieved by accumulating the noise of the whole ensemble into a reduced set of states by collective local operations, so that by measuring the reduced set one can detect the noise with enhanced probability, consuming only the copies of that set. This significantly reduces the amount of entanglement that is destroyed due to the certification process. We adapt techniques from entanglement purification in order to transfer noise from states in the ensemble into a few target states that are then measured. Crucially, the non-measured states remain untouched and hence entangled, and can still be used as a resource for various non-local quantum tasks. Although we focus on maximally entangled Bell states throughout this work, with particular applicability in communication scenarios, we remark that our techniques can be extended to different quantum states, including e.g. maximally entangled qudit states or multipartite GHZ states.

Problem statement.—Consider an ensemble of n identical copies of some arbitrary bipartite entangled state \( \rho_{AB} \) shared by to parties A and B, ideally prepared in the maximally entangled state \( |\Psi_0\rangle \rho_{AB} |\Psi_0\rangle \), where we denote by \( |\Psi_0\rangle \rho_{AB} \) the four Bell states. There is the promise that the states are all either perfect, i.e., \( \rho_{AB} = |\Psi_0\rangle \rho_{AB} |\Psi_0\rangle \), or they have some noise corresponding to a mixed state \( \rho \) with unknown fidelity \( F = \langle \Psi_0 \mid \rho \mid \Psi_0 \rangle \leq 1 - \epsilon \). Some verification device is able to perform local operations on the parts of the states at A and B with the task of discerning which is the case, with a failure probability \( \delta_{\text{fail}} \). In this process, part of the ensemble is destroyed in order to examine whether \( F = 1 \). If that is the case, the conclusion is extended to the whole ensemble. Otherwise, all states are discarded. We consider this scenario and we show how our collective approach outperforms previous optimal strategies based on individual measurements.

The counter gate and d-level systems.—Our protocol relies on the usage of an auxiliary bipartite entangled state of qudits of certain dimension \( d \) to encode information on the whole ensemble, similarly as in recent entanglement purification protocols. In particular, we denote the d-dimensional maximally entangled states as \( |\Phi_{mn}^d\rangle_{AB} = \sum_{k=0}^{d-1} e^{i \frac{2\pi}{d} km} |k\rangle_A |k\otimes n\rangle_B / \sqrt{d} \), where \( k \otimes n \equiv (k-n) \mod d \) and the index \( m(n) \) is called amplitude (phase) index. The auxiliary state is used to accumulate and measure the noise of an ensemble of multiple noisy states. This process is achieved by means of the so-called counter gate, that transfers information from the ensemble of qubit states into the amplitude index of the d-dimensional auxiliary state. This amplitude index can be read by locally measuring in the \( Z_A \) and \( Z_B \) basis, the generalization of the Pauli \( \sigma_z \) basis for qudits. The counter gate is defined as a bilateral controlled-X gate, acting from a qubit pair as the source, to a qudit pair as the target. If the target system is in a maximally entangled state with phase index zero, its action is given by

\[
bCX_{1 \leftrightarrow 2} |mn\rangle_1 |\Phi_{0j}^d\rangle_2 = |mn\rangle_1 |\Phi_{0j \oplus m \oplus n}^d\rangle_2.\]

where \( bCX_{1 \leftrightarrow 2} = CX_{A_1 \rightarrow A_2} \otimes CX_{B_1 \rightarrow B_2} \), and \( CX_{1 \rightarrow 2} \) is the
hybrid controlled-X gate \( \text{CX}_{1\rightarrow 2} = |0\rangle\langle 0| \otimes \mathbb{I}_d + |1\rangle\langle 1| \otimes X_d \). For convenience, 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, Eq. (1), from a type-1(2) error state acting as control, leads to the amplitude index value of the auxiliary state increased(decreased) by one, whereas it is left invariant if the control is a type-3 error state. Importantly, this invariance property also applies in case that the control system is in the \(|\Psi_{00}\rangle\) state.

Proof of concept.— We start by providing a basic example based on simplified assumptions in order to illustrate the details of our procedure. As stressed below, one can relax these assumptions to consider a completely general situation.

Consider an ensemble of identical copies with the promise that all the states are either perfect Bell states \(|\Psi_{00}\rangle\langle \Psi_{00}|\), or rank-2 states with only type-1 errors, i.e., \(\rho = F|\Psi_{00}\rangle\langle \Psi_{00}| + (1 - F)|01\rangle\langle 01|\). This corresponds (up to local unitaries) to a situation where independent decay channels act on a maximally entangled state \(|\Psi_{10}\rangle\langle \Psi_{10}|\). Such decay noise is a prominent noise source in atomic or ensemble-based quantum memories where electronic excitation decay, but also describes photon loss when using a photon numbering encoding. The protocol comprises the following steps (see also Fig. 1). First, we apply the counter gate Eq. (1) from each of \(n\) states in the ensemble to some available auxiliary entangled state \(|\Phi_{00}\rangle\langle \Phi_{00}|\) with \(d = d + 1\), which acts as target. We denote this operations together as the error number gate (ENG). The ENG changes the amplitude index of the auxiliary state depending on the actual form of the ensemble. (i) Pure ensemble: The ensemble is given by \(n\) copies of the \(|\Psi_{00}\rangle\langle \Psi_{00}|\) state, and the application of the ENG leaves the auxiliary state invariant. (ii) Noisy ensemble: The ensemble is given by \(n\) noisy copies and it can hence contain type-1 error states. Whenever the counter gate is applied with a single type-1 error state, the amplitude index of the auxiliary state is increased by one. After the application of the ENG the ensemble and auxiliary states get correlated, i.e.,

\[
\text{ENG} : \rho^{\otimes n} \otimes |\Phi_{00}\rangle\langle \Phi_{00}| \rightarrow \sum_{j=0}^{n} \binom{n}{j} F^{n-j} (1 - F)^j \Gamma_j \otimes |\Phi_{0j}\rangle\langle \Phi_{0j}|,
\]

(2)

where \(\Gamma_j\) is a density operator corresponding to all permutations of \(|\Phi_{00}\rangle\otimes|\Phi_{00}\rangle\Rightarrow|\Phi_{0j}\rangle\otimes|\Phi_{0j}\rangle\rangle\)

By measuring the auxiliary state, we learn the value of \(j\), each found with probability \(p(j) = \binom{n}{j} F^{n-j}(1 - F)^j\), what depends on the state fidelity \(F\). In this case, the value of \(j\) indeed corresponds to the actual number of errors in the ensemble, and one can use this information to estimate the fidelity.

Whenever a value \(j \neq 0\) is found, we can assert with certainty that we are in case (ii) and the ensemble is noisy with \(F < 1\). On the other hand, if we obtain \(j = 0\) we conclude, with some success probability, that the states of the ensemble are perfect Bell pairs \(F = 1\) (case (i)). In particular, the failure probability of measuring \(j = 0\) if the initial state was \(\rho^{\otimes n}\) is \(\delta = F^n\). In this case we failed to identify the noisy ensemble, and would draw a wrong conclusion. For a fixed failure probability, one can determine the minimum number of ensemble states \(n\) (and therefore the minimum dimension of the auxiliary state) necessary to identify the case (i). Notice that the dimension \(d\) of the auxiliary state increases linear with \(n\), leading to an amount of entanglement (e-bits) that only scales logarithmic with \(n\), \(\mathcal{O}(\log n)\). As we show below, this corresponds to the number of states from the initial ensemble that needs to be measured and destroyed.

A further improvement is possible. Since we are only interested in detecting whether \(j \neq 0\), directly measuring the whole auxiliary state might not be the most efficient strategy as in this case the whole auxiliary state (and its entanglement) is destroyed. By performing a two outcomes measurement on each part of the auxiliary ensemble of the form \(|\Phi_{10}\rangle\otimes|\Phi_{10}\rangle\Rightarrow|\Phi_{1j}\rangle\otimes|\Phi_{1j}\rangle\rangle\)

The noisy ensemble case is identified by consuming only 1 e-bit. On the other hand, if \(j\) even is found, the ensemble is considered to be perfect (option (i)) but with some failure probability \(\delta_1\). Such failure probability is now given by the probability of measuring that \(j\) is even, while the ensemble is still noisy, i.e., \(\delta_1 = \sum_{j=0}^{n/2} \binom{n}{j} F^{n/2}(1 - F)^j\). One can reduce the failure probability by iterative performing additional two outcome measurements of the same form, learning and consuming 1 e-bit of information from the auxiliary state. The \(m^{th}\) measurement can be written as \(|\Phi_{mj}\rangle\otimes|\Phi_{mj}\rangle\rangle\)

(3)

and it reveals whether the value of \(j\) is multiple of \(2^m\) (or 0), or not. The failure probability, i.e., the probability of the ensemble being noisy and the outcomes of all \(k\) measurements still coinciding for \(A\) and \(B\) is given by

\[
\delta_m = \sum_{k=0}^{n-2^m} \left( \frac{n}{2^m k} \right) F^{n-2^m k}(1 - F)^{2^m k}.
\]

(4)

For some fixed failure probability \(\delta_k\) one can hence ob-
tain the number \((m)\) of measurements—number of ebits—required as a function of the ensemble fidelity \(F\).

Observe that, in this case, by considering an asymptotically large ensemble \(n \to \infty\), the required auxiliary entanglement that needs to be consumed for a fixed failure probability becomes constant and independent of the fidelity of the initial states. In particular, the failure probability in the asymptotic case fulfills \(\delta_m = 2^{-m}\), where \(m\) is the number of subspaces measured. Note that the entanglement of the remaining subspaces is not spent nor destroyed.

**General case and results.**—We show now how all the assumptions can be relaxed and a completely general scenario can be tackled, exhibiting a performance enhancement with respect to previous approaches. We consider arbitrary ensembles, and importantly, the auxiliary state can be directly constructed from several copies of the ensemble states.

We have the promise that all the ensemble states are either perfect Bell states or Werner states \([28]\) of the form

\[
\rho = q |\Phi_0^d\rangle\langle\Phi_0^d| + \frac{1 - d}{d^2} \mathbb{1}_{d^2},
\]

where we restrict to the \(d = 2\) case, where the fidelity is given by \(F = (1 + 3q)/4\). This situation is completely general since any state can be brought to this Werner-type form my means of depolarization procedures \([28]\) without changing the fidelity. The protocol comprises the same steps as explained before, assuming for the moment (see below) that a maximally entangled state is available as auxiliary. However, one has to consider that now there are different kind of errors, i.e., type-1 that increase, type-2 that decrease and type-3 that leave invariant the value of the amplitude bit \(j\) of the auxiliary state under the action of the ENG operation. A single copy of a Werner state can be interpreted as a type-1, 2, 3 error state with probability \(p_{1,2,3} = (1 - F)/3\), and a Bell state with \(p_0 = F\). Therefore, when applying the ENG from an ensemble of \(n\) copies, the resulting value of the amplitude index of auxiliary state becomes \(j = \Delta_{12}\) mod \(d\), where \(\Delta_{12} = \#\text{type-1} - \#\text{type-2}\). The probability of obtaining a certain \(j\) is then given by

\[
\Pr(j) = \sum_{i,k,l=0}^{n} \frac{n!}{i!k!l!} \left(p_0 + p_3\right)^i p_1^k p_2^l.
\]

In each term of the sum, the number of type-1 and type-2 errors are given by \(k\) and \(l\) respectively, and the number of states that are either Bell states or type-3 error state is given by \(i\).

Note that the difference of errors can take \(2n + 1\) different values, i.e., \(\Delta_{12} \in \{-n, \ldots, n\}\), and hence we would need an auxiliary state of \(d = 2n + 1\) to distinguish between all of them. However, for our purpose we just need to determine when \(\Delta_{12} = 0\), and for that an auxiliary state of \(d = n + 1\) is sufficient, as \(\Delta_{12} = 0 \Leftrightarrow \Delta_{12}\) mod \((n + 1) = 0\). The failure probability, i.e., the probability of measuring \(j = 0\) but still being in the noisy case, reads now \(\delta = \Pr(j = 0)\).

We also consider the approach where only certain subspaces of the auxiliary state are measured. After measuring \(m\) subspaces, and following the same steps as before, one obtains information about the \(2^n\)-multiplicity value of the amplitude index \(j\). In this case, the probability of failing in determining the “good” scenario after measuring \(m\) different 2-level states is

\[
\delta_m = \sum_{k=0}^{\lfloor n2^{-m}\rfloor} \Pr(2^m k).
\]

Important, in the asymptotic limit we recover the constant behaviour, i.e., the number of copies for a fixed failure probability is insensitive to the fidelity of the initial states, such that \(\delta_m = 2^{-m}\), where \(m\) is the number of subspaces measured.

So far we have assumed, for illustrative purposes, that a maximally entangled auxiliary state is available. This assumption is however not necessary, and we show here that the \(d\)-level auxiliary state can be obtained by directly embedding —noisy— copies of the qubit ensemble states. Since the protocol is based on accumulating noise into the auxiliary state, by embedding several copies of the ensemble, the protocol performance is indeed enhanced, because noise already accumulates via embedding, before any other operation is applied. We define the embedding

---

**Algorithm 1:** General ENG protocol overview

**Input:** Ensemble of \(n\) identical quantum states, either \(|\Psi_0\rangle\) or general Werner-type states, Eq. (5), with \(F < 1\).

1. Construct an effective \(d = 2^m\) dimensional auxiliary state by embedding \(m\) —noisy— Bell pairs from the ensemble.
2. Apply the ENG between \(n = d - 1\) states of the ensemble and the auxiliary state.
3. Locally obtain the amplitude index \(j\) of the auxiliary state.

**Output:** Information of the number of errors contained in \(n\)-size ensemble. If \(j \neq 0\) the non-perfect case is identified with certainty. If \(j = 0\), the \(|\Psi_0\rangle\) case is identified with some failure probability.

**Algorithm 2:** Subspaces ENG protocol overview

**Input:** Ensemble of \(m\) identical quantum states, either \(|\Psi_0\rangle\) or Eq. (5).

1. Proceed as in Algorithm 1 steps 1-2.
2. Parties \(A\) and \(B\) measure the subspace corresponding to the first Bell pair of the auxiliary in computational basis.
3. If same measurement outcome is found in \(A\) and \(B\), measure the next Bell state subspace.
4. Continue until different outcome is found or until enough success probability is achieved after \(k\) rounds.

**Output:** \(2^k\)-multiplicity of the value of \(j\). The imperfect case is identified with certainty if measurement outcomes differ at any point, and the \(|\Psi_0\rangle\) case is identified with some failure probability that depends on the number of repetitions \(k\).
for perfect Bell states as
\[
\Phi_{00}^{\pm} = |\Psi_{00}^{\pm}\rangle_B^{\otimes k} = \frac{1}{\sqrt{2^k}} \sum_{i_1, \ldots, i_k} |i_k \ldots i_1\rangle_A |i_k \ldots i_1\rangle_B. \tag{8}
\]

This embedding with \( m \) copies of noisy Bell states \( \rho \) with fidelity \( F \), leads to a noisy \( d \)-level state of \( d = 2^m \). The resulting state can be always depolarized into an isotropic form \cite{29} of the form Eq. (3), with \( d = 2^m \) and \( q = (d^2 F^m - 1)/(d^2 - 1) \). If one directly measures the amplitude bit \( (j) \) of this state, before applying the ENG operation, the probability of measuring \( j = 0 \) is given by \( \delta = (1 + d^2 F^m)/(1 + d) \). The performance already approaches to the optimal possible strategy based on measurements –directly projecting the ensemble states into \( |\Psi_{00}\rangle \)–. The number of copies needed in this global optimal strategy based on measurements scales as \( k = \ln \delta / \ln F \) \cite{18, 30}. See Appendix B for more information.

One can however enhance the protocol performance –overcoming previous optimal single-copy strategies– by applying, as before, the ENG operation from the ensemble states into the auxiliary noisy state of Eq. (8). This process introduces and accumulates the noise of the ensemble states into the auxiliary and, together with the noise already accumulated by embedding, increases the probability of discerning between the perfect and the non-perfect case. As before, in case we detect noise in the ensemble, we discard all the states, whereas if we are in the perfect case the ensemble is kept and certified, and the only copies consumed are the ones corresponding to the embedding of the auxiliary state.

In order to construct an auxiliary state of dimension \( d = n + 1 \), which allows us to collect or accumulate information about the noise of \( n \) ensemble states, one just need to embed \( m = \log_2(n + 1) \) copies of the –noisy– ensemble. Therefore, only \( m \) copies are eventually consumed, and the dimension of the auxiliary scales exponentially with the number of embedded states, which leads to the exponential improvement in the scaling and allows us to overcome previous optimal bounds.

Fig. 2 shows several results comparing the performance of our protocol with respect to the best previous approaches based on individual measurements, under different situations. One can see an exponential-type improvement in all the cases. In particular, if an arbitrarily large ensemble is available, the subspaces ENG strategy exhibits a constant behaviour independent on the fidelity and the form of the initial states. We refer to Appendix C for further analysis.

Generalizations.— We have introduced tools and collective procedures to verify Bell states with improved performance with respect to previous ones. However, the applicability of our approach goes beyond Bell states. In particular, we show that these techniques can be applied to verify any set of states for which there exists a subspace which is invariant under the counter operations of Eq. 4 (or equivalent). In the case of the Bell-type states, the invariant subspace is spanned by \( |00\rangle \) and \( |11\rangle \), and therefore any state \( |\Psi_{00}\rangle \) leaves the auxiliary state invariant after the application of the counter gate, i.e., \( b\text{CX} |\Psi_{00}\rangle |\Phi_{ij}^D\rangle = |\Psi_{00}\rangle |\Phi_{ij}^D\rangle \).

Some instances of states that can be verified include maximally entangled qudit states, or more general multipartite states. For maximally entangled qudit states the generalization is very direct. One just need to generalize the controlled-X operations for qudit-qudit systems such that it acts as \cite{31} \( \text{GCX} |m\rangle |n\rangle = |m\rangle |n \oplus m\rangle \). When applied in a bilateral way between \cite{32} a bipartite qudits system and a maximally entangled system of dimension \( D \), the effect is \( b\text{GCX} |m^d n^d\rangle |\Phi_{0j}^D\rangle = |m^d n^d\rangle |\Phi_{0j}^D\rangle \) where \( j \oplus n \oplus m = (j - n + m) \mod D \) so that a similar effect than in the qubit case is achieved. Note that the dimension of the auxiliary should be adapted to the fact that errors can now increase or decrease the value of the amplitude bit of the auxiliary by more than one (up to \( d \)).

In a similar way, these techniques can be adapted to verify multipartite states. The invariant subspace of the generalized counter gate \( m\text{CX} \) \cite{25} is spanned by \( |00 \ldots 0\rangle \) and \( |11 \ldots 1\rangle \), while the amplitude vector of the auxiliary \( d \)-level systems is modified depending on the error state. Therefore, a verification procedure for the GHZ state \((|00 \ldots 0\rangle + |11 \ldots 1\rangle)/\sqrt{2} \) is directly obtained by extending the protocol for Bell states, as after applying the extended ENG the probability of obtaining a zero-valued amplitude index approaches zero when the number of copies in the ensemble increases. However, to make
the procedure fully general extra operations are required to detect phase errors, see Appendix D for details. Extension to more general graph states, following [33, 34], might be possible.

Conclusions.— We have proposed techniques and collective protocols that allow us to verify maximally entangled quantum states with enhanced performance as compared to previous (even optimal) strategies that operate on individual states. This is accomplished by transferring and accumulating (via a so-called ENG operation) the noise of some ensemble of states into a higher-dimensional auxiliary state. This auxiliary state can be constructed using and embedding a logarithmically reduced number of ensemble copies, which are the only ones eventually consumed. Because of the embedding process and the ENG operation, noise is enlarged into the auxiliary state, making its detection more efficient. In addition, we propose an strategy based on measuring only certain subspaces of the auxiliary state, such that in the asymptotic limit of a large enough ensemble, a constant number of consumed copies is enough for verifying the states, independently on the fidelity or the form of the states. The tools we introduce and make use here are not only interesting in the context of certification of quantum states, but they can be particularly useful in other scenarios such as e.g. fidelity estimation or fidelity witnessing. For the rank-2 example originating from decay noise, we can actually use our strategy not only to verify the ensemble, but to accurately estimate the fidelity by using only a logarithmic amount of extra entanglement, exponentially outperforming single-copy strategies.

This work was supported by the Austrian Science Fund (FWF) through project No. P30937-N27.

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).
[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] C. H. Bennett and G. Brassard, Theoretical Computer Science 560, 7 (2014).
[4] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A 59, 4249 (1999).
[5] M. Hayashi and T. Morimae, Phys. Rev. Lett. 115, 220502 (2015).
[6] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory of Computing Systems 63, 715 (2019).
[7] H. J. Kimble, Nature 453, 1023 (2008).
[8] S. Wehner, D. Elkouss, and R. Hanson, Science 362, eaam9288 (2018).
[9] W. Kozlowski and S. Wehner, Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, NANOCON 2019 (3345-497).
[10] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, AVS Quantum Science 3, 014101 (2021).
[11] A. Pirker, J. Wallnöfer, and W. Dür, New J. Phys. 20, 053054 (2018).
[12] A. Pirker and W. Dür, New J. Phys. 21, 034003 (2019).
[13] C. Meignant, D. Markham, and F. Grosshans, Phys. Rev. A 100, 052333 (2019).
[14] L. Gyongyosi and S. Imre, Scientific Reports 9, 2219 (2019).
[15] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. 2, 382 (2020).
[16] X.-D. Yu, J. Shang, and O. Gühne, Statistical methods for quantum state verification and fidelity estimation (2021), arXiv:2109.10805 [quant-ph].
[17] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. 1, 1 (2010).
[18] S. Pallister, N. Linden, and A. Montanaro, Phys. Rev. Lett. 120, 170502 (2018).
[19] Z. Li, Y.-G. Han, and H. Zhu, Phys. Rev. A 100, 032316 (2019).
[20] K. Wang and M. Hayashi, Phys. Rev. A 100, 032315 (2019).
[21] C. Bădescu, R. O’Donnell, and J. Wright, in Proc. 51 Ann. ACM SIGACT Symp. Th. Comput. (ACM, 2019).
[22] H. Zhu and M. Hayashi, Phys. Rev. A 99, 052346 (2019).
[23] J. Morris, V. Saggio, A. Gočanin, and B. Dakić, preprint arXiv: 2109.03860 (2021).
[24] 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, and G.-C. Guo, Phys. Rev. Lett. 125, 030506 (2020).
[25] F. Riera-Sábat, P. Sokatski, A. Pirker, and W. Dür, Phys. Rev. Lett. 127, 040502 (2021).
[26] F. Riera-Sábat, P. Sokatski, A. Pirker, and W. Dür, Phys. Rev. A 104, 012419 (2021).
[27] J. Daboul, X. Wang, and B. C. Sanders, 36, 2525 (2003).
[28] R. F. Werner, Phys. Rev. A 40, 4277 (1989).
[29] M. Horodecki and P. Horodecki, Phys. Rev. A 59, 4206 (1999).
[30] H. Zhu and M. Hayashi, Phys. Rev. A 99, 052346 (2019).
[31] G. Alber, A. Delgado, N. Gisin, and I. Jex, J. Phys. A 34, 8821 (2001).
[32] J. Miguel-Ramiro and W. Dür, Phys. Rev. A 98, 042309 (2018).
[33] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. 91, 107903 (2003).
[34] C. Kruszynska, A. Miyake, H. J. Briegel, and W. Dür, Phys. Rev. A 74, 052316 (2006).
[35] W. Dür and J. I. Cirac, Phys. Rev. A 61, 042314 (2000).
Appendix A: Uncorrelating the auxiliary state

In the main text, we show how one can verify Bell states by using qudits systems obtained from the same noisy ensemble. However, one can also consider the approach where perfect auxiliary maximally entangled qudit states are used. This situation can be particularly useful in possible extensions of the protocol to perform different tasks, such as fidelity estimation. In this section, we show how by using pure auxiliary states, the protocol can be applied without consuming all the auxiliary entanglement.

Consider the Werner state with fidelity \( F \), i.e.,
\[
\rho = q |\Psi_{00}\rangle\langle\Psi_{00}| + \frac{1-q}{4} \mathbb{I},
\]
where \( q = (4F - 1)/3 \). We rewrite the state as
\[
\rho = (p_0 + p_3) \sigma + p_1 |01\rangle\langle01| + p_2 |10\rangle\langle10|
\]
where \( p_{1,2,3} = (1 - F)/3, p_0 = F \) and
\[
\sigma = \frac{1}{p_0 + p_3} (p_0 |\Psi_{10}\rangle\langle\Psi_{10}| + p_3 |\Psi_{10}\rangle\langle\Psi_{10}|).
\]
describes a state that that can be either the type-3 error state or the target Bell state.

If we apply the ENG between and ensemble of \( n \) copies of a Werner state, Eq. (A2), and an auxiliary maximally entangled state of the form
\[
|\Psi_{00}\rangle_{AB} = \frac{1}{\sqrt{n}} \sum_{i_1, \ldots, i_k = 0}^{\text{mod } n} |i_k, \ldots, i_1\rangle_{A_k \ldots A_1} |i_k, \ldots, i_1\rangle_{B_k \ldots B_1},
\]
the state of the whole system is transformed into
\[
\text{ENG} : \rho^\otimes n \otimes |\Psi_{00}\rangle\langle\Psi_{00}| \rightarrow \Omega = \sum_{j=0}^{d-1} p(j) \Gamma_j \otimes |\Phi_{0j}\rangle\langle\Phi_{0j}|,
\]
where
\[
p(j) = \sum_{i, k, \ell=0}^{n} \frac{n!}{i! k! \ell!} (p_0 + p_3)^i p_1^k p_2^\ell
\]
is the probability of measuring a difference of errors given by \( j = (k - \ell) \mod d \) and \( \Gamma_j \) is the density matrix describing the ensemble if a certain value of \( j \) is obtained, i.e.,
\[
\Gamma_j = \frac{1}{p(j)} \sum_{i, k, \ell=0}^{n} (p_0 + p_3)^i p_1^k p_2^\ell \Pi \left[ \sigma^\otimes i \otimes |01\rangle\langle01| \otimes |10\rangle\langle10| \right]
\]
where \( \Pi \) denotes the sum over all \( n!/(i! k! \ell!) \) permutations of the states.

After applying the ENG, we can obtain the parity of \( j \) by locally measuring qubits \( A_1 \) and \( B_1 \) in the Z basis, i.e., the measurement given by
\[
\mathcal{M} : \{M_1 = |00\rangle\langle00|, M_2 = |01\rangle\langle01|, M_3 = |10\rangle\langle10|, M_4 = |11\rangle\langle11|\}.
\]
If the outcomes of both measurements coincide, i.e., if we obtain \( M_1 \) or \( M_4 \), then \( j \) is even, otherwise \( j \) is odd. This measurement modify the auxiliary state, which is transformed as
\[
M_{1,4} |\Phi_{0j}\rangle = |\Phi_{d/2,0j/2}\rangle
\]
\[
M_2 |\Phi_{0j}\rangle = |\Phi_{d/2,0(j-1)/2}\rangle
\]
\[
M_3 |\Phi_{0j}\rangle = |\Phi_{d/2,0(j+1)/2}\rangle
\]
where systems $A_1$ and $B_1$ are no longer considered. After determining the parity of $j$ the state of the state of the ensemble also changes and whole system is given by

$$M_{1,4} \Omega M_{1,4} = \sum_{j \text{ even}} \Gamma_j \otimes |\Phi_{0,j/2}^d \rangle \langle \Phi_{0,j/2}^d|$$

$$M_2 \Omega M_2 = \sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,(j-1)/2}^d \rangle \langle \Phi_{0,(j-1)/2}^d|$$

$$M_3 \Omega M_3 = \sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,(j+1)/2}^d \rangle \langle \Phi_{0,(j+1)/2}^d|$$

(A10)

This step can be iterated obtaining the parity of the new amplitude index, and so on until $j$ is fully determined. However, our protocol aborts if a $j \neq 0$ is obtained. Therefore, if the auxiliary state is not fully measured and we already obtained that $j \neq 0$, we can uncorrelate the auxiliary system keeping the entanglement left.

Then, we can take a copies of an auxiliary pure Bell state $|\Psi_{00}\rangle$, and embed it in the remaining auxiliary state, what duplicating its dimension by two, i.e.,

$$\sum_{j \text{ even}} \Gamma_j \otimes |\Phi_{0,j/2}^d \rangle \langle \Phi_{0,j/2}^d| \otimes |\Psi_{00}\rangle \langle \Psi_{00}| = \sum_{j \text{ even}} \Gamma_j \otimes |\Phi_{0,j}^d \rangle \langle \Phi_{0,j}^d|$$

$$\sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,(j-1)/2}^d \rangle \langle \Phi_{0,(j-1)/2}^d| \otimes |\Psi_{00}\rangle \langle \Psi_{00}| = \sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,j\oplus 1}^d \rangle \langle \Phi_{0,j\oplus 1}^d|$$

$$\sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,(j+1)/2}^d \rangle \langle \Phi_{0,(j+1)/2}^d| \otimes |\Psi_{00}\rangle \langle \Psi_{00}| = \sum_{j \text{ odd}} \Gamma_j \otimes |\Phi_{0,j\oplus 1}^d \rangle \langle \Phi_{0,j\oplus 1}^d|$$

(A11)

where we use that

$$|\Phi_{0,j}^d\rangle_{A_1B_1} |\Psi_{00}\rangle_{A_2B_2} = \frac{1}{\sqrt{2^d}} \sum_{k=0}^{d-1} \left( |k,0\rangle_{A_1A_2} |k \oplus j,0\rangle_{B_1B_2} + |k,1\rangle_{A_1A_2} |k \oplus j,1\rangle_{B_1B_2} \right)$$

$$= \frac{1}{\sqrt{2^d}} \sum_{k'=0}^{2^d-1} |k'\rangle_A |k' \oplus 2j\rangle_B = |\Phi_{0,2j}^{2d}\rangle_{AB}.$$  

(A12)

Then by applying a certain correction operation depending on the measurement outcome, we obtain the same state before taking any measure $\Omega$. Note that this procedure can be iterated to recover the state $\Omega$ if 2m subsystems of the auxiliary system $A_m \ldots A_1B_m \ldots B_1$ have been measured. In this case, we need $m$ copies of the Bell state $|\Psi_{00}\rangle$.

Once the state $\Omega$ is recovered, we uncorrelate the auxiliary system form the ensemble by applying the inverse of the ENG i.e.,

$$\text{ENG}^1 : \Gamma_j \otimes |\Phi_{0,j}^d\rangle \langle \Phi_{0,j}^d| \rightarrow \Gamma_j \otimes |\Phi_{00}\rangle \langle \Phi_{00}|.$$  

(A13)

In this way, we can obtain the $m$-multiplicity of $j$ by consuming $m$ ebits.

**Appendix B: Alternative expression for the failure probability**

Here, we introduce an alternative expression to compute the failure probability, i.e., the probability $\delta$ of measuring $j = 0$ but still being in the non-perfect case. The failure probability is given by

$$\delta = \sum_{i=0}^{n} \binom{n}{i} q^{n-i}(1-q)^i \Omega_{(n-i)}.$$  

(B1)

where

$$\Omega_{(s)} = \sum_{j=0}^{s/2} \left( \frac{1}{4} \right)^{j} \left( \frac{1}{2} \right)^{s-2j} \frac{s!}{j!(s-2j)!}.$$  

(B2)

determines the number of situations where the value of $j$ is left invariant—the same number of increasing and decreasing errors for each value $s = n - i$.

We also consider the approach where only certain subspaces of the auxiliary state are measured. After measuring $m$ subspaces, and following the same steps as before, one obtains information about the $2^m$-multiplicity value of the
amplitude index $j$. In this case, the probability of failing in determining the perfect scenario after measuring $m$ different 2-level states is

$$\delta = 2 \sum_{i=0}^{n} \sum_{i=0}^{n} \binom{n}{i} q^i (1-q)^{n-i} \Omega(n-i,m),$$

where

$$\Omega(s,m) = \sum_{j=0}^{s} \binom{1/4}{j} \binom{1/4}{j+2m} \binom{1/2}{s-2j-2m} \frac{s!}{j!(j+2m)!!(s-2j-2m)!},$$

determines now the number of cases where the net sum of different error types is $m$-multiple of 2. Importantly, in the asymptotic limit we recover the constant behaviour, i.e., the number of copies for a fixed failure probability is insensitive to the fidelity of the initial states, such that $\delta_{fail} = 2^{-k}$, where $k$ is the number of subspaces measured.

Appendix C: Additional protocol performance analysis

We complete here the protocols analyses provided in the main text by including extra illustrative information for different problem settings.

Fig. 3 shows the performance of the protocols introduced in this work under different situations. Fig 3 (a), (b) represents the ratio or improvement of the protocols introduced in comparison to the best previously known strategies, for rank-2 and general Werner states respectively. One can see an exponential improvement in both cases. In addition, Fig 3 (c) shows the advantages derived from using the noisy states of the ensemble to construct the auxiliary states. By doing so, and before the ENG that accumulate noise on the auxiliary, a measurement on the auxiliary system would already reveal information very close to the previous optimal strategies. Finally, Fig 3 (d) stresses the suitability of using copies of the ensemble to construct auxiliary systems, and the enhancement obtained with our approaches.
Appendix D: m-party GHZ state

In a multipartite scenario, our verification protocol can be extended to verify m-partite GHZ states, i.e., the state given by

\[ |\text{GHZ}_m\rangle_{AB...M} = \frac{1}{\sqrt{2}} \left( |00...0\rangle_{AB...M} + |11...1\rangle_{AB...M} \right). \]  

(D1)

Consider the orthonormal qubit GHZ-basis given by

\[ |\Psi_{ij}\rangle_{AB...M} = \frac{1}{\sqrt{2}} \sum_{k=0}^{d-1} e^{i\pi k i} |k\rangle_A |k \oplus j_1\rangle_B \cdots |k \oplus j_{m-1}\rangle_M, \]  

(D2)

where \( i \) is the phase bit and \( j \) is the amplitude bit vector. Note that our target state corresponds to \( |\text{GHZ}_0\rangle = |\Psi_{00}\rangle \).

In a similar way as in the bipartite case, in this scenario the auxiliary system is given by a \( d \)-level \( m \)-partite GHZ state \(|\Phi_{00}^d\rangle\), with

\[ |\Phi_{ij}^d\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{d-1} e^{i\pi k |j|} |k\rangle \oplus j_1\rangle \cdots |k \oplus j_{m-1}\rangle, \]  

(D3)

where \( i \) is the phase index and \( j = (j_1, \ldots, j_{m-1}) \) is the amplitude vector. Note that in the bipartite case, one can obtain either the value of the phase index \( i \) or the value of the amplitude vector \( j \) by measuring each qubit on the \( X \) or the \( Z \) basis respectively and communicating the outcomes to the other parties afterwards.

We define the \( m \)-partite counter gate given by a multilateral control-\( X \) gate with a qubit system as a control and a qudit system as target, i.e.,

\[ m\text{CX} = \text{CX}_{A_1 A_2} \otimes \text{CX}_{B_1 B_2} \otimes \cdots \text{CX}_{M_1 M_2}, \]  

(D4)

with \( \text{CX}_{12} = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \). The action of the counter gate with respect to a state of the computational basis acting as control, and an a \( d \)-level system of the form \(|\Phi_{ij}^d\rangle\) as target, is given by

\[ m\text{CX} |i_1\rangle_{A_1} \cdots |i_m\rangle_{M_1} |\Phi_{ij}^d\rangle_{A_2...M_2} = |i_1\rangle_{A_1} \cdots |i_m\rangle_{M_1} \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k \oplus i_1\rangle_{A_2} |k \oplus j_1 \oplus i_2\rangle_{B_2} \cdots |k \oplus j_{m-1} \oplus i_m\rangle_{M_2}, \]  

(D5)

\[ = |i_1\rangle_{A_1} \cdots |i_m\rangle_{M_1} \frac{1}{\sqrt{d}} \sum_{k'=0}^{d-1} |k'\rangle_{A_2} |k' \oplus j_1 \oplus i_2 \oplus i_1\rangle_{B_2} \cdots |k' \oplus j_{m-1} \oplus i_m \oplus i_1\rangle_{M_2}, \]

\[ = |i_1\rangle_{A_1} \cdots |i_m\rangle_{M_1} |\Phi_{ij'}^d\rangle_{A_2...M_2}, \]

where the components of \( j' = (j'_1, \ldots, j'_{m-1}) \) are given by

\[ j'_k = j_k \oplus i_{k+1} \oplus i_1. \]  

(D6)

Note that the application of the counter gate transforms the amplitude vector of the auxiliary system for each state of the computational basis, except for the subspace span\{\( |00...0\rangle \), \( |11...1\rangle \}\) that leaves the \( d \)-level system invariant. In other words, if the control system is of the form \(|\psi\rangle = \alpha |00...0\rangle + \beta |11...1\rangle\), the counter gate leaves the target system unchanged, i.e.,

\[ m\text{CX} (\alpha |00...0\rangle + \beta |11...1\rangle) |\Phi_{ij}^d\rangle = (\alpha |00...0\rangle + \beta |11...1\rangle) |\Phi_{ij'}^d\rangle. \]  

(D7)

Therefore, the target state \(|\Psi_{00}\rangle\) keeps the auxiliary state invariant, and hence we can apply an analogous protocol as in the bipartite case, for noisy GHZ states. In the bipartite case, we can always depolarize the ensemble into an unknown collection of pure states, where each state is either the \(|\text{GHZ}_m\rangle\) state or an error state. However, in the multipartite case, we find that some kinds of errors cannot be detected with by means of the counter gate.

As shown in [55], for \( d = 2 \) (i.e. qubits) one can always depolarize any noise GHZ state \( \rho \) to the form

\[ \text{DEP}: \rho \rightarrow \rho = F|\Psi_{00}\rangle\langle\Psi_{00}| + \lambda_0 |\Psi_{10}\rangle\langle\Psi_{10}| + \sum_{k=1}^{2^{m-1}-1} \lambda_k (|0k\rangle\langle0k| + |1\bar{k}\rangle\langle1\bar{k}|), \]  

(D8)
where $|k⟩ = |k_{m-1}) \cdots |k_2) |k_1⟩$, with $k_i$ being the $i$-digit of $k$ in the binary form, and $|\tilde{k}⟩ = |\tilde{k}_{m-1}) \cdots |\tilde{k}_2) |\tilde{k}_1⟩$ with $\tilde{k}_j = k_j \oplus 1$. The values of $\lambda_k$ are given by

$$F = \langle \Psi_{00} | \rho | \Psi_{00} \rangle$$
$$\lambda_0 = \langle \Psi_{10} | \rho | \Psi_{10} \rangle$$
$$\lambda_k = \frac{1}{2} \left( \langle \Psi_{0k} | \rho | \Psi_{0k} \rangle + \langle \Psi_{1k} | \rho | \Psi_{1k} \rangle \right).$$

Note in the depolarization procedure the fidelity $F$ of the state and the weight of $|\Psi_{10}⟩⟨\Psi_{10}|$ given by $\lambda_0$ are kept. In this case it is hence necessary to differentiate between two sources of errors: amplitude error and phase errors. Amplitude error are given by states of the computational basis orthogonal to the target system, i.e., $\{|k⟩\}_{k=1}^{d-2}$. On the other hand, phase errors are described by the state $|\Psi_{10}⟩$. Note that if we apply the counter gate with a amplitude error state acting as a control, the auxiliary state is modified and the error can be probabilistically detected. However, if the control system is in a phase error the auxiliary state remains invariant and it cannot be detected. In conclusion, our protocol can be used to verify unknown noisy GHZ state when they are affected by amplitude errors.

To verify general noisy GHZ states, we can proceed with the standard protocol to probabilistically detect amplitude errors. Then, in case of no errors detected we can apply a second round with a different control operation to detect the phase errors. For instance, with an auxiliary system of $d = 2$, applying the counter gate with the auxiliary system as a control, i.e.,

$$mCX_{aux} → 1 |\Psi_{m0}⟩_1 |\Psi_{n0}⟩_{aux} = |\Psi_{m0}⟩_1 |\Psi_{n\oplus m,0}⟩_{aux},$$

the phase bit of the auxiliary system is changed if the control system is a phase error and it is leaved invariant if the control system is the target state.