Entanglement-Assisted Entanglement Purification

F. Riera-Sàbat, P. Sekatski, A. Pirker and W. Dür

1 Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, 6020 Innsbruck, Austria
2 Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Switzerland

(Dated: July 22, 2021)

The efficient generation of high-fidelity entangled states is the key element for long-distance quantum communication, quantum computation, and other quantum technologies, and at the same time the most resource-consuming part in many schemes. We present a class of entanglement-assisted entanglement purification protocols that can generate high-fidelity entanglement from noisy, finite-size ensembles with improved yield and fidelity as compared to previous approaches. The scheme utilizes high-dimensional auxiliary entanglement to perform entangling nonlocal measurements and determine the number and positions of errors in an ensemble in a controlled and efficient way, without disturbing the entanglement of good pairs. Our protocols can deal with arbitrary errors, but are best suited for few errors, and work particularly well for decay noise. Our methods are applicable to moderately sized ensembles, as will be important for near term quantum devices.

Introduction. — Entanglement plays a dominant role in most applications of quantum technologies, ranging from metrology [1–3] and quantum computation [4–9] to quantum communication. Quantum advantages in metrology are based on using entangled states, and there exist models for quantum computation where information processing takes place solely by performing measurements on universal resource states [7–9], or certain gates are implemented in a fault-tolerant fashion by consuming (magic) entangled states [10–12]. Most importantly, quantum networks [13, 14] and long-distance quantum communication are based on the generation of high-fidelity entanglement using quantum repeaters [15–24]. The key elements in all these schemes are methods to generate and maintain high-fidelity entanglement. Entanglement purification protocols (EPPs) [25–50] achieve this aim by locally manipulating ensembles of multiple copies of noisy entangled states in such a way that fewer copies with increased fidelity are produced. The yield and the reachable fidelity of these schemes determine the performance of higher-level applications, as EPPs are used as elementary blocks that are e.g., in the case of quantum repeaters, iteratively applied and, in fact, give rise to the major part of the required resources [15, 16, 28]. Improving the efficiency of these schemes has hence a huge impact on the performance of entanglement-based quantum technologies.

Here we introduce a class of entanglement-assisted entanglement purification protocols with improved yield and reachable fidelity. The basic idea is to use auxiliary, high-dimensional entangled states to read out locally inaccessible information about an ensemble of noisy entangled states, thereby purifying it. The advantage that qudits instead of qubits provide in quantum information theory has already been shown, and many experimental demonstrations regarding the control and generation of entangled d-level systems have been reported [51–54]. In contrast to asymptotic schemes such as hashing or breeding [26], the usage of high-dimensional entanglement allows for direct and controlled access to the number, type, and position of errors and the design of efficient schemes that work for an arbitrary finite number of copies. Our error identification protocols (EIPs) interpolate between recurrence protocols [25–28] that operate on few copies and are iteratively applied and asymptotic schemes [26, 28] that operate on large ensembles where partial information is repeatedly accessed and interpreted using laws of large numbers, but outperform both in the important regime of small and moderate number of copies. The EIPs can deal with any noise, including nonindependent identically distributed (IID) situations, but are particularly simple and efficient if the dominant noise process is such as decay. This is the case for many setups, where, e.g., the decay of an excited state of an atom or the loss of a photon (in photon-number entanglement) constitute most relevant processes. Even though the EIPs require auxiliary entanglement, we show how to use only noisy states from the initial ensemble and to deal with errors in operations (in a similar fashion as the breeding protocol leads to hashing). The key ingredient of our protocols is a class of entangling nonlocal measurements, implemented via local operation and classical communication with the help of auxiliary entanglement. This method to read out locally inaccessible information is, however, not limited to EPP, but can in fact be used whenever such “nonlocal information” about ensembles should be learned, e.g., for entanglement certification or decision problems.

Setting. — We consider two parties sharing an ensemble \( \Gamma = \rho^{\otimes n} \) of \( n \) copies of a noisy Bell state \( \rho \) with initial local fidelity \( F = \langle \Psi_{00} | \rho | \Psi_{00} \rangle \) and global fidelity \( F_g = \langle \Psi_{00}^{(\otimes n)\Gamma} | \Psi_{00}^{(\otimes n)} \rangle \). Here we denote by \( | \Psi_{ij} \rangle_{AB} = 1 \otimes \sigma_i \Psi_{j}^{(00)}_{AB} + |11\rangle_{AB} / \sqrt{2} \) the four Bell states, and we consider shared auxiliary maximally entangled states of qudits \( | \Psi_{00}^{(d)} \rangle \), where \( | \Psi_{mn}^{(d)} \rangle_{AB} = \sum_{k=0}^{d-1} e^{i2\pi km/d} |k\rangle_A |k\otimes n\rangle_B / \sqrt{d} \). By performing local operations, the parties aim to purify the ensemble, i.e., probabilistically generate a new ensemble \( \Gamma' \) of 2m qubits, with increased global fidelity \( F_g' \) or local fidelity \( F^{(k)} = \langle \Psi_{00}^{(\otimes n)\Gamma'} | \Psi_{00}^{(\otimes n)} \rangle \). Usually, we are concerned with reaching a certain global or local target fidelity and define the yield of the procedure as \( Y = m'/n \), where \( m' \) is the number of final copies that fulfill this fidelity criterion. The prime on \( m' \) indicates that auxiliary entanglement that was consumed during the process needs to be restored from the \( m' \) output pairs. For a better comparison, we assume that \( \nu \) pairs with fidelity \( F \) correspond to a maximally entangled system with \( d = 2^{(1-S(F))\nu} \), which corresponds to the (reachable) yield of the asymptotic hashing protocol. Here, \( S(F) \) denotes the entropy with respect to diagonal
coefficients of the state in the Bell basis, and we use that $|\Psi_{00}\rangle \otimes^n \sim |\Psi_{20}^{(n)}\rangle$ [55]. The EIPs we introduce have the possibility to abort in unfavorable cases, providing higher fidelities or yield.

We consider noisy initial states of the form

$$\rho = \sum_{j=0}^{3} p_j |\phi_j\rangle \langle \phi_j|,$$

with $|\phi_j\rangle \in \{|\Psi_{00}\rangle, |01\rangle, |10\rangle, |\Psi_{10}\rangle\}$. Any state can be depolarized, i.e., transformed by applying randomly local operations, to this standard form keeping the fidelity $F = p_0$. The depolarizing procedure (DEP) is given by channels $D_2 \circ D_1$ the Kraus operators of which are $D_1 : \{1/2 \sigma_i \otimes \sigma_i\}_{i=0}^{3}$ and $D_2 : \{1/\sqrt{2} \mathbb{1} \otimes 1, 1/\sqrt{2} e^{i\pi/4} (1 \otimes e^{i\pi/2})\}$. We call $|01\rangle$, $|10\rangle$ and $|\Psi_{10}\rangle$ the error states. An ensemble $\rho^{\otimes n}$ can be understood as a mixture of (all permutations of) pure states of the form $\bigotimes_{j=0}^{3} |\phi_j\rangle^{\otimes n_j}$ with $\sum n_j = n$, where the corresponding probabilities follow a multinomial distribution. Our task is to figure out which of these configurations is present, i.e., to identify the position of all error states. This knowledge corresponds to a purification that provides at most $n_0$ Bell states. In contrast to hashing [26, 28] we do not require to distinguish between all possible configurations (a) while using a photon-number encoding. This is a relevant class of states, as such noise processes are dominant in many implementations.

At step (ii) from above, we do not learn the total number of errors but the difference $k = n_1 - n_2$. Therefore, if in step (ii) more than a certain number of errors, $k_{\text{max}}$, are found, one can decide to abort the protocol, discarding the whole ensemble. Therefore, the yield is given by

$$Y = \sum_{k=0}^{k_{\text{max}}} p_k (n - k - R_k) / n,$$

where $R_k$ is the number of resources needed to locate all $k$ errors [57].

**Approximate EIP for rank-3 states.**— For states as above, we consider the case $p_3 = 0$, we have two different error states, with an opposite behavior with the counter gate, see Eq. (3). Such situation is given, for instance, by bit-flip noise. Consequently, applying the EPG as in step (ii) from above, we do not learn the total number of errors but the difference $k = n_1 - n_2$. Therefore, we are left with an ensemble consisting of permutations of $\{|\Psi_{00}\rangle^{\otimes n_0}, |01\rangle^{\otimes n_1}, |10\rangle^{\otimes n_2}\}$.

As distinguishing between all possible configurations becomes more involved, and requires increasing amounts of auxiliary entanglement, we relax our requirements and

---

![Fig. 1. (a) Schematic representation of an ensemble of rank-2 states in one of the possible configurations. (b) Diagram illustrating the EIP damp.](image)
allow for errors in the purified ensemble. That is, we consider approximate EIPs that do not aim to output pure Bell states, but only require that the fidelity of the target ensemble exceeds some threshold value. To this aim, we fix some $\lambda \geq 1$ and consider only configurations up to $\lambda$ error states. Configurations with more than $\lambda$ errors will not be detected by our EIP($\lambda$), and hence lower the final fidelity. Notice that the expected number of errors in the ensemble is given by $\lambda_0 = (1-F)n$, and the corresponding binomial probability distribution has almost all of its weight in the interval $\lambda_0 \pm O(\sqrt{n})$, which is the basic property of the typical set at the core of standard hashing and breeding protocols [25, 26, 28]. Therefore, for small $n$ we choose a $\lambda > \lambda_0$ sufficiently large to ensure that the probability for configurations with $k > \lambda$ errors is small enough to neglect them. That is what we do in the following. If $n$ is too large, such that $\lambda_0$ is considerable, there is always the possibility of “blocking” dividing the ensemble into smaller parts that are purified independently.

**EIP(1):** The simplest case is $\lambda = 1$, i.e., we assume there is at most one error in the ensemble. The ENG from step (ii) is applied in the same way as before, but with a $d = 3$-auxiliary register. In this way we distinguish between no error ($k = 0$) and one error of kind $|01 \rangle$ ($k = 1$) or $|10 \rangle$ ($k = 2 = (-1)^{\text{mod}3}$). In case of one error, we apply step (iii) from above to locate it.

**EIP(2):** For $\lambda = 2$, we use a $d = 5$-auxiliary state for ENG in step (ii). If we find $k \neq 0$, there is a unique error configuration of exactly one or two errors of a certain kind, and we proceed as in the case of rank-2 states in step (iii). For $k = 0$, there is ambiguity, as it can stem from either no errors ($n_1 = n_2 = 0$) or one error of each kind, $n_1 = n_2 = 1$. To distinguish between the two cases, we use the EPG with an $d = 2n - 1$ auxiliary. This leads to a result $j' = (r - l) \text{mod}(2n - 1)$, where $r [l]$ is the position of the $|01 \rangle \ [|10 \rangle$] error. $j'$ corresponds to the difference of the positions of the two errors, and $j' = 0$ if there are no errors. As detailed in [57], for each $j'$ one can identify two subensembles with one error in each and proceed with (iii) in each subensemble.

In principle, one can devise protocols for larger $\lambda$, and the blocking strategy always allows one to eventually reduce the problem to the case of $\lambda = 1, 2$. In [57], we also describe aEIP(3), up to three errors, where for one and two errors the error positions are obtained, while for three errors the protocol aborts since identifying error positions is too costly. The approximate EIP($\lambda$) no longer produce states with unit fidelity, but give states with a fidelity that depends on the particular branch of the protocol one ends up with. The higher the $\lambda$, the larger the reachable fidelity, but the yield is reduced. Notice that one cannot restore perfect entangled pairs, and we use a (virtual) asymptotic hashing protocol to provide conversion rates to estimate yields [57].

**EIP for full-rank states.**— To purify full-rank states, a two-step procedure is required, as the counter gate is not sensitive to $|\Psi_{10} \rangle$ errors. In step I we treat error states $|\phi_1 \rangle, |\phi_2 \rangle$ as described above. In step II, we transform the error state $|\phi_3 \rangle$ to an equal mixture of $|\phi_1 \rangle, |\phi_2 \rangle$, while keeping the desired state $|\phi_0 \rangle$ unchanged. This is another DEP, given by $D_2 \circ (H \otimes H)$, where $H$ is the Hadamard gate. At this point the same procedure as before allows one to detect error states originating from $|\phi_3 \rangle$. See [57] for details.

**Results.**— In Fig. 2a we show the yield for EIP$_{\text{damp}}$ (rank-2 states). Fig. 2b and Fig. 2c show the reachable global fidelity and yield for EIP(2) and aEIP(3) (rank-3 states). In Fig. 2d, we compare with finite-size hashing protocols and recurrence protocols [22]. One clearly sees that for moderate system sizes the EIPs perform better than both hashing, breeding, and recurrence protocols.

**Discussion.**— The key element of our EIPs is the readout of locally inaccessible information from a noisy ensemble using auxiliary high-dimensional entanglement [51–54]. We have put forward concrete schemes to treat particular situations with a fixed number of error states. However, in general, the total number of errors cannot be efficiently obtained which, restricts one to distinguish between situations with at most a certain number of errors. This makes EIPs suitable for ensembles with a small expected number of errors $\lambda_0$. This is appreciated in Fig. 2b, where the output fidelity is close to 1 when the expected number of errors justifies to only distinguish between configurations with at most $\lambda$ errors. Instead, the output fidelity drops when $\lambda_0$ is too large.

On the other hand, the methods we discuss here are not restricted to entanglement purification but have other applications, for instance, to certify the fidelity of a noisy ensemble. Rather than doing state tomography, using entanglement witnesses, or other methods discussed in the literature [58], which all destroy parts of the ensemble, one may use a small amount of auxiliary entanglement to achieve this aim. In such general settings, the entanglement cost of performing nonlocal measurements determines the required resources and, ultimately, the efficiency of the schemes. For ensembles of Bell-diagonal states, we show in [57] that deterministically distinguishing between two nonidentical sequences of Bell states requires exactly 1-ebit of entanglement, i.e., an auxiliary Bell state. However, we also find that general dichotomic measurements can require more than 1 ebit [57] (e.g., to distinguish the singlet state from the other three Bell states), and the entanglement cost to distinguish configurations that contain Bell states and product states is unknown.

Another relevant aspect is the influence of noise. We have discussed the EIP assuming perfect auxiliary states, and noiseless operations. In principle, one can always use other EPP to purify part of the ensemble and use the resulting high-fidelity states as auxiliary states for the EIP. However, as we demonstrate in [57], EIPs also work using noisy auxiliary states with only $X$ errors. For initial qubit states that are mixtures of only two Bell pairs, e.g., resulting from bit-flip noise, one can generate the high-dimensional auxiliary states from multiple copies of the noisy initial qubit states. For full-rank states one can use the EPP introduced in [27] to obtain such kind of noisy Bell states from the initial ensemble. Errors accumulated in the auxiliary state due to local operations can be dealt with in this way, as long as the error rate is sufficiently small as it affects the ensemble. However, EIPs are robust
under X errors in the operations, see [57] for details.

Conclusions and outlook. — We have introduced a class of EPPs based on gathering nonlocal information about an ensemble in a controlled and efficient way. We put forward explicit schemes that work particularly well for ensembles of moderate size where errors result from photon loss or amplitude damping noise. Furthermore, one can extend the protocols for arbitrary noisy initial states and purify large ensembles by blocking them. Alternatively, the possibility of extending our EIPs to locate multiple errors is still open. While we did our analysis for ensembles of the form $\rho^n$, the same protocols are applicable for non-IID situations, as they rely on the determination of the number and position of errors in the ensemble as a whole, regardless of the particular distribution of errors. The protocols can thus also be applied to ensembles where errors are not distributed identically nor independently; only the yield and the final fidelity have to be reevaluated. Given the fact that high-fidelity entanglement is at the heart of most applications in quantum technology, the development of efficient and practical entanglement purification schemes is of crucial importance for their practical realization. For practical reasons, such purification schemes have to be efficient for moderately sized ensembles, at least in the near term. We believe, however, that the techniques and ideas put forward here are not limited to EPP, but have much broader applications. From a practical point of view, establishing methods to perform fidelity estimation or state certification in an entanglement-assisted way is highly relevant, and the counter gate we introduce is a powerful tool in this context. From a more fundamental perspective, the question of entanglement cost of different nonlocal entangling measurements that we put forward and answer partially seems to be worth pursuing further.

This work was supported by the Austrian Science Fund (FWF) through Project No. P30937-N27 and the Swiss National Science Foundation (SNSF) and the NCCR Quantum Science and Technology, through Grant No. PP00P2-179109 in particular.

We thank Julius Wallnöfer for interesting discussions.

---

Fig. 2. Yield (a), (c) and global fidelity (b) of different EPP (EIP, dashed lines; aEIP, solid lines) for rank-2 input states (a) and rank-3 input states (b), (c) for different initial fidelities as a function of number of initial copies. (d) Comparison of EIP and aEIP (asterisk indicates abort whenever error is detected) to recurrence DEJMPS and hashing protocols (upper bound, see [57]) in a global fidelity vs yield plot for rank-3 ensembles with $n = 16$ copies (EIP, dashed lines; aEIP, circles; rank-2 ensembles, which are equivalent for hashing and DEJMPS protocols).
[11] S. Bravyi and A. Kitaev, Phys. Rev. A 71, 022316 (2005).
[12] E. Knill, Nature (London) 434, 39 (2005).
[13] H. J. Kimble, Nature (London) 453, 1023 (2008).
[14] S. Wehner, D. Elkouss, and R. Hanson, Science 362 (2018).
[15] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. 81, 5932 (1998).
[16] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A 59, 169 (1999).
[17] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. 8, 184 (2006).
[18] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. 83, 33 (2011).
[19] Y.-B. Sheng, L. Zhou, and G.-L. Long, Phys. Rev. A 88, 022302 (2013).
[20] K. Azuma, K. Tamaki, and H.-K. Lo, Nat. Commun. 6, 6787 (2015).
[21] M. Zwerger, H. Briegel, and W. Dür, Appl. Phys. B 122, 50 (2016).
[22] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, Phys. Rev. Lett. 120, 030503 (2018).
[23] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. 8, 15043 (2017).
[24] S. Pirandola, Commun. Phys. 2, 1 (2019).
[25] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[26] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).
[27] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. 77, 2818 (1996).
[28] W. Dür and H. J. Briegel, Rep. Prog. Phys. 70, 1381 (2007).
[29] T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A 64, 012304 (2001).
[30] E. M. Rains, IEEE Trans. Inf. Theory 47, 2921 (2001).
[31] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A 67, 022310 (2003).
[32] K. G. H. Vollbrecht and F. Verstraete, Phys. Rev. A 71, 062325 (2005).
[33] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A 72, 032313 (2005).
[34] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. 97, 180501 (2006).
[35] K. Fuji and K. Yamamoto, Phys. Rev. A 80, 042308 (2009).
[36] F. Buscemi and N. Datta, J. Math. Phys. (N.Y.) 51, 102201 (2010).
[37] F. G. Brandao and N. Datta, IEEE Trans. Inf. Theory 57, 1754 (2011).
[38] M. Zwerger, H. J. Briegel, and W. Dür, Phys. Rev. Lett. 110, 260503 (2013).
[39] S. Bratzik, S. Abuzzo, H. Kampermann, and D. Bruß, Phys. Rev. A 87, 062335 (2013).
[40] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, Phys. Rev. X 4, 041041 (2014).
[41] L. Ruan, W. Dai, and M. Z. Win, Phys. Rev. A 97, 052332 (2018).
[42] F. Rozpędźek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, Phys. Rev. A 97, 062333 (2018).
[43] J. Wallnöfer, A. Pirker, M. Zwerger, and W. Dür, Sci. Rep 9, 314 (2019).
[44] S. Krastanov, V. V. Albert, and L. Jiang, Quantum 3, 123 (2019).
[45] K. Fang, X. Wang, M. Tomamichel, and R. Duan, IEEE Trans. Inf. Theory 65, 6454 (2019).
[46] S. de Bone, R. Ouyang, K. Goodenough, and D. Elkouss, IEEE Trans. Quantum Eng. 1, 1 (2020).
[47] K. Fang and Z.-W. Liu, Phys. Rev. Lett. 125, 060405 (2020).
[48] K. Fang and Z.-W. Liu, arXiv: 2010.11822 .
[49] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Phys. Rev. Lett. 126, 010503 (2021).
[50] L. Zhou, W. Zhong, and Y.-B. Sheng, Opt. Express 28, 2291 (2020).
[51] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, Adv. Quantum Technol. 2, 1900038 (2019).
[52] M. Erhard, M. Krenn, and A. Zeilinger, Nat. Rev. Phys. 2, 365 (2020).
[53] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Front. Phys. 8, 479 (2020).
[54] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Phys. Rev. X 9, 041042 (2019).
[55] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).
[56] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, 2010).
[57] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, Phys. Rev. A 104, 012419 (2021).
[58] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. 2, 382 (2020).