Renormalising entanglement distillation

S. Wäldchen,[1] J. Gertis,[1] E. T. Campbell,[1,2] and J. Eisert[1]

[1]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, DE*
[2]*Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, UK*

(Dated: October 24, 2014)

It has long been noted in the field of quantum information science that entanglement constitutes the key resource in various information processing and specifically communication tasks [1]. Secure quantum key distribution necessarily relies on entanglement, even in a sense in prepare and measure schemes [2–4]. One of the main efforts in quantum information science has therefore been directed towards getting an understanding of manipulating entanglement and of finding ways to transform less usable forms of entanglement into more suitable ones. The task of entanglement distillation specifically captures the resource character of entanglement, in that it aims at preparing maximally entangled states from noisy or less entangled ones [1]. Distillation steps are part of *quantum repeater protocols* [5–7], necessary to distribute entanglement over arbitrary distances over noisy quantum channels: In such a scheme, entanglement is being established between different repeater stations and transferred to the final designated nodes via suitable entanglement swapping steps. Distillation schemes thought of in this context are often iterative schemes, such as the recurrence protocol[1, 8] and deterministic protocols based on error-correction codes. While they are usually not achieving the maximum rates set by the distillable entanglement, they are more practically feasible.

The silent assumption in almost exclusively all of the proposed distillation schemes, however, is that the initial resources have been identically prepared and they show no correlations whatsoever. Depending on the type of preparation, this may or may not be a reasonable assumption at all. Whenever memory effects or channels [9–11] are involved, one expects some correlations between the involved entangled pairs, going beyond an i.i.d. setting. These correlations are expected to decay rapidly over several pairs sent through a channel – reflecting the natural correlation structure arising from a *memory channel* (see Fig. 1). Steps have been taken concerning the mathematical definition of distillable entanglement in the presence of correlations [12, 13]. The important practical problem of how to distill entanglement from correlated pairs arising from quantum memory channels is still wide open.

In this work, we propose a conceptually novel way forward to solve this problem, bringing together ideas from entanglement theory with those of condensed matter theory, specifically of renormalisation and tensor network states. We start by identifying the natural class of states arising from preparations and memory channels as bi-partite *matrix-product operators*. Such classes of states are usually considered in the condensed matter context to capture thermal many-body states or those arising from open systems dynamics. Here, we encounter natural bi-partite – and still multi-partite – instances thereof. Entanglement distillation is then identified as a *renormalisation of bi-partite matrix-product operators*. Viewed in this mindset, the methods are inspired and derive from renormalisation [14] of *matrix-product states* [15–20], again from many-body theory. Specifically, what we show is that both the recurrence protocol and the error correction protocol converge to pairs of maximally entangled pure states for subsequently correlated pairs naturally described by an MPO. This leads to entanglement distillation very similar to the i.i.d. case and numerical evidence suggests that allowing for unwanted correlations between subsequent pairs can in some cases even speed up the convergence to maximally entangled pairs compared to the uncorrelated i.i.d. case.

Setting and formalism. We consider a sequence of L pairs of qubits, where two parties (say Alice and Bob) each hold one qubit from each pair. These pairs are entangled, as well as correlated with each other, as a consequence of the preparation procedure involving stationary quantum memory effects. We work in a numerically indexed Bell basis $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle\}$, which are more commonly labelled as $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. We consider a sequence of L pairs of qubits, with the basis vectors $|\Phi_{\mathbf{x}}\rangle = |\phi_{x_1}\rangle |\phi_{x_2}\rangle \dots |\phi_{x_L}\rangle$, where Alice holds the first qubit of each pair and Bob holds its partner. Translationally invariant mixtures of these states reflecting stationarity of the source are described in the MPO language as $\langle\Phi_{\mathbf{x}}| \rho |\Phi_{\mathbf{y}}\rangle = \mathrm{Tr}\left[M^{x_1,y_1} M^{x_2,y_2} \dots M^{x_L,y_L}\right]$.

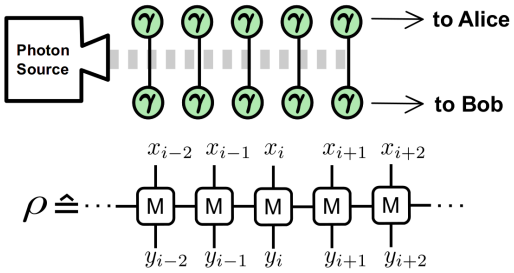


FIG. 1. Photon source with memory emitting weakly correlated photon pairs and the MPO ρ naturally describing this setting.

The dimension of the matrices $M^{x,y}$ limits the correlations between pairs, and by increasing this so-called bond dimension arbitrary quantum states can be described in this formalism. There is a gauge freedom in our choice of MPO matrices as for any invertible X mapping $M^{x,y} \mapsto XM^{x,y}X^{-1}$ will give an alternative description of the same physical state. Generally, 16 matrices are needed for the description of each pair, since a two-particle density matrix has 16 entries. However, we assume Bell diagonality. If the state was not Bell diagonal in the beginning it could be made so by a suitable group twirling. Since the errors and our protocols only apply Clifford operations, the twirling can be commuted with it and be done at the end. For this reason we herein use the shorthand $A = M^{1,1}$, $B = M^{2,2}$, $C = M^{3,3}$ and $D = M^{4,4}$. Without loss of generality, we consider the distillation of maximally entangled ϕ^+ pairs. The "A" matrix will be the dominant matrix and the rest we call noise matrices.

Protocols and renormalisation. An $N \to M$ iterative protocol for entanglement distillation of i.i.d. states will act on N pairs and output M (where $M < N$) pairs. Given more than N i.i.d. pairs the protocol is performed in parallel on blocks of N pairs. In the MPO setting pairs are not i.d.d. and so we must specify which pairs are involved in each block of a protocol. We choose neighbouring pairs so the first N pairs are distilled into M pairs, while simultaneously the next N pairs are distilled, and so on. This choice has the practical merit of respecting chain locality, but also has the advanatage that the output state is easily shown to again be an MPO of the same bond dimension. Every iteration of the distillation protocol now acts as a map from an old MPO to a new one, and reducing the chain length from L to LN/M and so is naturally seen as process of MPO renormalisation. After the n-th step, we label the MPO operators $\{A_n, B_n, C_n, D_n\}$, where the initial raw state provides the $n = 0$ matrices. We prove several results on convergence to entangled states that can also be interpreted as convergence proofs for renormalisation flow of the MPOs. Specifically we consider the recurrence protocol and a distillation through error correction using the 5-qubit code. Both protocols solely use local operations and classical communication with respect to the partition between Alice and Bob.

Recurrence protocol. The recurrence protocol is a $2 \to 1$, which uses post-selection. At every round produces measurement outcomes and we only proceed if certain outcomes are obtained. Here we use a slightly improved version of recurrence [8], and the iteration formula between two rounds is

$$A_{n+1} = A_n^2 + B_n^2, \quad B_{n+1} = C_n^2 + D_n^2, \quad C_{n+1} = A_nB_n + B_nA_n, \quad D_{n+1} = C_nD_n + D_nC_n.$$

Replacing matrices by commuative scalar recovers the orginal i.i.d. result. Proving convergence of the initial MPO in the state ρ to the maximally entangled state ϕ^+ is achieved by showing that the noise matrices vanish exponentially faster than the A_n matrices. Specifically, an appropriate ratio of norms will be exponentially suppressed. We define a norm $\|M\|$ in terms of a channel $\mathcal{M}$ Choi-isomorphic to M, so that $\|M\| = \|\mathcal{M}\|_{1\to1}$ where we use the induced "'1-to-1'" Schatten norm. We introduce the noise contribution of the coefficient matrices B, C and D as $\epsilon_n = \max\left(\|\mathcal{B}_n\|_{1\to1}, \|\mathcal{C}_n\|_{1\to1}, \|\mathcal{D}_n\|_{1\to1}\right)$ defined in a common gauge where $\mathcal{A}_n$ is trace preserving. Throughout sub-multiplicativity, we expect that small noise matrices shrink in size. However, ensuring A_{n+1} stays large is the main technical challenge. Proving this relies on the ergodicity of the matrices, which is measured by the ergodicity coefficient $\tau(\mathcal{M}) = \max_{\mathrm{Tr}[\sigma]=0} \frac{\|\mathcal{M}(\sigma)\|_1}{\|\sigma\|_1}$. Given these concepts we show the following sufficient conditions for entanglement distillation.

Theorem 1 (Convergence in the recurrence protocol)**.** *Given a translationally invariant bell diagonal MPO ρ_0 with coefficients A_0, B_0, C_0, and D_0, the iterative application of the recurrence protocol leads to convergence of ρ_n to uncorrelated pairs in the pure and maximally entangled state ϕ_+ for $\tau_n := \tau(\mathcal{A}_n) \leq \tau_0$ and $\epsilon_0 \leq \min(0.152, \frac{5}{22}\frac{1-\tau_0^4}{1+\tau_0^4})$.*

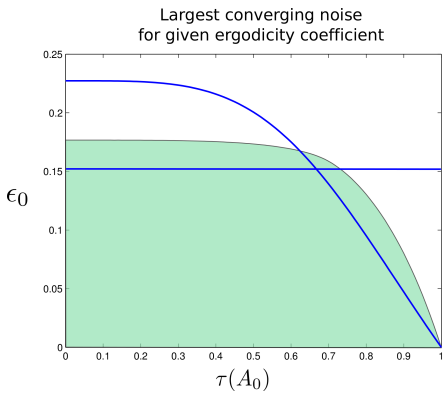


FIG. 2. Parameter region for the recurrence protocol. The intersection of the area under both the blue lines reflects the bounds given in Theorem 1. The green region is a slightly improved bound that will be derived in the paper.

The conditions for convergence are illustrated in Fig. 2. The proof is technical and will be presented in full length in the full paper (in preparation). To show convergence, we want to make sure B_n, C_n, and D_n are reduced exponentially compared to A_n. In every iteration of the protocol, in addition to raising the matrix A_n to a power, perturbative terms are added. Since it is unclear how to bound the norm of a power of a general matrix, we rely on the ergodicity of the matrix. We use our gauge freedom, to make $\mathcal{A}_{n+1}$ trace preserving in every step of the protocol. This takes the form of a perturbed Markov chain. There are two major insights we use: First, a slight perturbation does not change the trace preserving property too much. We express it in a perturbation of the left Perron vector. Second, the condition number of the perturbation depends on the ergodicity coefficient of the channel before the perturbation and it gets closer to 1 the closer the channel is to a projector. By constraining both the ergodicity coefficient τ_0 of the initial dominant matrix A_0 and the initial noise contribution ϵ_0, we find a parameter space for which convergence is proven. Finally, we show that convergence in MPO norm entails convergence in fidelity to a chain of maximally entangled $|\phi^+\rangle$ pairs.

5-qubit protocol. For every error correcting code that encodes k qubits into N physical qubits, there exists an iterative $N \to k$ one-way entanglement distillation protocol [1]. In these protocols, noise information is extracted by local measurements, but instead of post-selecting when errors are detected we attempt to correct by determining the smallest weight error consistent with the measurement data. The advantage over the recurrence protocol is that this protocol is deterministic, and that one-way distillation schemes require less classical communication. In particular, we consider using the 5-qubit code (so a $5 \to 1$ protocol), which is a the smallest code capable of correcting any single qubit error. We again find a closed form for the map on the coefficient matrices between the iterations, though we omit it here as each expression contains 4^4 terms. We further introduce the transition matrix $E_n = A_n + B_n + C_n + D_n$ and its corresponding map $\mathcal{E}_n$, and state the following theorem.

Theorem 2 (Error correction)**.** *Given a translationally invariant bell diagonal MPO ρ_0 with coefficients A_0, B_0, C_0, and D_0, the iterative application of the 5-qubit error correcting code leads to convergence of ρ_n to uncorrelated pairs in the pure and maximally entangled state ϕ_+ for $\epsilon_0 \leq \frac{1}{33}$. ϵ_0 is defined as above in the gauge where $\mathcal{E}_0$ is trace preserving.*

Again, the full proof will be appear in the forthcoming paper. Similar to the post-selective case, we show that the contribution of the noise matrices B_n, C_n, D_n to the state ρ_n are suppressed exponentially compared to the contribution of the dominant matrix A_n. Since we do not post-select, we do not need to renormalise ρ_n in every round. The transition matrix is always mapped as $E_{n+1} = E_n^5$. If we initially choose a gauge where the corresponding map $\mathcal{E}_0$ is trace preserving, the transition matrix will keep this property over the course of the iteration. Using combinatorical arguments, we then prove that for suitable small ϵ_0, ϵ_n converges to zero, and again entailing convergence in fidelity of the physical state.

Conclusion. The recurrence protocol and the 5-qubit error correction protocol are proven to work for i.i.d. pairs with a certain threshold fidelity. We extended these proofs to find similar criterions to ensure convergence of correlated pairs described by an MPO to a number of independent maximally entangled pure states. It is reasonable to assume that if the MPO is only weakly correlated between the pairs and the reduced density matrix of a single pair is sufficiently close to a bell pair, the distillation protocols should behave similarily to the i.i.d. case. Indeed, convergence can be proven for threshold fidelities and conditions on the correlation between the pairs.

Acknowledgements. We acknowledge funding from the BMBF (QuOReP), the EU (RAQUEL, SIQS, COST, AQuS), and the ERC (TAQ).

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] N. Gisin and R. Thew, Nature Phot. **1**, 165 (2007).
[4] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[5] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).
[7] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).
[8] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[9] A. Ahlbrecht, F. Richter, and R. F. Werner, Int. J. Quant. Inf. **10**, 1250057 (2012).
[10] M. B. Plenio and S. Virmani, Phys. Rev. Lett. **99**, 120504 (2007).
[11] D. Kretschmann and R. F. Werner, Phys. Rev. A **72**, 062323 (2005).
[12] F. G. S. L. Brandao and J. Eisert, J. Math. Phys. **49**, 042102 (2008).
[13] F. Buscemi and N. Datta, J. Math. Phys. **51**, 102201 (2010).
[14] F. Verstraete, J. I. Cirac, J. I. Latorre, E. Rico, and M. Wolf, Phys. Rev. Lett. **94**, 140601 (2005).
[15] M. Fannes, B. Nachtergaele, and R. F. Werner, Commun. Math. Phys. **144**, 443 (1992).
[16] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, Quant. Inf. Comp. **5**&**6**, 401 (2006).
[17] U. Schollwöck, Ann. Phys. **326**, 96 (2011).
[18] J. Eisert, Modeling and Simulation **3**, 520 (2013).
[19] R. Orus, Ann. Phys. **349**, 117 (2014).
[20] N. Schuch, ArXiv:1306.5551.