

Evaluating convex roof entanglement measures

Géza Tóth,^{1,2,3,*} Tobias Moroder,⁴ and Otfried Gühne⁴

¹*Department of Theoretical Physics, University of the Basque Country UPV/EHU, P.O. Box 644, E-48080 Bilbao, Spain*

²*IKERBASQUE, Basque Foundation for Science, E-48011 Bilbao, Spain*

³*Wigner Research Centre for Physics, Hungarian Academy of Sciences, P.O. Box 49, H-1525 Budapest, Hungary*

⁴*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Str. 3, 57068 Siegen, Germany*

(Dated: October 21, 2014)

We show a powerful method to compute entanglement measures based on convex roof constructions. In particular, our method is applicable to measures that, for pure states, can be written as low order polynomials of operator expectation values. We show how to compute the linear entropy of entanglement, the linear entanglement of assistance, and a bound on the dimension of the entanglement for bipartite systems. We discuss how to obtain the convex roof of the three-tangle for three-qubit states. We also show how to calculate the linear entropy of entanglement and the quantum Fisher information based on partial information or device independent information. We demonstrate the usefulness of our method by concrete examples.

PACS numbers: 03.67.Mn, 03.65.Ud, 42.50.St

Quantum entanglement plays a central role in quantum information science and quantum optics [1]. There are now efficient methods to detect entanglement, that have even been used in many experiments [2]. These mostly answer the yes or no question: "Is the quantum state entangled?" or "Is the quantum state genuine multipartite entangled?" After verifying the presence of entanglement, the next step is quantifying it. Calculating measures is becoming increasingly important in experiments in quantum information science [3–5] and it also plays a crucial role in investigations in quantum statistical physics, e.g., in studying phase transitions [6].

Most entanglement measures are based on the convex roof of a quantity on pure states such as the entropy of the reduced state [7–9]. Measures of this type can also be used to classify states according to their membership in some convex sets, for example, based on their Schmidt rank [10, 11]. They play a central role in quantum information theory, however, in most of the cases they are not computable as there are no efficient ways to calculate convex roofs. Most importantly, the simplest multipartite entanglement measure, the three-tangle for three-qubits, cannot be computed for a general state.

Thus, for obtaining entanglement measures in theory and experiments, it would be crucial to find methods to calculate convex roof constructions efficiently, at least for not too large systems. This seems to be a very difficult task since straightforward numerical search means an optimization over an infinite number of convex decompositions of the density matrix. Such an approach will lead to an *upper* bound on the measure, since a multi-variable numerical optimization is not guaranteed to find the global optimum [12]. Upper bounds, however, are often not very useful as the amount of entanglement can be much lower or even zero even if the procedure signals considerable entanglement.

In this paper, we present a method that produces a

series of very good *lower* bounds on important entanglement measures. Our method has the following characteristics: (i) It is based on semidefinite programming. The series of bounds obtained converge in a controllable way to the true value. Even the first lower bound in the series is non-trivial. (ii) We have a clear physical picture for what states our method yields a nonzero value for the measures. (iii) The set of separable states is used in the optimization procedure. This way we connect calculating convex roofs to the separability problem, which might help to find applications of the separability problem in other areas of physics. We will demonstrate the use of our method with the example of computing bipartite entanglement measures for bound entangled states, computing the convex roof of the tangle for various three-qubit states, and even quantities outside of quantum information science. Our method can also be used to compute a lower bound from incomplete data of the quantum state or in device independent scenarios [13–16].

Convex roof of linear entropy. For pure states, the linear entropy of entanglement is given as

$$E_{\text{lin}}(|\Psi\rangle) = S_{\text{lin}}[\text{Tr}_1(|\Psi\rangle)], \quad (1)$$

where we used the definition of the linear entropy $S_{\text{lin}}(\varrho) = 1 - \text{Tr}(\varrho^2)$. Hence, the linear entropy of entanglement for pure states equals also $C^2/2$, where C is the concurrence [7], and it is also equal to the I -tangle [17]. The definition (1) can be extended to mixed states by a convex roof construction as

$$E_{\text{lin}}(\varrho) = \min_{\{p_k, |\Psi_k\rangle\}} \left(\sum_k p_k E_{\text{lin}}(|\Psi_k\rangle) \right), \quad (2)$$

where $\{p_k, |\Psi_k\rangle\}$ is a decomposition to pure states

$$\varrho = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|. \quad (3)$$

It can be shown that $E_{\text{lin}}(\varrho)$ does not increase under local operations and classical communication (LOCC) on average, hence it is an entanglement monotone [18]. Consequently, $E_{\text{lin}}(\varrho)$ has also been used to characterize entanglement even in the multipartite setting [19].

Next, we will show a method to compute Eq. (2). For this aim, first we write the linear entropy of entanglement as an expectation value of an operator acting on two copies of a bipartite pure state $|\Psi\rangle$ as [20]

$$E_{\text{lin}}(|\Psi\rangle) = \text{Tr}[\mathcal{A}_{AA'} \otimes \mathbb{1}_{BB'} (|\Psi\rangle\langle\Psi|)_{AB} \otimes (|\Psi\rangle\langle\Psi|)_{A'B'}]. \quad (4)$$

Here, A and B denote the parties of the first copy while A' and B' denote the parties of the second copy. Moreover, the projector to the antisymmetric space is defined as $\mathcal{A}_{AA'} := (\mathbb{1} - \mathcal{F})_{AA'}$, \mathcal{F} is the flip operator, and we explicitly wrote out $\mathbb{1}_{BB'}$ for clarity [21].

Next, we will consider mixed states. Let us assume that $\{\tilde{p}_k, |\tilde{\Psi}_k\rangle\}$ is the decomposition attaining the convex roof. Then, for a state with such a decomposition we obtain

$$\begin{aligned} E_{\text{lin}}(\varrho) &= \sum_k \tilde{p}_k E_{\text{lin}}(|\tilde{\Psi}_k\rangle) \\ &= \sum_k \tilde{p}_k \text{Tr}(\mathcal{A}_{AA'} |\tilde{\Psi}_k\rangle\langle\tilde{\Psi}_k|^{\otimes 2}) \\ &= \text{Tr}(\mathcal{A}_{AA'} \omega_{12}), \end{aligned} \quad (5)$$

where the state on the two-copy space is defined as

$$\omega_{12} = \sum_k \tilde{p}_k |\tilde{\Psi}_k\rangle\langle\tilde{\Psi}_k| \otimes |\tilde{\Psi}_k\rangle\langle\tilde{\Psi}_k|. \quad (6)$$

The density matrix ω_{12} has three important properties. It is a mixture of product states, i.e., a separable state [22]. Moreover, all the pure product components are symmetric. Thus, ω_{12} is supported on the symmetric subspace. In fact, any symmetric separable states can be written in the form (6) [23]. Finally, $\text{Tr}_2(\omega_{12}) = \varrho$.

Hence, we arrive at our first main result.

Observation 1.—The convex roof of the linear entropy can be written as

$$\begin{aligned} E_{\text{lin}}(\varrho) &= \min_{\omega_{12}} \text{Tr}(\mathcal{A}_{AA'} \omega_{12}), \\ \text{s.t.} \quad &\omega_{12} \text{ symmetric, separable,} \\ &\omega_1 = \varrho, \end{aligned} \quad (7)$$

where $\omega_1 \equiv \text{Tr}_2(\omega_{12})$.

Observation 1 connects the separability problem of symmetric bipartite states, i.e., answering the question "Is the state entangled?" mentioned in the introduction, to entanglement quantification. In principle, to obtain a lower bound on $E_{\text{lin}}(\varrho)$, any necessary condition for separability could be used. We will consider the method based on the positivity of partial transpose (PPT) [24]

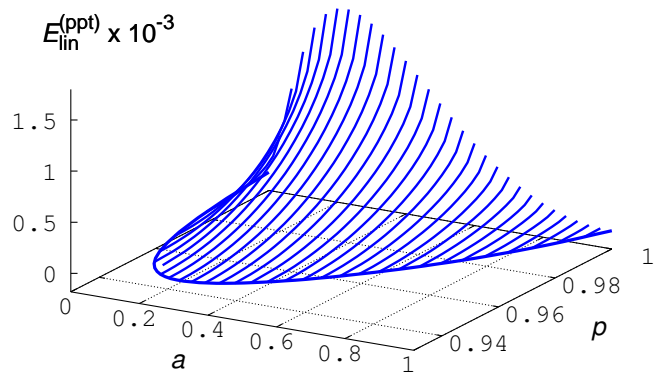


FIG. 1: (Color online) Entanglement quantification for the noisy 3×3 Horodecki bound entangled state $\varrho_a(p)$ using $E_{\text{lin}}^{(\text{ppt})}(\varrho)$ defined after Observation 1. We plot $E_{\text{lin}}^{(\text{ppt})}(\varrho)$ as a function of the parameter of the state, a , and the weight-parameter p .

and obtain a lower bound as

$$\begin{aligned} E_{\text{lin}}^{(\text{ppt})}(\varrho) &= \min_{\omega_{12}} \text{Tr}(\mathcal{A}_{AA'} \omega_{12}), \\ \text{s.t.} \quad &\omega_{12} \text{ symmetric, PPT,} \\ &\omega_1 = \varrho, \end{aligned} \quad (8)$$

Next, we will demonstrate that our method can be used to quantify the entanglement of states not detected by the PPT condition, called bound entangled states [25–27].

Horodecki state.—We test our method to calculate entanglement measures for the one-parameter family of the 3×3 bound entangled state ϱ_a^{PH} introduced by P. Horodecki [26]. We mix the state with white noise according to $\varrho_a(p) = p\varrho_a^{\text{PH}} + (1-p)\mathbb{1}/9$ and calculate the entanglement as a function of a and p . The results can be seen in Fig. 1. The critical noise for which $E_{\text{lin}}^{(\text{ppt})}(\varrho) = 0$ agrees with the calculations of Ref. [21] and Ref. [28]. We note that we made the computer program calculating $E_{\text{lin}}^{(\text{ppt})}(\varrho)$, with all other programs used for this publication, publicly available [29]. Other methods for calculating entanglement measures are in Refs. [30, 31].

It is a surprise that, while the bound relies on the PPT criterion, the method is still able to detect PPT entangled states. In order to obtain more information on what kind of states are detected, we need to know the separability criterion based on symmetric extensions [32]. A given bipartite state ϱ_{AB} is said to have a $n : m$ symmetric extension if it can be written as the reduced state of a multipartite state $\varrho_{A_1 \dots A_n B_1 \dots B_m}$, which is symmetric under $A_k \leftrightarrow A_l$ and $B_k \leftrightarrow B_l$ for all $k \neq l$. If we also require that the state is PPT for all bipartitions, then it is a PPT symmetric extension. Separable states have such extensions for arbitrarily large n and m , while the lack of such an extension signals the presence of entanglement.

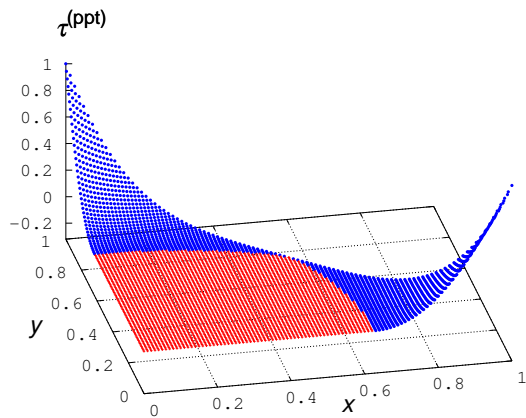


FIG. 2: (Color online) Three-tangle of a family of states (12) as a function of the parameters x and y . Light color indicates the region where the tangle is zero, darker color indicates a nonzero value.

Observation 2.—For all non-PPT states and for all states that do not have a $2 : 2$ symmetric extension we have $E_{\text{lin}}^{(\text{ppt})}(\varrho) > 0$. Moreover, for all states having a $2 : 2$ PPT symmetric extension $E_{\text{lin}}^{(\text{ppt})}(\varrho) = 0$ holds. The proof can be found in the Supplement [33].

Before we continue let us point out that we can also obtain a lower bound on $E_{\text{lin}}(\varrho)$ if we choose any other entanglement condition, such as the method based on local uncertainty relations [46], the covariance matrix criterion [47], or the computable cross norm or realignment criterion (CCNR) [48]. However, for symmetric states these are all equivalent to the PPT condition [49].

Therefore, to strengthen the bound a stronger criterion must be employed. Here again the method of PPT symmetric extensions can be used [32]. Rather than approximating ω_{12} by PPT states, we demand that ω_{12} has an $n : 1$ PPT symmetric extension [50]. In this way we obtain a sequence of lower bounds $E_{\text{lin}}^{(n)}$ with increasing accuracies. The corresponding optimization can similarly be carried out by semidefinite programming. Note that the PPT symmetric extensions converge to the set of separable states in a controlled way [51]. Finally, note also that semidefinite programs not only detect entanglement, but through solving the dual problem, it is possible to find entanglement witnesses [32]. In our case, these witnesses can even bound entanglement measures, as explained in the Supplement [33].

Generalization and further examples.—The previous ideas can straightforwardly be generalized to compute the convex roof of any quantity that can be written as a polynomial of expectation values for pure states as

$$E(|\Psi\rangle) = \sum_{m=1}^M \sum_{n=0}^N c_{mn} \langle A_m \rangle^n, \quad (9)$$

where A_m are operators and c_{mn} are constants (see e.g.,

[52, 53]). It is possible to define an operator $L := \sum_{m,n} c_{mn} A_m^{\otimes n} \otimes \mathbb{1}^{\otimes (N-n)}$, whose expectation value on several copies reproduces Eq. (9). Then, the convex roof of Eq. (9) can be obtained as an optimization over N -copy symmetric fully separable states [23]

$$\begin{aligned} E(\varrho) = \min_{\omega_{12..N}} & \quad \text{Tr}(L\omega_{12..N}), \\ \text{s.t.} & \quad \omega_{12..N} \text{ symmetric, fully separable,} \\ & \quad \omega_1 = \varrho. \end{aligned} \quad (10)$$

Three-tangle.—Our next example is the calculation of the three-tangle, a three-qubit entanglement monotone [54]. For pure states, it has been defined by Coffmann, Kundu and Wootters [9]. Remarkably, it can be written as a fourth-order polynomial in expectation values [52]. Hence, for mixed states, the tangle can be defined through a convex roof extension, which we can now map to the optimization problem

$$\begin{aligned} \tau(\varrho) = \min_{\omega_{12}} & \quad \text{Tr}(T\omega_{1234}), \\ \text{s.t.} & \quad \omega_{1234} \text{ symmetric, fully separable,} \\ & \quad \omega_1 = \varrho, \end{aligned} \quad (11)$$

where T is an operator acting on four copies of the three-qubit state [55]. Note that if we know $\tau(\varrho)$, we can decide whether a three-qubit fully entangled state is in the W or in the GHZ class [10].

The optimization can be carried out for symmetric multiqubit states that are PPT with respect to all bipartitions rather than symmetric separable states, leading to the lower bound $\tau^{(\text{ppt})}$. The results are shown in Fig. 2 for states of the form

$$\begin{aligned} \varrho(x, y) = & \quad x|\text{GHZ}^+\rangle\langle\text{GHZ}^+| + y|\text{GHZ}^-\rangle\langle\text{GHZ}^-| \\ & \quad + (1-x-y)|W\rangle\langle W|, \end{aligned} \quad (12)$$

where $|\text{GHZ}^\pm\rangle = (|000\rangle \pm |111\rangle)/\sqrt{2}$, and $|W\rangle = (|100\rangle + |010\rangle + |001\rangle)/\sqrt{3}$. Note that a lower bound for the convex roof of the tangle for general states, which is exact for states with certain symmetries, has been developed [56].

As a practical comment, we add that the numerical computation is challenging, but $\tau^{(\text{ppt})}$ can be computed on a standard laptop with standard free packages for semidefinite programming [57], if the state has some symmetries, or has a rank up to six. Calculations for general three-qubit states of rank eight are realistic with computer clusters and professional packages.

Schmidt rank.—Let us consider the quantities R_r that are nonzero for states with a Schmidt rank larger than r . For example, $R_2(|\Psi\rangle) = \sum_{i<j} \lambda_i \lambda_j \equiv 4S_{\text{lin}}(|\Psi\rangle)$, $R_3(|\Psi\rangle) = \sum_{i<j<k} \lambda_i \lambda_j \lambda_k$, where λ_k are the eigenvalues of the reduced state. The R_k quantities are proven to be entanglement monotones [58]. We can calculate the convex roof of R_r with our method. Convex roofs for such quantities allow us to bound the dimensionality of the entanglement from below. A powerful bound

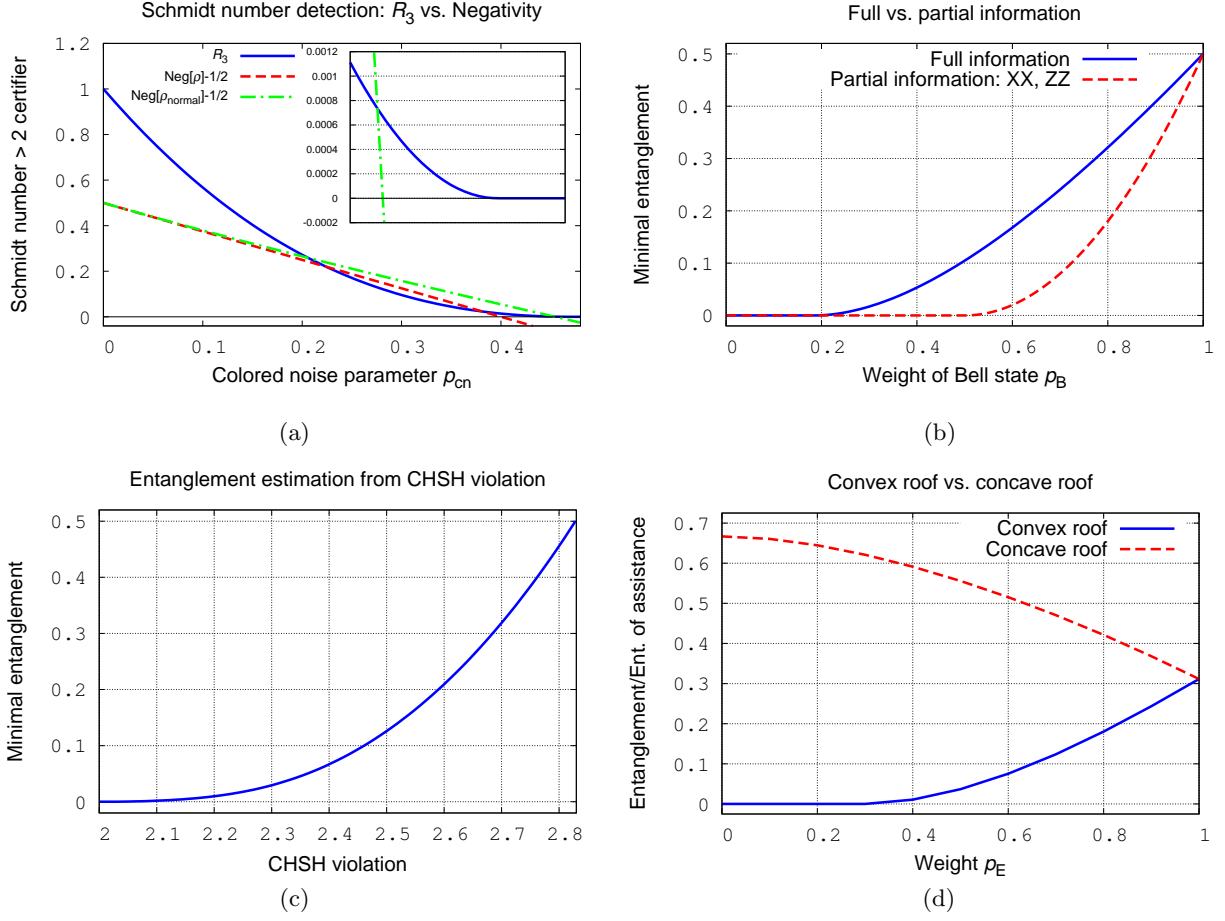


FIG. 3: (Color online) (a) Schmidt-number witness vs. negativity for a state of the type (13) as a function of p_{cn} . As the inset shows, even when we consider negativity of the normal form, obtained through stochastic local operations and classical communications (SLOCC) such that all local matrices are fully mixed [59], our numerical method is superior. (b) $E_{lin}^{(ppt)}(\varrho)$, given in Eq. (8), based on partial information for the state (14). (c) Estimation of $E_{lin}^{(ppt)}(\varrho)$ as a function of the violation of the CHSH inequality. (d) $E_{lin}^{(ppt)}(\varrho)$ and the corresponding bound for the entanglement of assistance (defined with the linear entropy) for a state of the type (15) as a function of p .

can be obtained by carrying out the optimisation for r -qudit symmetric states that are PPT with respect to all bipartitions. An alternative is computing the negativity [60, 61]. In particular, $\mathcal{N}(\varrho) - 1/2 > 0$ signals that the Schmidt number is larger than 2. We show that our method outperforms the negativity as a dimension witness in Fig. 3(a) for the family of states

$$\varrho_S(p_{cn}) = (1 - p_{cn})|\Psi_S\rangle\langle\Psi_S| + p_{cn}\varrho_{cn}, \quad (13)$$

with $|\Psi_S\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ and colored noise $\varrho_{cn} = \mathbb{1}_2 \otimes \mathbb{1}_2/4$ with $\mathbb{1}_2 = (|0\rangle\langle 0| + |1\rangle\langle 1|)$.

We add that we checked several random 3×3 edge states to test the conjecture of Sanpera, Bruß and Lewenstein claiming that all bound entangled states in such systems have a Schmidt rank 2, and did not find a counterexample [11].

Evaluation of entanglement measures based on incomplete information.—Experimentally it is very important

that entanglement measures can be evaluated based on incomplete knowledge on the quantum state. There are efficient methods to bound entanglement measures based on an operator expectation value from below [3–5]. The current method can be adapted straightforwardly to the partial information case by replacing the condition $\omega_1 = \varrho$ with the set of linear constraints $\text{Tr}(\omega_1 O_i) = v_i$, where O_i are the measured observables and v_i are the corresponding expectation values. As an example, see Fig. 3(b), where the entanglement is bounded from below based on complete information and based on $\langle\sigma_x \otimes \sigma_x\rangle$ and $\langle\sigma_z \otimes \sigma_z\rangle$ measurements for the state

$$\varrho_B(p) = p_B|\Phi_{3 \times 3}^+\rangle\langle\Phi_{3 \times 3}^+| + (1 - p_B)\frac{1}{9}\mathbb{1}, \quad (14)$$

where $|\Phi_{3 \times 3}^+\rangle$ is a two-qubit Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ embedded in the 3×3 system and $\sigma_l \otimes \sigma_l$ acts on this two-qubit system.

Device independent scenario.—The amount of entan-

glement can be bounded *exclusively* from the observed data but independent of the quantum description. Depending whether only one or both sides are untrusted one distinguishes between a steering-type or a Bell-type scenario. The necessary steps to lift the method using only partial information to such device independent scenarios employs the translation idea highlighted in Ref. [15] and is explained in more detail in the supplement [33]. As an example, in Fig. 3(c) we plot a lower bound on the linear entropy of entanglement given as a function of the violation of the CHSH Bell inequality [1].

Concave roof.—Besides convex roofs, concave roofs can also be computed. For example, if in Eq. (2) a concave roof is used instead of a convex roof, then we compute the linear entanglement of assistance [62], which is the maximal entanglement available if the mixed state is given as a purification to us, and a third party which holds the ancilla needed for the purification is assisting us. In this case, in our method minimum must be replaced by maximum. In this way, we obtain a converging series of *upper* bounds on the entanglement of assistance. The results are shown in Fig. 3(d) for the family of 3×3 states

$$\rho_E(p_E) = p_E |\Psi_E\rangle\langle\Psi_E| + (1 - p_E) \frac{1}{9} \mathbb{1}, \quad (15)$$

where $|\Psi_E\rangle = \epsilon|00\rangle + \epsilon|11\rangle + \sqrt{1 - 2\epsilon^2}|22\rangle$ and $\epsilon = 0.3$. As a reference, the linear entropy of entanglement is also shown for the same state.

Conclusions.—We have shown a general framework for calculating convex roof-based entanglement measures. We demonstrated its use in calculating the entanglement for bipartite systems, as well as, the three-tangle for three-qubits. We discussed several other quantities for which it can be applied. In the future, we would like to explore further possibilities of using our algorithm to compute convex roofs, in calculating the linear Holevo capacity [63, 64], the quantum Fisher information based on incomplete information [65], or the convex or concave roofs of sums of several variances, as outlined in the Supplement [33].

We thank C. Eltschka, M. Kús, J. Siewert, and M. Tiersch for stimulating discussions. We thank the EU (ERC Starting Grant GEDENTQOPT, CHISTERA QUASAR, Marie Curie CIG 293993/ENFOQI), the MINECO (Project No. FIS2012-36673-C03-03), the Basque Government (Project No. IT4720-10), the OTKA (Contract No. K83858), the UPV/EHU program UFI 11/55, the FQXi Fund (Silicon Valley Community Foundation), and the DFG.

* Electronic address: toth@alumni.nd.edu;
URL: <http://www.gtoth.eu>

[1] R. Horodecki *et al.*, Rev. Mod. Phys. **81**, 865 (2009); O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

- [2] J.-W. Pan *et al.*, Nature (London) **403**, 515 (2000); M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004); W. Wiczkorek *et al.*, Phys. Rev. Lett. **103**, 020504 (2009).
- [3] O. Gühne, M. Reimpell, and R. F. Werner Phys. Rev. Lett. **77**, 052317 (2008).
- [4] J. Eisert, F. G. S. L. Brandao, and K. M. R. Audenaert, New J. Phys. **9**, 46 (2007).
- [5] H. Wunderlich and M. B. Plenio, J. Mod. Opt. **56**, 2100 (2009).
- [6] A. Osterloh *et al.*, Nature (London) **416**, 608 (2002); M. Cramer *et al.*, Nat. Commun. **4**, 2161 (2013).
- [7] W. K. Wootters, Phys. Rev. Lett. **80** 2245, (1998).
- [8] T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).
- [9] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
- [10] A. Acín *et al.*, Phys. Rev. Lett. **87**, 040401 (2001).
- [11] A. Sanpera, D. Bruß, and M. Lewenstein, Phys. Rev. A **63**, 050301 (2001).
- [12] B. Röthlisberger, J. Lehmann, and D. Loss, Phys. Rev. A **80**, 042301 (2009).
- [13] F. Verstraete and M. M. Wolf, Phys. Rev. Lett. **89**, 170401 (2002).
- [14] Y.-C. Liang, T. Vértesi, and N. Brunner, Phys. Rev. A **83**, 022108 (2011).
- [15] T. Moroder *et al.*, Phys. Rev. Lett. **111**, 030501 (2013).
- [16] M. Pusey, Phys. Rev. A **88**, 032313 (2013)
- [17] P. Rungta *et al.*, Phys. Rev. A **64**, 042315 (2001).
- [18] P. Rungta and C. M. Caves, Phys. Rev. A **67**, 012307 (2003); G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [19] M. Huber, and J. I. de Vicente, Phys. Rev. Lett. **110**, 030501 (2013); M. Huber, M. Perarnau-Llobet, and J.I. de Vicente, Phys. Rev. A **88**, 042328 (2013).
- [20] P. Horodecki, Phys. Rev. A **68**, 052101 (2003).
- [21] F. Mintert, M. Kus, and A. Buchleitner, Phys. Rev. Lett. **95**, 260502 (2005).
- [22] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [23] Every symmetric separable state of N particles can be written as $\sum_k q_k |\Phi_k\rangle\langle\Phi_k|^{\otimes N}$, $\sum_k q_k = 1$, and $q_k > 0$. See J. Korbicz, J. I. Cirac, and M. Lewenstein, Phys. Rev. Lett. **95**, 120502 (2005).
- [24] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [25] M. Horodecki *et al.*, Phys. Rev. Lett. **80**, 5239 (1998); for a review see P. Horodecki in D. Bruß and G. Leuchs (eds.), *Lectures on Quantum Information* (Wiley-VCH, Berlin, 2006).
- [26] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [27] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005); A. Acín *et al.*, Phys. Rev. Lett. **92**, 107903 (2004); G. Tóth *et al.*, Phys. Rev. Lett. **99**, 250405 (2007).
- [28] Z.-H. Chen, Z.-H. Ma, O. Gühne, and S. Severini, Phys. Rev. Lett. **109**, 200503 (2012).
- [29] The CoRoNa package can be downloaded at <http://www.mathworks.com/matlabcentral/fileexchange/47823-corona>
- [30] K. Chen, S. Albeverio, and S.-M. Fei, Phys. Rev. Lett. **95**, 040504 (2005); J. I. de Vicente, Phys. Rev. A **75**, 052320 (2007); **77**, 039903(E) (2008); O. Gittsovich and O. Gühne, Phys. Rev. A **81**, 032333 (2010).
- [31] E. Gerjuoy, Phys. Rev. A **67**, 052308 (2003); Y.-C. Ou, H. Fan, and S.-M. Fei, Phys. Rev. A **78**, 012311 (2008); M. Li, S.-M. Fei, and Z.-X. Wang, J. Phys. A: Math.

- Theor. **42**, 145303 (2009).
- [32] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004); **71**, 032333 (2005).
- [33] See Supplemental Material, which includes Refs. [34–41, 43–45].
- [34] D. A. Meyer and N. R. Wallach, J. Math. Phys. **43** 4273 (2002).
- [35] A. J. Scott, Phys. Rev. A **69**, 052330 (2004).
- [36] G. Tóth, Phys. Rev. A **85**, 022322 (2012); P. Hyllus *et al.*, Phys. Rev. A **85**, 022321 (2012).
- [37] G. Tóth *et al.*, Phys. Rev. Lett. **99**, 250405 (2007).
- [38] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
- [39] Z. Léka and D. Petz, Probab. Math. Statist. **33**, 191 (2013).
- [40] D. Viosztek and D. Petz, arXiv:1311.3908.
- [41] G. Tóth and D. Petz, Phys. Rev. A **87**, 032324 (2013); S. Yu, arXiv:1302.5311.
- [42] B. Jungnitsch, T. Moroder, and O. Gühne, Phys. Rev. Lett. **106**, 190502 (2011).
- [43] T. Moroder and O. Gühne, unpublished (2014). This problem is in the problem book of the National Quantum Information Centre, Gdansk.
- [44] M. Navascués, S. Pironio, A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); New J. Phys. **10**, 073013 (2008)
- [45] A. C. Doherty *et al.*, Proceedings of IEEE Conference on Computational Complexity 2008, pages 199–210; arXiv:0803.4373.
- [46] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
- [47] O. Gühne *et al.*, Phys. Rev. Lett. **99**, 130504 (2007).
- [48] O. Rudolph, Quantum Inf. Process. **4**, 219 (2005); K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).
- [49] G. Tóth and O. Gühne, Phys. Rev. Lett. **102**, 170503 (2009); Appl. Phys. B **98**, 617 (2010).
- [50] This extension is different from the one in Observation 2 as it adds new copies of the entire bipartite system, rather than adding new copies of the parties A and B. Moreover, it can be shown that since the state ω_{12} is symmetric, an $1 : n$ PPT symmetric extension is the same as an $1 + \Delta : n - \Delta$ extension for any integer $0 < \Delta < n$.
- [51] M. Navascués, M. Owari, and M. B. Plenio, Phys. Rev. A **80**, 052306 (2009).
- [52] A. Osterloh and J. Siewert, Phys. Rev. A **86**, 042302 (2012).
- [53] G. Gour, Phys. Rev. A **71**, 012318 (2005).
- [54] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [55] The operator T can be obtained based on Eqs. (10-11) of Ref. [52].
- [56] More precisely, a bound has been developed for the convex roof of $\sqrt{\tau}$ in C. Eltschka and J. Siewert, Sci. Rep. **2**, 942 (2012). This quantity is also an entanglement monotone and, for pure states, it remains invariant under determinant 1 stochastic local operations and communication (SLOCC). See also C. Eltschka and J. Siewert, Phys. Rev. Lett. **108**, 230502 (2012).
- [57] L. Vandenbergh, S. Boyd, SIAM Review **38**, 49 (1996). We used YALMIP and SeDuMi. See J. Löfberg, in Proceedings of the CACSD Conference (Taipei, Taiwan, 2004), p. 284; J. F. Sturm, Optimization Methods and Software **17**, 1105 (2002).
- [58] M. M. Sinolecka, K. Życzkowski, and M. Kus, Act. Phys. Pol. B **33**, 2081 (2002).
- [59] F. Verstraete, J. Dehaene, and B. De Moor, Phys. Rev. A **68**, 012103 (2003).
- [60] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
- [61] C. Eltschka and J. Siewert, Phys. Rev. Lett. **111**, 100503 (2013)
- [62] D. P. DiVincenzo *et al.*, Entanglement of assistance. In *Quantum Computing and Quantum Communications* (pp. 247-257) (Springer, Berlin Heidelberg, 1999); arXiv:quant-ph/9803033.
- [63] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
- [64] T. J. Osborne and F. Verstraete, Phys. Rev. Lett. **96**, 220503 (2006).
- [65] C. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976); A. Holevo, Probabilistic and Statistical Aspects of Quantum Theory (North-Holland, Amsterdam, 1982); S.L. Braunstein and C.M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

Supplemental Material

In this supplemental material, we give some further details of our derivations.

Proof of Observation 2.

Let us assume that the state has $E_{\text{lin}}^{(\text{ppt})}(\varrho) = 0$. Then, from Eq. (8) it follows that there is a symmetric PPT state ω_{12} such that $\text{Tr}(\mathcal{A}_{AA'}\omega_{12}) = 0$ and $\text{Tr}_1(\omega_{12}) = \varrho$. Hence, for this state $\text{Tr}_{A'B'}(\omega_{12}) = \varrho$ and $\mathcal{F}_{AA'}\omega_{12} = \omega_{12}$. The symmetry of ω_{12} means that $\mathcal{F}_{AA'}\mathcal{F}_{BB'}\omega_{12} = \omega_{12}$. Hence, $\mathcal{F}_{BB'}\omega_{12} = \omega_{12}$ also holds. We can write

$$\omega_{12}^{TAB} = (\mathcal{F}_{AA'}\omega_{12}\mathcal{F}_{AA'})^{TAB} = \mathcal{F}_{AA'}\omega_{12}^{TA'B}\mathcal{F}_{AA'}. \quad (\text{S1})$$

Since $\mathcal{F}_{AA'}$ is unitary, $\omega_{12}^{TAB} \geq 0$ implies $\omega_{12}^{TA'B} \geq 0$. Finally, we obtain

$$\varrho^{TA} = \text{Tr}_{A'B'}(\omega_{12}^{TA'B}). \quad (\text{S2})$$

Hence, $\omega_{12}^{TA'B} \geq 0$ implies $\varrho^{TA} \geq 0$. This proves the first part of our observation.

To prove the second part, note that based on the discussion above ω_{12} is a 2:2 symmetric extension of ϱ . It is not necessarily a PPT symmetric extension since for the $A : BA'B'$ partition it can also be non-PPT.

Finally, the third part can be proved as follows. Let us assume that ϱ has a 2 : 2 PPT symmetric extension denoted by ω_{12} . Hence, $\mathcal{F}_{AA'}\omega_{12} = \omega_{12}$ and $\mathcal{F}_{BB'}\omega_{12} = \omega_{12}$. Moreover, ω_{12} is a PPT state. Hence, $\text{Tr}(\mathcal{A}_{AA'}\omega_{12}) = 0$. ■

Note that Theorem 2 can be generalized to states that have $E_{\text{lin}}^{(n)}(\varrho) > 0$, involving PPT symmetric extensions and symmetric extensions to several parties.

Quantitative entanglement witnesses

In this section, we describe how our method can be used to construct quantitative entanglement witnesses. As an example, we present a condition for entanglement witnesses, such that the expectation value of all witnesses satisfying the condition gives a lower bound on $E_{\text{lin}}^{(\text{ppt})}$ defined in Eq. (8). We also prove that for every state ϱ_{AB} there is a witness of this type that gives not only a lower bound, but gives the value of $E_{\text{lin}}^{(\text{ppt})}$ exactly.

For the linear entropy of entanglement we needed to minimize the expectation value of the operator $M = \mathcal{A}_{AA'} \otimes \mathbb{1}_{BB'}$ over all symmetric separable states ω_{12} with a fixed reduced marginal $\text{Tr}_2(\omega_{12}) = \rho_{AB}$. Consider now an operator $W = W_{AB}$ that acts on the original bipartite Hilbert space. We require that it satisfies

$$M - \Pi_{\text{sym}}(W \otimes \mathbb{1})\Pi_{\text{sym}} = P + \Pi_{\text{sym}}Q^{T_1}\Pi_{\text{sym}} \quad (\text{S3})$$

where $P, Q \geq 0$. Here P is an operator acting only on the symmetric subspace of the two copies $\text{Sym}(\mathcal{H}_{AB}^{\otimes 2})$, while Q acts on the full tensor product $\mathcal{H}_{AB}^{\otimes 2}$ but we only used the projected symmetric part of the partial transpose. For such a decomposition, it can be shown that its expectation value for ω_{12} is

$$\begin{aligned} \text{Tr}\{[M - \Pi_{\text{sym}}(W \otimes \mathbb{1})\Pi_{\text{sym}}]\omega_{12}\} \\ &= \text{Tr}(P\omega_{12}) + \text{Tr}(\Pi_{\text{sym}}\omega_{12}\Pi_{\text{sym}}Q^{T_1}) \\ &= \text{Tr}(P\omega_{12}) + \text{Tr}(\omega_{12}Q^{T_1}) \\ &= \text{Tr}(P\omega_{12}) + \text{Tr}(\omega_{12}^{T_1}Q) \geq 0. \end{aligned} \quad (\text{S4})$$

The projectors onto the symmetric subspace Π_{sym} can be dropped in the third line since ω_{12} is supported only on it. In the last line we used $\text{Tr}(XY^{T_1}) = \text{Tr}(X^{T_1}Y)$, while nonnegativity holds because all occurring operators are positive semidefinite. Hence, Eq. (S4) can be rewritten as

$$\begin{aligned} \text{Tr}(M\omega_{12}) &\geq \text{Tr}(\Pi_{\text{sym}}(W \otimes \mathbb{1})\Pi_{\text{sym}}\omega_{12}) \\ &= \text{Tr}(W\rho_{AB}), \end{aligned} \quad (\text{S5})$$

where we have further simplified the right-hand side using that ω_{12} has a fixed reduced density matrix. Since Eq. (S5) holds for any valid state ω_{12} , it holds in particular for the one yielding the linear entropy of entanglement, thus we arrive at

$$E_{\text{lin}}(\rho_{AB}) \geq \text{Tr}(W\rho_{AB}). \quad (\text{S6})$$

Hence the expectation value of our witness provides a lower bound on the linear entropy of entanglement.

Next, we will show that for a given quantum state ρ_{AB} , if we optimize over all such witness operators, it is always possible to find one that saturates the inequality (S6).

Observation 3.—For the linear entropy of entanglement we obtain

$$E_{\text{lin}}(\rho_{AB}) \geq E_{(\text{lin})}^{(\text{ppt})}(\rho_{AB}) = \sup_{W \in \mathcal{W}} \text{Tr}(W\rho_{AB}), \quad (\text{S7})$$

with \mathcal{W} being the set of all operators W of Eq. (S3).

Proof. The proof is given by applying the dual form of a semidefinite program [57], which has been employed in a variety of different quantum information problems. In particular we refer to Ref. [32] which explains such a procedure very nicely for the separability criterion based on symmetric extensions. We have structured the proof in two parts: In the first part, we show an equivalent formulation on the two-copy level. Afterwards we further simplify this dual problem to interpret it as an operator acting on a single density operator using techniques that were introduced in Ref. [32].

In the first part, we parse the original problem as given in Observation 1 into the form of a semidefinite program and invoke its dual, which provides the same solution. In order to achieve this one should note that the two

conditions, ω_{12} just supported on the symmetric subspace and the linear equations $\text{Tr}_1(\omega) = \text{Tr}_2(\omega) = \rho_{AB}$ can be satisfied automatically with an appropriate ansatz $\omega_{12}(\mathbf{x}) = \omega_{12}^{\text{fix}} + \sum_i x_i F_i$. Here $\omega_{12}^{\text{fix}} = \sum_i s_i B_i$ is the fixed part of two-copy density operator such that the marginals equal to ρ_{AB} (its precise form being discussed later), while the remaining part $\sum_i x_i F_i$ is the yet to be determined part on the symmetric subspace, *i.e.*, the set of operators $\{B_i\}_i \cup \{F_i\}_i$ is a Hermitian operator basis for the symmetric subspace $\text{Sym}(\mathcal{H}^{\otimes 2})$. With this the primal problem reads

$$\begin{aligned} \inf \quad & \text{Tr}(M\omega_{12}^{\text{fix}}) + \sum_i x_i \text{Tr}(MF_i) & (\text{S8}) \\ \text{s.t.} \quad & \omega_{12}(\mathbf{x}) = \omega_{12}^{\text{fix}} + \sum_i x_i F_i \geq 0, \\ & \omega_{12}(\mathbf{x})^{T_1} = (\omega_{12}^{\text{fix}})^{T_1} + \sum_i x_i F_i^{T_1} \geq 0, \end{aligned}$$

where one should note that $\omega_{12}(\mathbf{x})$ acts on the symmetric subspace, while $\omega_{12}(\mathbf{x})^{T_1}$ acts on the full tensor $\mathcal{H}^{\otimes 2}$.

Taking this into account, it is straightforward to invoke the dual and to derive an equivalent optimization problem. That this dual program provides the same solution is certified for instance via the Slater regularity condition [57], which holds since this problem has an inner point, *i.e.*, $\omega_{12} = \Pi_{\text{sym}}(\rho_{AB} \otimes \rho_{AB})\Pi_{\text{sym}} > 0$ if ρ_{AB} has full rank; otherwise one should constrain \mathcal{H} anyway to the range of ρ_{AB} . Since such reformulations have been carried out quite frequently, we refer here only to the literature, and continue with its solution, which is given by

$$\begin{aligned} \sup \quad & \text{Tr}(Z_{\text{fix}}\omega_{12}^{\text{fix}}) & (\text{S9}) \\ \text{s.t.} \quad & M - Z_{\text{fix}} = P_{\text{sym}} + \Pi_{\text{sym}}Q^{T_1}\Pi_{\text{sym}}, \\ & Z_{\text{fix}} = \sum_i z_i B_i, \\ & P_{\text{sym}} \geq 0, Q \geq 0, \end{aligned}$$

where similarly P_{sym} acts on $\text{Sym}(\mathcal{H}^{\otimes 2})$ and Q on the full tensor product space. This finishes the first part.

In the remaining part we show how the objective of Eq. (S9) can be interpreted as an operator on the single copy. For that we need some structure of the fixed part ω_{12}^{fix} that is given by the reduced state ρ_{AB} . The idea follows closely the ideas of Ref. [32], though we need to do it here for the symmetric subspace.

To start, note that any given density operator ρ_{AB} can be written as $\rho_{AB} = \mathbb{1}/d + \sum_i \text{Tr}(S_i\rho_{AB})S_i$ with $\{S_i\}_i$ being an operator basis for the traceless Hermitian operators. Next let us define $O_i = \Pi_{\text{sym}}(S_i \otimes \mathbb{1})\Pi_{\text{sym}}$. The expectation values of all these operators O_i are completely determined by the reduced state $\text{Tr}(O_i\omega_{12}(\mathbf{x})) = \text{Tr}(O_i\omega_{12}^{\text{fix}}) = \text{Tr}(S_i\rho_{AB})$, and since all these state coefficients are independent this means that the set $\{O_i\}_i$ is linearly independent. This implies a positive definite

Gram matrix $G_{ij} = \text{Tr}(O_i O_j) > 0$, a unique inverse G^{-1} , and the existence of the operators $\tilde{O}_i = \sum_j (G^{-1})_{ij} O_j$. These operators are the corresponding orthogonal operators $\text{Tr}(\tilde{O}_i O_j) = \delta_{ij}$, so that the fixed part becomes

$$\begin{aligned} \omega_{12}^{\text{fix}} &= \Pi_{\text{sym}}/d_{\text{sym}} + \sum_i \text{Tr}(O_i\omega_{12}^{\text{fix}})\tilde{O}_i \\ &= \Pi_{\text{sym}}/d_{\text{sym}} + \sum_i \text{Tr}(S_i\rho_{AB})\tilde{O}_i. \end{aligned} \quad (\text{S10})$$

Note that also the desired dimensionality of d^2 matches, since $\text{Tr}_1(\omega_{12}) = \text{Tr}_2(\omega_{12}) = \rho_{AB}$ are exactly d^2 independent linear equations. To transfer this to the single copy level we write this solution in terms of a map applied to $\Lambda[\rho_{AB}] = \omega_{12}^{\text{fix}}$,

$$\Lambda[\rho_{AB}] = \text{Tr}(\rho_{AB})\Pi_{\text{sym}}/d_{\text{sym}} + \sum_i \text{Tr}(S_i\rho_{AB})\tilde{O}_i. \quad (\text{S11})$$

This map has the adjoint map, *i.e.*, the map satisfying $\text{Tr}(X\Lambda[Y]) = \text{Tr}(\Lambda^\dagger[X]Y)$ for all matrices X, Y ,

$$\Lambda^\dagger[Z] = \text{Tr}(Z)\mathbb{1}/d_{\text{sym}} + \sum_i \text{Tr}(\tilde{O}_i Z)S_i. \quad (\text{S12})$$

Via this we can finally make the connection to the single copy level by

$$\begin{aligned} \text{Tr}(Z_{\text{fix}}\omega_{12}^{\text{fix}}) &= \text{Tr}(Z_{\text{fix}}\Lambda[\rho_{AB}]) \\ &= \text{Tr}(\Lambda^\dagger[Z_{\text{fix}}]\rho_{AB}) \equiv \text{Tr}(W_Z\rho_{AB}), \end{aligned} \quad (\text{S13})$$

where we defined the single copy witness $W_Z = \Lambda^\dagger[Z_{\text{fix}}]$ in the last equation, parametrized in terms of the coefficients of Z_{fix} . However since we want to have the witness as the open parameter we need to parametrize $Z_{\text{fix}}(W)$ in terms of the witness W . Setting

$$\begin{aligned} Z_{\text{fix}}(W) &= \Pi_{\text{sym}}(W \otimes \mathbb{1})\Pi_{\text{sym}}, \\ &= d\text{Tr}(W)\Pi_{\text{sym}} + \sum_i \text{Tr}(S_i W)O_i \end{aligned} \quad (\text{S14})$$

achieves $\Lambda[Z_{\text{fix}}(W)] = W$. Via this we can finally replace all occurrences of Z_{fix} in Eq. (S9) by W and we obtain the stated result of the observation. \blacksquare

Note that one can obtain other quantitative entanglement witnesses if one replaces the decomposable structure, as given in Eq. (S3), by a different entanglement witness condition. It is easy to see that if the operator $M - \Pi_{\text{sym}}(W \otimes \mathbb{1})\Pi_{\text{sym}}$ is non-negative on separable states then $\text{Tr}(W\rho_{AB})$ gives a lower bound. Compared to other possibilities, the advantage of the witness (S3) is that the optimization (S7) to get the lower bound can be carried out with semidefinite programming.

We also add that if one only has measured a few observables $\{O_i\}_i$ then to get a lower bound one merely has to add the constraint $W = \sum_i w_i O_i$, which means that the witness is a linear combination of the measured observables with coefficients w_i . Then, we have to optimize

$\sum_i w_i v_i$, where v_i are the corresponding expectation values $\langle O_i \rangle_\rho$.

Finally, if one also wants quantitative entanglement witness for the other tasks one can proceed similarly. For instance, if one likes to bound the tangle one demands that $T - \Pi_{\text{sym}}(W \otimes \mathbb{1}^{\otimes 3})\Pi_{\text{sym}}$ is a non-negative on all fully separable states, thus it is an entanglement witness to test against full separability.

Other quantities that can be calculated by our approach

Convex roof of the Meyer-Wallach measure.—The Meyer-Wallach measure is an entanglement measure for pure states defined as [34]

$$Q = \frac{1}{N} \sum_{n=1}^N 2S_{\text{lin}}(\varrho_n), \quad (\text{S15})$$

where ϱ_n is the reduced state of the n^{th} qubits. This measure can be generalized to include the reduced states of multi-qubit groups [35]. Our method can calculate the convex roof of the measure (S15) and the generalized measures as well.

Holevo capacity.—The linear Holevo χ capacity is defined as [63, 64]

$$\chi_2(\Lambda) = \max_{\{p_k, |\Psi_k\rangle\}} \left\{ S_{\text{lin}}(\Lambda(\varrho)) - \sum_k p_k S_{\text{lin}}[\Lambda(|\Psi_k\rangle)] \right\}. \quad (\text{S16})$$

It is a capacity measure for a channel Λ . For qubit channels, explicit formula is given in Ref. [64].

Convex and concave roofs in entanglement conditions with the quantum Fisher information and the variance.—First, let us see simple entanglement conditions with the quantum Fisher information and the variance. We start from the fact that for pure N -qubit states

$$(\Delta J_x)^2 + (\Delta J_y)^2 + (\Delta J_z)^2 = \frac{N}{2} \quad (\text{S17})$$

holds. Next, we need the fundamental properties of the quantum Fisher information $F_Q[\varrho, A]$ in our criteria [65]: (i) For pure states $F_Q[\varrho, A]$ equals four times the variance $(\Delta A)_\varrho^2$. (ii) For mixed states, it is a convex function of the state. Hence, for separable states follows [36]

$$\frac{1}{4} \sum_{l=x,y,z} F_Q[\varrho, J_l] \leq \frac{N}{2}. \quad (\text{S18})$$

Due to the concavity of the variance, we can obtain a similar entanglement condition with variances as [37]

$$(\Delta J_x)^2 + (\Delta J_y)^2 + (\Delta J_z)^2 \geq \frac{N}{2}. \quad (\text{S19})$$

Any state that violates Eq. (S18) or Eq. (S19) is entangled.

The conditions (S18) and (S19) can be improved if we take the concave and convex roofs, respectively, of the left-hand sides of Eq. (S17). Hence, alternative separability conditions arise

$$\min_{\{p_k, |\Psi_k\rangle\}} \sum_k p_k \sum_{l=x,y,z} (\Delta J_l)_{\Psi_k}^2 \leq \frac{N}{2}, \quad (\text{S20})$$

and

$$\max_{\{p_k, |\Psi_k\rangle\}} \sum_k p_k \sum_{l=x,y,z} (\Delta J_l)_{\Psi_k}^2 \geq \frac{N}{2}. \quad (\text{S21})$$

Any state that violates these is entangled. Numerical evidence shows that Eq. (S20) is stronger than Eq. (S18). Moreover, numerical evidence shows also that Eq. (S21) is stronger than Eq. (S19). These ideas can be extended to improve other entanglement conditions based on variances [38].

We note that Ref. [39] shows that 2×2 covariance matrices $C_\varrho(A, B)$ can always be decomposed as the

$$C_\varrho(A, B) = \sum_k p_k C_{\Psi_k}(A, B), \quad (\text{S22})$$

where ϱ has the decomposition as in Eq. (3). Hence, we know that the bound on the sum of two variances cannot be improved this way. However, Ref. [40] demonstrates that such a decomposition is not always possible for 3×3 covariance matrices. This is connected to the fact that the bound for separable states for the sum of three variances can be improved.

Quantum Fisher information based on incomplete data.—The quantum Fisher information can be bounded from below from partially known data. That is, we know the expectation value of some operators, and want to find a lower bound for the quantum Fisher information. The problem can be mapped to a semidefinite optimization in the two-copy space. A very good lower bound can be obtained if we optimize over PPT states.

For that we can use that the quantum Fisher information is, apart from a constant factor, the convex roof of the variance [41]

$$F_Q[\varrho, A] = 4 \min_{\{p_k, |\Psi_k\rangle\}} \sum_k p_k (\Delta A)_{\Psi_k}^2. \quad (\text{S23})$$

The variance of a pure state $|\Psi\rangle$ can be expressed on two copies as

$$(\Delta A)_\Psi^2 = \text{Tr}[(A^2 \otimes \mathbb{1} - A \otimes A)|\Psi\rangle\langle\Psi| \otimes |\Psi\rangle\langle\Psi|]. \quad (\text{S24})$$

Hence, a lower bound on the quantum Fisher information can be obtained as

$$\begin{aligned} F_Q^{(\text{ppt})}[\varrho, A] &= \min_{\omega_{12}} \text{Tr}[(A^2 \otimes \mathbb{1} - A \otimes A)\omega_{12}], \\ &\text{s.t. } \omega_{12} \text{ symmetric, PPT,} \\ &\text{Tr}(O_i \omega_1) = v_i, \end{aligned} \quad (\text{S25})$$

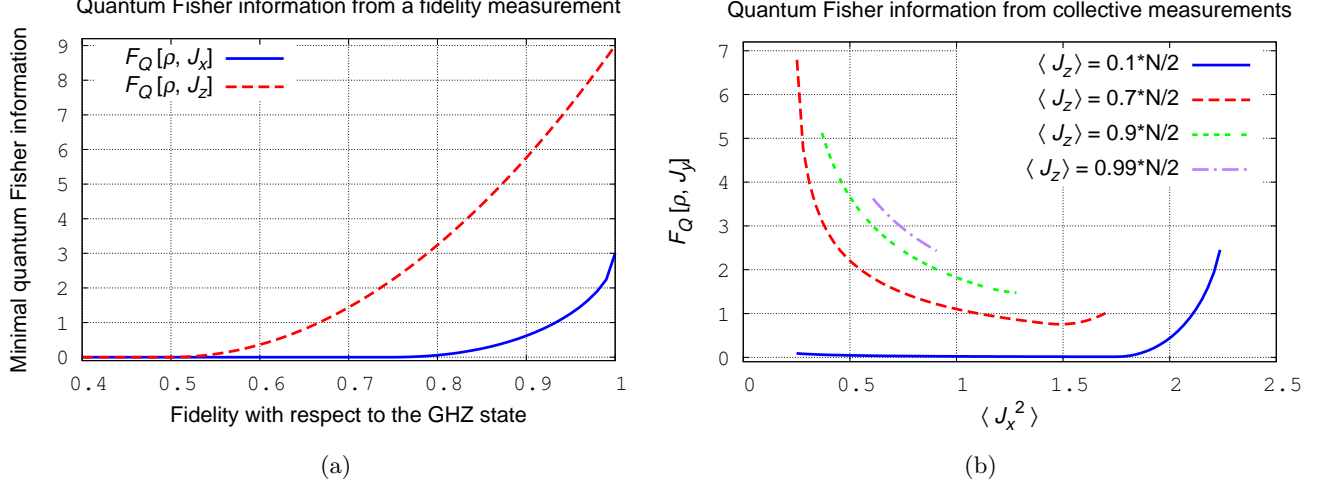


FIG. S1: (a) Lower bound on $F_Q[\rho, J_z]$ based on the fidelity with respect to the three-qubit GHZ state. (b) Lower bound on $F_Q[\rho, J_y]$ based on $\langle J_x^2 \rangle$ for various values of $\langle J_z \rangle$ and for $\langle J_x \rangle = 0$, for $N = 3$ qubits.

where the constraints are given with the expectation values $v_i = \langle O_i \rangle_\rho$. The optimization (S25) can straightforwardly be carried out with semidefinite programming.

In Fig. S1(a), we present a simple example where a lower bound on the quantum Fisher information $F_Q[\rho, J_z]$ is shown based on measurements of the fidelity with respect to the GHZ state. Below a fidelity of $1/2$, the bound for $F_Q[\rho, J_z]$ is zero. This is due to the fact that the product state $|11..111\rangle$ reaches this fidelity value, while $F_Q[\rho, J_z]$ is zero for this state. If the fidelity is 1, we obtain $F_Q[\rho, J_z] = N^2$ and $F_Q[\rho, J_x] = N$, as expected [36].

In Fig. S1(b), we present a bound on the quantum Fisher information based on collective measurements, relevant to spin squeezing. Note that for well polarized ensembles, increasing $\langle J_x^2 \rangle$ leads to decreasing $F_Q[\rho, J_y]$. On the other hand, for small $\langle J_z \rangle$, increasing $\langle J_x^2 \rangle$ leads to increasing $F_Q[\rho, J_y]$. Some of the curves have points only in certain ranges of $\langle J_x^2 \rangle$, as there are no physical states corresponding to measurement results outside of these ranges, assuming a given value for $\langle J_z \rangle$ and $\langle J_x \rangle = 0$.

Similar methods can be used for bounding the variance of an observable from above based on the expectation value of other observables. We can use that the variance is the concave roof of itself [41]

$$(\Delta A)^2 = \max_{\{p_k, |\Psi_k\rangle\}} \sum_k p_k (\Delta A)_{\Psi_k}^2. \quad (\text{S26})$$

The difference between the two cases is that for the quantum Fisher information we have to look for the minimum, while for the variance we have to look for the maximum.

Genuine multipartite entanglement.—It is possible to define quantities that detect true multipartite entanglement and can be evaluated with our method. Let us

define

$$G = \min_{\{p_k, |\Psi_k\rangle\}} \sum_k p_k \prod_n S_{\text{lin}n}(|\Psi\rangle_k) \quad (\text{S27})$$

where $S_{\text{lin}n}(|\Psi\rangle)$ is the linear entropy for the n^{th} bipartition of the qudits. To be more precise, $S_{\text{lin}n}(|\Psi\rangle)$ is the linear entropy of the reduced state of the qudits in one of the two partitions for the n^{th} bipartition. If $G = 0$ then the state is biseparable, otherwise it is genuine multipartite entangled.

Similar idea can work such that only a sum of entropies must be computed by defining

$$H = \min_{\{\rho_n\}} \sum_n p_n E_{\text{lin}n}(\rho_n), \quad (\text{S28})$$

$$\text{s.t.} \quad \sum_n p_n \rho_n = \rho,$$

where $E_{\text{lin}n}$ is linear entropy for the n^{th} bipartition. If $H = 0$ then the state is biseparable, otherwise it is genuine multipartite entangled. If, instead of $E_{\text{lin}}(\rho)$, we calculate $E_{\text{lin}}^{\text{(ppt)}}$ given in Eq. (8) then Eq. (S28) can be obtained via a semidefinite program. The advantage of Eq. (S28) is that only two copies of the original state are needed to calculate the value with our approach, while for the formula (S27) we need much more copies. The formalism of Eq. (S28) is in the spirit of the PPT mixer detecting genuine multipartite entanglement [42].

Note that a three-qubit state mixed from states that are PPT with respect to some partitions have been found that is genuine multipartite entangled [43]. Thus, detecting genuine multipartite entanglement is a non-trivial task.

Device independent programs

In this section, we explain the methods to obtain lower bounds on the linear entropy of entanglement for the device independent scenarios; either in the steering case where only the apparatus of one side is uncharacterized, or in Bell-type scenarios where both sides are unknown.

We will use the tool presented in Ref. [15], resting on ideas from Ref. [44, 45], which transforms the problem of estimating entanglement in a device independent scenario into the more common problem to lower bound the entanglement of a given fixed finite-dimensional system having only partial information. The method uses instead of the quantum state ρ of unknown dimension, a finite dimensional object χ which captures most of the properties of the state.

To set the stage, let us assume that on a given side, say system A , one only knows the number of settings $x = 1, \dots, n$ and respective outcomes $a = 1, \dots, m$. This measurement scheme is described by a collection of POVM elements $M_{a|x}$, which act on a Hilbert space \mathcal{H}_A of unknown dimension. To this measurement scenario one now associates a specific completely positive local map: $\Lambda_A(\rho_A) = \sum_k F_k \rho_A F_k^\dagger$ with Kraus operators $F_k = \sum_{\mathbf{i}} |\mathbf{i}\rangle_{\bar{A}} \langle k| M_{\mathbf{i}}$. Here $|k\rangle_A$ and $|\mathbf{i}\rangle_{\bar{A}}$ are respective basis states of the input and output Hilbert spaces, while $M_{\mathbf{i}}$ are operators out of a chosen set \mathcal{M} on which we comment shortly. However, via this structure, first observe that this map transforms a given input state ρ_A to

$$\chi_{\bar{A}} = \Lambda_A[\rho_A] = \sum_{\mathbf{i}, \mathbf{j}} |\mathbf{i}\rangle \langle \mathbf{j}| \text{Tr}(M_{\mathbf{j}}^\dagger M_{\mathbf{i}} \rho_A), \quad (\text{S29})$$

hence an output with matrix elements given by certain expectation values. At this stage the specific operator set \mathcal{M} becomes important, since so far we know nothing about $\chi_{\bar{A}}$ because we neither know ρ_A nor $M_{\mathbf{i}}$. The only knowledge that we have are certain generic properties of the POVM elements $M_{a|x}$, more precisely we have (i) positivity $M_{a|x} \geq 0$, (ii) normalization $\sum_a M_{a|x} = \mathbb{1}$ and (iii) that each operator $M_{a|x}$ is a projector. Here note that by Naimark's extension any measurement can be written as a projector onto a larger dimensional space. Since for most device independent tasks this extension does not change the underlying tasks this property can be assumed without loss of generality. $M_{a|x} M_{a'|x} = \delta_{aa'} M_{a|x}$. In addition note that the expectation values of each measurement operator is observable, (iv) $\text{Tr}(M_{a|x} \rho_A) = P(a|x)$.

Via these four properties one can thus choose specific operator sets \mathcal{M} such that one has at least some partial information on $\chi_{\bar{A}}$. For instance, if one chooses \mathcal{M} to consist of the measurement operators $\mathcal{M} = \{M_{a|x}\}_{a,x}$ one knows for instance

$$\begin{aligned} \text{Tr}(M_{a|x} M_{a'|x} \rho_A) &= \delta_{aa'} \text{Tr}(M_{a|x} \rho_A) \\ &= \delta_{aa'} P(a|x), \end{aligned} \quad (\text{S30})$$

while other entries like $\text{Tr}(M_{a|x} M_{a'|x'} \rho_A)$ with $x \neq x'$ are still unknown. Nevertheless via this one gets some partial knowledge and some structure of $\chi_{\bar{A}}$, which can be captured by an explicit parametrization as

$$\begin{aligned} \chi_{\bar{A}}[P, u] &= \chi^{\text{fix}}[P] + \chi^{\text{open}}[u] \\ &= \sum_{a|x} P(a|x) Z_{a|x} + \sum_v u_v Z_v, \end{aligned} \quad (\text{S31})$$

using appropriate operators $Z_{a|x}$ and Z_v . Here the first part represents the known part of $\chi_{\bar{A}}$, while the second one is the restricted open unknown part.

Such a structure can be inferred for any choice of \mathcal{M} . For instance, one could remove some linear dependencies of the just given example set if one adds the identity and erases the last outcome for each measurement setting $\mathcal{M}_1 = \{\mathbb{1}\} \cup \{M_{a|x}\}_{a < n, x}$. In addition note that one could also enlarge this set by including also products up to N POVM elements \mathcal{M}_N , so for instance $\mathcal{M}_2 = \mathcal{M}_1 \cup \{M_{a|x} M_{a'|x'}\}_{a, a' < n, x \neq x'}$, already removing trivial parts. In this way one gets further relations like

$$\sum_{a'} \text{Tr}(M_{a|x} M_{a'|x'} M_{a''|x'} M_{a|x}) = P(a|x) \quad (\text{S32})$$

if $x \neq x'$. The advantage of including products is that one gets a tighter, more constrained, description. This set of operators \mathcal{M}_N is precisely the one which has been mostly used [15], since it is very straightforward to “decode” all the known structure. Still there are other possibilities, like $\mathcal{M}_t = \{M_{a_1|1} M_{a_2|2} \dots M_{a_n|n}\}_{a_1, \dots, a_n}$. Here it might be harder to deduce all the structure but it has for instance the advantage that the associated map Λ_A is then even trace-preserving, thus $\chi_{\bar{A}}$ can be completely interpreted as an output quantum state; something which is not directly possible if one uses \mathcal{M}_N .

Now let us come to the concrete cases. At first let us discuss the fully device independent case where both sides are completely uncharacterized. If we locally apply the just described trace-preserving physical map (using for instance the choice \mathcal{M}_t) we transform any state ρ_{AB} into another bipartite state $\chi_{\bar{A}\bar{B}} = \Lambda_A \otimes \Lambda_B(\rho_{AB})$. Since an entanglement monotone does not increase under local operators and classical communication, we get $E(\rho_{AB}) \geq E(\chi_{\bar{A}\bar{B}})$ and thus we obtain a valid lower bound by estimating the entanglement of the output state. Hence if we want to bound the linear entropy of entanglement by seeing a certain value of a Bell inequality $I \cdot P = V$ we use

$$\begin{aligned} E_{\min}(I \cdot P = V) & \geq \min_{\omega_{12}, u, P} \text{Tr}(\mathcal{A}_{12} \omega_{12}) \\ & \text{s.t. } \omega_{12} \text{ is } d_{\bar{A}} \times d_{\bar{B}}, \text{ symmetric, separable,} \\ & \omega_1 = \chi_{\bar{A}\bar{B}} = \chi_{\bar{A}\bar{B}}^{\text{fix}}[P] + \chi_{\bar{A}\bar{B}}^{\text{open}}[u] \geq 0, \\ & I_{\text{chsh}} \cdot P = V, \end{aligned} \quad (\text{S33})$$

Now let us turn to the steering case, where we assume that Alice's side is uncharacterized while Bob obtains complete tomography. Then the data are given by the collection of unnormalized density operators $\mathcal{E} = \{\varrho_{a|x}\}_{a,x}$ for Bob with $P(a|x) = \text{Tr}(\varrho_{a|x})$. In principle we can use the same method as for the fully device independent case by employ the trace-preserving local map only on one side $\chi_{\bar{A}B} = \Lambda_A \otimes \text{id}[\varrho_{AB}]$ and then bounding the linear entropy of entanglement of the output state.

However in this case we can do slightly better, since it is possible to bound the linear entropy of entanglement more directly on the original state ϱ_{AB} . This is in similar spirit as the negativity of Ref. [15] and Ref. [16]. Suppose we apply the same local, not necessarily trace-preserving, local map to the two copies $\chi_{12} \equiv \chi_{\bar{A}\bar{A}'BB'} = \Lambda_A \otimes \Lambda_A \otimes \text{id}[\omega_{12}]$. Then we can relax the constraint that ω_{12} is the symmetric PPT state of two qudits by $\chi_{12} \geq 0$, $\chi_{12}^{T_1} \geq 0$ and the permutation invariance

$$\begin{aligned} \mathcal{F}\chi_{12}\mathcal{F} &= \Lambda_A \otimes \Lambda_A \otimes \text{id}[\mathcal{F}\omega_{12}\mathcal{F}] \\ &= \Lambda_A \otimes \Lambda_A \otimes \text{id}[\omega_{12}] = \chi_{12}. \end{aligned} \quad (\text{S34})$$

Note that since the identity is within the set \mathcal{M} we have that the data of $\chi_{AB} = \Lambda_A \otimes \text{id}[\varrho_{AB}]$ are included in χ_{12} , thus we can directly parametrize $\chi_{12} = \chi_{12}^{\text{fix}}[\mathcal{E}] + \chi_{12}^{\text{open}}[u]$. The key difference compared to the previous case is that the objective value is still accessible. Due to the symmetry of the linear entropy of pure states, it is not surprising that $\mathcal{A}_{AA'}\mathbb{1}_{BB'} = \mathbb{1}_{AA'}\mathcal{A}_{BB'}$ holds on the symmetric subspace of the two copies. However, because the identity is included in \mathcal{M} and because Bob's side is characterized, the expectation value of $\mathbb{1}_{AA'}\mathcal{A}_{BB'}$ is given by a linear function of the values χ_{12} ; this linear function is denoted by $\text{Tr}(\hat{E}\chi_{12})$ as a shorthand. Then we get as a lower bound

$$\begin{aligned} E_{\min}(\mathcal{E}) &\geq \min_u \text{Tr}(\hat{E}\chi_{12}) \\ \text{s.t.} \quad &\chi_{12} = \chi_{12}^{\text{fix}}[\mathcal{E}] + \chi_{12}^{\text{open}}[u] \geq 0, \chi_{12}^{T_1} \geq 0. \end{aligned} \quad (\text{S35})$$

Before we conclude, let us point out that for both programs one can obtain sharper bounds if one includes more products into the generating set \mathcal{M} . This is very straightforward for the steering case, but even such programs quickly reach the border of being feasible. Here it remains to investigate which particular sets \mathcal{M} are more suitable than others. We leave this open for further investigation. If one combines these ideas with, for instance, the

Schmidt number program then one could access even the Schmidt number (often taken as a synonym for quantum dimension) also in a device independent way.

As an example we were investigating the simplest steering scenarios, where Alice, the uncharacterized side, has either two or three dichotomic measurements and Bob performs full tomography on his qubit. In this case the available data are given by the corresponding probabilities for Alice $P(r|s)$, with $r \in \{\pm 1\}$ denoting the out-

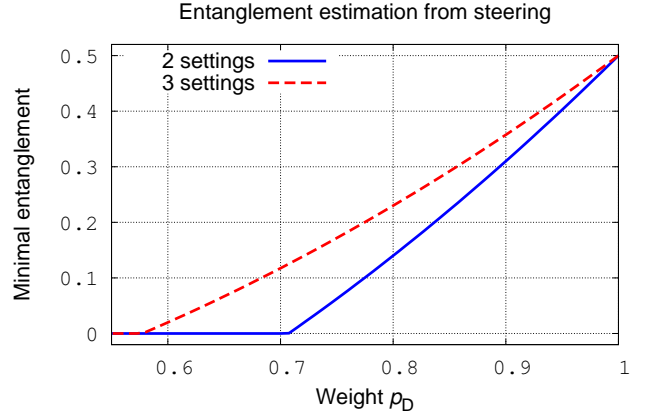


FIG. S2: Entanglement quantification via the simplest steering cases according to Eq. (S36).

come and $s \in \{1, 2, 3\}$ the setting, and the corresponding conditional states for Bob $\rho_{r|s}$.

For the examples we assume the following data

$$P(r|s) = \frac{1}{2}, \quad \rho_{r|s} = \frac{1}{2}(\mathbb{1} - rp_D\sigma_s), \quad (\text{S36})$$

with σ_s denoting the standard Pauli matrices. Such data are for instance generated by measuring the noisy singlet state of two qubits in the standard spin directions. Figure S2 shows the corresponding lower bound for the linear entropy of entanglement. We remark that the points where the lower bound becomes trivial coincide with the analytic cut-off value $p_D \leq 1/\sqrt{2}$ and $p_D \leq 1/\sqrt{3}$ respectively, while the lower bound at the maximum, $E_{\min} = 1$ is exact, since such observations require at least a maximally entangled two-qubit state.