# Detection of Multiparticle Entanglement: Quantifying the Search for Symmetric Extensions

Fernando G. S. L. Brandão[1,2] and Matthias Christandl[1]

[1]*Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Strasse 27, 8097 Zurich, Switzerland*
[2]*Departamento de Física, Universidade Federal de Minas Gerais, Belo Horizonte, Brazil*

(Received 30 May 2011; revised manuscript received 5 June 2012; published 17 October 2012)

We provide quantitative bounds on the characterization of multiparticle separable states by states that have locally symmetric extensions. The bounds are derived from two-particle bounds and relate to recent studies on quantum versions of de Finetti's theorem. We discuss algorithmic applications of our results, in particular a quasipolynomial-time algorithm to decide whether a multiparticle quantum state is separable or entangled (for constant number of particles and constant error in the norm induced by one-way local operations and classical communication, or in the Frobenius norm). Our results provide a theoretical justification for the use of the search for symmetric extensions as a test for multiparticle entanglement.

DOI: 10.1103/PhysRevLett.109.160502 PACS numbers: 03.67.Mn

Entanglement between two particles is a fundamental resource in quantum communication theory, being of vital importance in quantum teleportation [1], quantum key distribution [2,3], as well as more exotic tasks such as the simulation of noisy channels by noiseless ones [4,5]. The most famous criterion for deciding whether or not a state is entangled is the Peres-Horodecki test [6,7]: it is based on the observation that the partial transpose of a separable state is positive semidefinite and hence, if the partial transpose of a quantum state $\rho_{AB}$ is not positive semidefinite, then $\rho_{AB}$ must be entangled. Unfortunately, this criterion is only complete for two-by-two and two-by-three dimensional systems [8].

A hierarchy of separability criteria that detects every entangled state is the search for symmetric extensions [9]. This hierarchy is based on the observation that if $\rho_{AB}$ is separable, i.e., of the form $\sum_i p_i |\phi_i\rangle\langle\phi_i|_A \otimes |\psi_i\rangle\langle\psi_i|_B$, then for every $k$, we can define the state $\sum_i p_i |\phi_i\rangle\langle\phi_i|_A^{\otimes k} \otimes |\psi_i\rangle\langle\psi_i|_B$ which is manifestly symmetric under the permutation of the $A$ systems and extends the original state $\rho_{AB}$ [10]. Hence, if for some $k$ a given state $\rho_{AB}$ does not have an extension to $k$ copies of $A$ that is symmetric under interchange of the copies of $A$, then it must be entangled. The $k$th separability criterion is thus the search for a symmetric extension to $k$ copies of $A$. Quantum versions of the famous de Finetti theorem from statistics show that this hierarchy of criteria is complete [11–15]—i.e., every entangled state fails to have a symmetric extension for some $k$—and even provide quantitative bounds for the distance to the set of separable states measured in the trace norm [16,17] (see Fig. 1). Interestingly, these bounds can be improved if we add the Peres-Horodecki test as has been shown in Refs. [18,19] following a proposal to use the search for such extensions by semidefinite programming as a test to detect bipartite entanglement [9]. Whereas the algorithm works well in practice, from the bounds one can only infer a runtime exponential in the dimension the state, suggestively in agreement with the well-known result that the separability problem is NP hard [20,21].

In recent work jointly with Jon Yard, we have shown that the algorithm runs in quasipolynomial time (even without the Peres-Horodecki test) for constant error when one is willing to consider the weaker one-way local operation and classical communication (LOCC) norm [22–24]. The one-way LOCC norm is an operationally defined norm giving the optimal probability of distinguishing two two-particle states by local operations and one-way classical communication. Locality restricted norms, such as the one considered here, may actually be regarded as the more relevant norms in the distant laboratories paradigm, where Alice and Bob each hold part of a state and are restricted in their communication: a state that has a small distance to the set of separable states in such a norm, namely, will behave just like a separable state. This observation leads to a number of unexpected consequences of our results ranging from quantum data hiding to quantum complexity theory. It further follows that the algorithm remains fast if the Frobenius norm is considered instead. This provides a geometric interpretation of the results since the Frobenius norm is just the Euclidean norm when considering quantum states as elements in a real vector space.

Following their work in the two-particle case, Doherty *et al*. proposed a similar search for extensions in order to detect multiparticle entanglement [25]. With this Letter we provide a quantitative analysis of this proposal and prove that this hierarchy provides a family of necessary and sufficient conditions for multiparticle entanglement [26]. We do this by deriving a bound on the distance between multiparticle states that have symmetric extensions and multiparticle separable states in terms of the corresponding two-particle bounds (Theorem 1). We illustrate the result by considering the best known two-particle bounds (Corollary 1). As in the two-particle case, the one-way LOCC norm (and the Frobenius norm) result is shown to imply a quasipolynomial-time algorithm for the detection

 

of entanglement for a constant number of parties and for constant error (Corollary 2). The use of the search for symmetric extensions as multiparticle entanglement criteria has therefore been given a theoretical underpinning. We also show how our results can lead to a novel quantum version de Finetti's theorem in the one-way LOCC norm that depends only logarithmically on the local dimension (Corollary 3). This stands in sharp contrast to the trace norm case, where the dependence on the local dimension is at least linear [17].

*Symmetric extensions.*—We denote by $A_1, A_2, \cdots$ Hilbert spaces of finite but possibly different dimensions $|A_i|$ and let $\mathcal{S}_{A_1:A_2:\cdots:A_N} := \mathrm{conv}\{|\phi_1\rangle\langle\phi_1|_{A_1} \otimes |\phi_2\rangle \times \langle\phi_2|_{A_2} \cdots \otimes |\phi_N\rangle\langle\phi_N|_{A_N}\}$ be the set of separable states, where conv denotes the convex hull. We also define the convex sets of symmetrically extendible states $\mathcal{E}^{k_1,k_2,\cdots k_N}_{A_1:A_2:\cdots:A_N}$ consisting of all $\rho_{A_1A_2\cdots A_N}$ for which there is a state $\rho_{S^{k_1}(A_1)S^{k_2}(A_2)\cdots S^{k_N}(A_N)}$ with

$$\rho_{A_1A_2\cdots A_N} = \mathrm{tr}_{A_1^{k_1-1}A_2^{k_2-1}\cdots A_N^{k_N-1}} \rho_{S^{k_1}(A_1)S^{k_2}(A_2)\cdots S^{k_N}(A_N)}.$$

Here, $S^k(A)$ denotes the symmetric subspace of $A^k \equiv A^{\otimes k}$ and $\mathrm{tr}_{A^{k-1}}$ stands for the partial trace of all but one of the $A$ systems [27].

In order to measure distances between quantum states we consider a norm $\|*\|$ that is defined for all spaces of linear operators $\mathcal{L}(A_1 \otimes \cdots \otimes A_N)$ and that may depend on the decomposition into tensor factors (here indicated by colons) satisfying the following compatibility conditions: for all finite dimensional $A_1, A_2, \cdots, A_N, A_1', A_2', \cdots, A_N'$ and for all completely positive trace preserving maps $\Lambda_i: \mathcal{L}(A_i) \to \mathcal{L}(A_i')$ we have

$$\|\Lambda_1 \otimes \Lambda_2 \otimes \cdots \otimes \Lambda_N(*)\|_{A_1':A_2':\cdots:A_N'} \leq \|*\|_{A_1:A_2:\cdots:A_N} \quad (1)$$

and

$$\|*\|_{A_1\cdots A_j:A_{j+1}\cdots A_N} \leq \|*\|_{A_1:\cdots:A_j:A_{j+1}:\cdots:A_N}. \quad (2)$$

An example of a norm which satisfies the two conditions is the trace norm which can be written in the form

$$\|X\|_1 = \sup_{0\leq M\leq \mathbf{1}} \mathrm{tr}[(2M - \mathbf{1})X].$$

Note that it is independent of the split of the total Hilbert space into tensor products. A second norm satisfying the conditions is the one-way LOCC norm, defined in analogy with the trace norm as

$$\|X\|_{\mathsf{LOCC}^{\rightarrow}(A_1:\cdots:A_N)} := \sup_{M\in \mathsf{LOCC}^{\rightarrow}(A_1:\cdots:A_N)} \mathrm{tr}[(2M - \mathbf{1})X],$$

where $\mathsf{LOCC}^{\rightarrow}(A_1{:}A_2{:}\cdots{:}A_N)$ is the convex set of matrices $0 \leq M \leq \mathbf{1}$ such that there is a two-outcome measurement $\{M, \mathbf{1} - M\}$ that can be realized by one-way LOCC from $A_1$ to $A_2$ to $A_3$ and so on until $A_N$ (see Fig. 2). Note that the one-way LOCC norm does depend on the tensor product split.

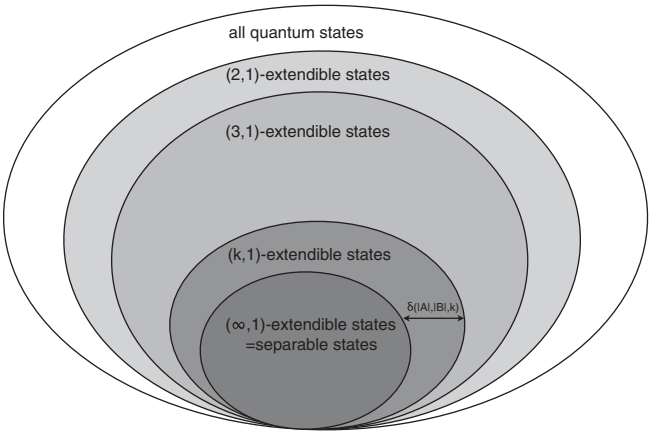


FIG. 1. Illustration of the hierarchy for two particles.

We say that $\delta \equiv \delta(|A|, |B|, k)$ is a two-particle bound for a norm $\|*\|$ if for all $\rho_{AB} \in \mathcal{E}^{k,1}_{A:B}$ there exists $\sigma \in \mathcal{S}_{A:B}$ with (see Fig. 1)

$$\|\rho - \sigma\|_{A:B} \leq \delta(|A|, |B|, k).$$

Note that $\delta(|A|, |B|, k)$ does not equal $\delta(|B|, |A|, k)$ in general. In fact, all known bounds either depend only on $|A|$ or only on $|B|$, the dimensions of $A$ and $B$, respectively.

*Multiparticle entanglement.*—We derive two results that quantify the closeness of a separable state to a symmetrically extendible multiparticle state in terms of two-particle bounds. The first result is tailored to a two-particle bound that only depends on $|A|$; the second depends only on $|B|$. We disregard nonappearing dimensions by setting them to infinity.

*Theorem 1.*—Let $\|*\|$ be a norm that satisfies Eqs. (1) and (2), assume that $\delta(|A|, |B|, k)$ is a two-particle bound for $\|*\|$, and let $\rho \in \mathcal{E}^{k_1,k_2,\ldots,k_N}_{A_1:A_2:\cdots:A_N}$. Then there exists $\sigma \in \mathcal{S}_{A_1:A_2:\cdots:A_N}$ with

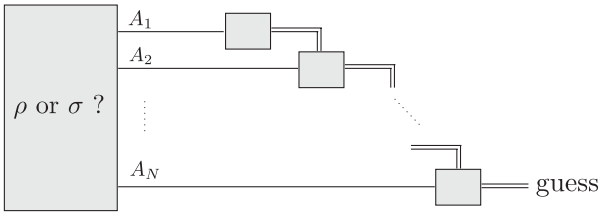


FIG. 2. $\frac{1}{4}\|\rho - \sigma\|_{\mathsf{LOCC}^{\rightarrow}}$ equals the maximal bias of correctly distinguishing $\rho$ from $\sigma$ by one-way LOCC, i.e., by a protocol that first measures $A_1$, then, depending on the outcome, measures $A_2$, and so on until $A_N$ has been measured, and that then makes a guess as to which state has been prepared. Classical information is indicated by double lines. Whereas restricting to one-way LOCC measurements in general reduces the power to distinguish quantum states [34–36], we remark that such measurements are still powerful enough to distinguish any two orthogonal pure states [37,38].

$$\|\rho - \sigma\|_{A_1:A_2:\cdots:A_N} \leq \sum_{i=1}^{N-1} \delta(|A_i|, \infty, k_i).$$

Furthermore there exists $\sigma \in \mathcal{S}_{A_1:A_2:\cdots:A_N}$ with

$$\|\rho - \sigma\|_{A_1:A_2:\cdots:A_N} \leq \sum_{i=1}^{N-1} \delta(\infty, |A_{i+1}|, \ell_i),$$

in the case where $(k_1, k_2, \cdots k_{N-1}, 1) := (\ell_1\ell_2\cdots\ell_{N-1}, \ell_2\ell_3\cdots\ell_{N-1}, \cdots, \ell_{N-1}, 1)$.

*Proof.*—For ease of notation we introduce $k_N := 1$ and use $S^{k_N}(A_N) = A_N$. By assumption there exists an extension $\rho_{S^{k_1}(A_1)S^{k_2}(A_2)\cdots S^{k_N}(A_N)}$ of $\rho_{A_1A_2\cdots A_N}$. Since clearly $\rho_{A_1S^{k_2}(A_2)\cdots S^{k_N}(A_N)} \in \mathcal{E}^{k_1,1}_{A_1:S^{k_2}(A_2)\cdots S^{k_N}(A_N)}$ there exists a state $\sigma_{A_1S^{k_2}(A_2)\cdots S^{k_N}(A_N)}$ of the form

$$\sigma_{A_1S^{k_2}(A_2)\cdots S^{k_N}(A_N)} = \sum_{i_1} p_{i_1} \chi^{i_1}_{A_1} \otimes \rho^{i_1}_{S^{k_2}(A_2)\cdots S^{k_N}(A_N)},$$

such that

$$\|\rho - \sigma\|_{A_1:S^{k_2}(A_2)\cdots S^{k_N}(A_N)} \leq \delta(|A_1|, \infty, k_1).$$

We now apply the same reasoning to each of the $\rho^{i_1}_{S^{k_2}(A_2)\cdots S^{k_N}(A_N)}$ and find that there are states

$$\sigma^{i_1}_{A_2S^{k_3}(A_3)\cdots S^{k_N}(A_N)} = \sum_{i_2} p_{i_2|i_1} \chi^{i_1i_2}_{A_2} \otimes \rho^{i_1i_2}_{S^{k_3}(A_3)\cdots S^{k_N}(A_N)}$$

satisfying

$$\|\rho^{i_1} - \sigma^{i_1}\|_{A_2:S^{k_3}(A_3)\cdots S^{k_N}(A_N)} \leq \delta(|A_2|, \infty, k_2).$$

We continue this way until

$$\|\rho^{i_1i_2\cdots i_{N-2}} - \sigma^{i_1i_2\cdots i_{N-2}}\|_{A_{N-1}:S^{k_N}(A_N)} \leq \delta(|A_{N-1}|, \infty, k_{N-1})$$

for

$$\sigma^{i_1i_2\cdots i_{N-2}}_{A_{N-1}S^{k_N}(A_N)} = \sum_{i_{N-1}} p_{i_{N-1}|i_1i_2\cdots i_{N-2}} \chi^{i_1i_2\cdots i_{N-1}}_{A_{N-1}} \otimes \rho^{i_1i_2\cdots i_{N-1}}_{S^{k_N}(A_N)}.$$

We now tensor $\chi^{i_1}_{A_1} \otimes \chi^{i_1i_2}_{A_2} \otimes \cdots \otimes \chi^{i_1i_2\cdots i_j}_{A_j}$ to $\rho^{i_1\cdots i_j}_{A_{j+1}\cdots A_N}$ and denote the state resulting from taking the convex combination with the distribution $p_{i_1\cdots i_{j+1}} := p_{i_1}p_{i_2|i_1}\cdots p_{i_j|i_1\cdots i_{j-1}}$ by $\tau^j$. By the above bounds, the monotonicity under completely positive trace preserving maps, and the triangle inequality we find (for $0 \leq j \leq N-2$ where $\tau^0 := \rho$)

$$\|\tau^j - \tau^{j+1}\|_{A_1\cdots A_{j+1}:A_{j+2}\cdots A_N} \leq \delta(|A_{j+1}|, \infty, k_j). \quad (3)$$

Then we convert all the bounds into the norm $\|*\|_{A_1:A_2:\cdots:A_N}$ using Eq. (2). Finally, we use the triangle inequality in the telescope estimate

$$\|\tau^0 - \tau^{N-1}\|_{A_1:A_2:\cdots:A_N} \leq \sum_{j=0}^{N-2} \|\tau^j - \tau^{j+1}\|_{A_1:A_2:\cdots:A_N},$$

which together with Eq. (3) proves the first bound since $\tau^{N-1}$ is fully separable.

For the second bound note that by assumption there exists an extension $\rho_{S^{k_1}(A_1)S^{k_1}(A_2)\cdots S^{k_{N-1}}(A_{N-1})A_N}$ of $\rho_{A_1A_2\cdots A_N}$. Since clearly $\rho_{B_{N-1}A_N} \in \mathcal{E}^{\ell_{N-1},1}_{B_{N-1}A_N}$, where

$$B_{N-1} := S^{k_1/\ell_{N-1}}(A_1)S^{k_2/\ell_{N-1}}(A_2)\cdots S^{k_{N-2}/\ell_{N-1}}(A_{N-2})A_{N-1},$$

there exists a state

$$\sigma_{B_{N-1}A_N} = \sum_{i_{N-1}} p_{i_{N-1}} \rho^{i_{N-1}}_{B_{N-1}} \otimes \sigma^{i_{N-1}}_{A_N}$$

satisfying

$$\|\rho - \sigma\|_{B_{N-1}:A_N} \leq \delta(\infty, |A_N|, \ell_{N-1}).$$

We then repeat the same argument for the states $\rho^{i_{N-1}}_{B_{N-1}}$ thereby decoupling system $A_{N-1}$ from

$$B_{N-2} := S^{k_1/(\ell_{N-2}\ell_{N-1})}(A_1)S^{k_2/(\ell_{N-2}\ell_{N-1})}(A_2) \cdots S^{k_{N-3}/(\ell_{N-2}\ell_{N-1})}(A_{N-3})A_{N-2}.$$

We continue this way until we have decoupled $A_2$ from $B_1 := A_1$. We then combine all the estimates as we had done in the first proof and obtain the claim. ■

The following corollary is obtained by inserting the trace norm quantum de Finetti theorem from Theorem II.8' of Ref. [17] into the first bound and by inserting the one-way LOCC norm bound from Ref. [22] into the second bound of Theorem 1.

*Corollary 1.*—For all $\rho \in \mathcal{E}^{k_1,\ldots,k_N}_{A_1:A_2:\cdots:A_N}$ there exists $\sigma \in \mathcal{S}_{A_1:A_2:\cdots:A_N}$ with

$$\|\rho - \sigma\|_1 \leq 4 \sum_{i=1}^{N-1} \frac{|A_i|}{k_i}.$$

Furthermore, for all $\rho \in \mathcal{E}^{k_1,\ldots,k_N}_{A_1:A_2:\cdots:A_N}$ there exists $\sigma \in \mathcal{S}_{A_1:A_2:\cdots:A_N}$ with

$$\|\rho - \sigma\|_{\mathrm{LOCC}\to(A_1:A_2:\cdots:A_N)} \leq \frac{1}{8\ln 2} \sum_{i=1}^{N-1} \sqrt{\frac{\log|A_i|}{\ell_i}}.$$

Note that we recover the first part of the statement (Theorem 1 and Ref. [9]) when we let all $k_i$ approach infinity. Examples of extendible states that saturate the two particle bounds used here can be found in Refs. [22,28], respectively. By carefully going through the proof of Theorem 1 one can check that by demanding that $\rho$ satisfy the Peres-Horodecki test, the first bound improves to $O(\sum_{i=1}^{N-1} \frac{|A_i|^2}{k_i^2})$ as Refs. [18,19] can be applied. Similarly one can check that (up to a loss of $\frac{1}{\sqrt{153}}$) the second bound holds for the Frobenius norm due to Ref. [29], even though the Frobenius norm violates Eq. (1).

Whereas the first result on the trace norm may provide a useful characterization of multiparticle separable states that is applicable in a wide variety of situations, the second result on the one-way LOCC norm is more specific, but features an interesting exponential improvement with respect to the dimension dependence. In particular, we will now show that the one-way LOCC norm result implies that detecting multiparticle separability is much more efficient than what was previously anticipated. For this we set $\ell_i := \frac{1}{(8\ln 2)^2}(N-1)^2\epsilon^{-2}\log|A_{i+1}|$. Then we search for an extension to $\otimes_i S^{k_i}(A_i)$ with a semidefinite program. If we find the extension, then we output *separable*, if not, we output *entangled*. This algorithm solves the weak membership problem for separability with error $\varepsilon$ correctly, since by Corollary 1 the one-way LOCC norm distance is bounded by $\varepsilon$ for extendible states. Since every separable state has arbitrary extensions, an output of *entangled* will always be correct. The runtime equals a polynomial in the number of variables, which is smaller than $|A_N||A_{N-1}|^{\ell_{N-1}}\cdots|A_1|^{\ell_1\ell_2\cdots\ell_{N-1}} = \exp\{O[(N-1)^{2N-1}\times \epsilon^{2(N-1)}\prod_{i=1}^N \log|A_i|]\}$ since $|S^k(A)| \leq |A|^k$; the latter is a good bound for large $|A|$, a regime in which we are interested. Since a similar conclusion is true for the Frobenius norm, we obtain the following corollary.

*Corollary 2.*—Deciding separability up to error $\varepsilon$, in the one-way LOCC or Frobenius norm can be done in time $\exp[O(\varepsilon^{-2(N-1)}N^{2N-1}\prod_{i=1}^N \log|A_i|)]$, i.e., in quasipolynomial time for constant error and a constant number of parties.

*Quantum de Finetti theorem.*—A quantum de Finetti theorem is a statement about the approximation of a permutation-invariant state $\rho_{A^k}$, i.e., $[U_\pi, \rho_{A^k}] = 0\ \forall \pi \in S_k$, by convex combinations of identical tensor products $\sigma^{\otimes k}$, so-called de Finetti states [11,13,15–17,30]. Apart from their appeal as remarkable quantum analogues of de Finetti's theorem for exchangeable random variables, quantum de Finetti theorems are important tools in the context of mean-field theory [13], quantum cryptography [30], and complexity theory [31].

Quantum de Finetti theorems have previously been proven for the trace norm, where the best bounds are quadratic in the local dimension. There also is a linear lower bound on the dimension dependence [17] which marks an important difference with classical range-independent de Finetti theorems due to Diaconis and Freedman [32]. Since in many applications the dimension dependence is a crucial bottleneck in the applicability of quantum de Finetti theorems, it could be very interesting if one could beat the linear bound by using a weaker norm. Corollary 1 suggests that the one-way LOCC norm may allow for a logarithmic dimension dependence and it is this result which we will explain in the following. For this, let $\rho_{(A\bar{A})^k}$ be a state supported on the symmetric subspace $S^k(A\bar{A})$ that extends $\rho_{A^k}$ ($\bar{A} \cong A$) (Lemma II.5 of Ref. [17]). By Corollary 1 there exists a separable state $\sigma_{(A\bar{A})^N}$ with

$$\|\rho_{(A\bar{A})^N} - \sigma_{(A\bar{A})^N}\|_{\mathsf{LOCC}^{\rightarrow}(A\bar{A}:\cdots:A\bar{A})} \leq \frac{(N-1)\sqrt{\log|A|^2}}{k^{1/(2N)}}.$$

Now we apply the dimension-independent de Finetti theorem for separable states (Theorem 6 of Ref. [33]) to $\sigma$ and conclude that there exists a de Finetti state $\tau_{(A\bar{A})^n}$ with

$$\|\sigma_{(A\bar{A})^n} - \tau_{(A\bar{A})^n}\|_1 \leq 2\frac{n^2}{N}.$$

Using $\|\star\|_{\mathsf{LOCC}^{\rightarrow}} \leq \|\star\|$ and tracing out the $\bar{A}$ systems we find the following de Finetti type theorem which only depends logarithmically on the local dimension.

*Corollary 3.*—Let $n \leq N \leq k$. For all permutation-invariant states $\rho_{A^k}$ there exists a state $\tau_{A^k} = \sum_i p_i \sigma_{A,i}^{\otimes k}$ with

$$\|\rho_{A^k} - \tau_{A^k}\|_{\mathsf{LOCC}^{\rightarrow}(A:A:\cdots:A)} \leq (N-1)\frac{\sqrt{2\log|A|}}{k^{\frac{1}{2N}}} + 2\frac{n^2}{N}.$$

Whereas arguably $k$ has to be rather large for the bound to be of any use (i.e., it decreases for $N = \sqrt{\log k}$ and large $k$), we feel that this result—by drastically breaking the linear dimension barrier of the trace norm—may find application in theoretical aspects of quantum information theory and provide new insights into the study of quantum de Finetti theorems.

*Conclusion.*—Fast algorithms for deciding the separability of quantum states are important both from a theoretical perspective in quantum information theory and from the point of view of experimental work, where the proof of a successful experiment often lies in the certification of entanglement in the created multiparticle quantum state. In this work we have shown that the detection of multiparticle entanglement can be done much faster than previously anticipated by providing new runtime bounds on the search for symmetric extensions. We hope that this work fosters further theoretical and experimental investigation into the detection of multiparticle entanglement.

F. B. is supported by a "Conhecimento Novo" fellowship from FAPEMIG. M. C. is supported by the Swiss National Science Foundation (Grant No. PP00P2-128455) and the German Science Foundation (Grant No. CH 843/2-1).

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, (IEEE, New York, 1984), pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, arXiv:0912.5537v1.
[5] M. Berta, M. Christandl, and R. Renner, Commun. Math. Phys. **306**, 579 (2011).

[6] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[9] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[10] We say that $\rho_{A^kB}$ extends $\rho_{AB}$ if $\mathrm{tr}_{A^{k-1}}\rho_{A^kB} = \rho_{AB}$.
[11] E. Størmer, J. Funct. Anal. **3**, 48 (1969).
[12] R. L. Hudson and G. R. Moody, Z. Wahrsch. Verw. Geb. **33**, 343 (1976).
[13] G. A. Raggio and R. F. Werner, Helv. Phys. Acta **62**, 980 (1989).
[14] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).
[15] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. (N.Y.) **43**, 4537 (2002); J. Math. Phys. (N.Y.) **49**, 019902 (E) (2008).
[16] R. König and R. Renner, J. Math. Phys. (N.Y.) **46**, 122108 (2005).
[17] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[18] M. Navascués, M. Owari, and M. B. Plenio, Phys. Rev. Lett. **103**, 160404 (2009).
[19] M. Navascués, M. Owari, and M. B. Plenio, Phys. Rev. A **80**, 052306 (2009).
[20] L. Gurvits, J. Comput. Syst. Sci. **69**, 448 (2004).
[21] S. Gharibian, Quantum Inf. Comput. **10**, 343 (2010).
[22] F. G. S. L. Brandão, M. Christandl, and J. Yard, Commun. Math. Phys. **306**, 805 (2011).
[23] F. G. S. L. Brandão, M. Christandl, and J. Yard, in *STOC '11: Proceedings of the 43rd Annual ACM Symposium on Theory of Computing* (ACM, New York, 2011), pp. 343–351; , arXiv:1011.2751.
[24] The algorithm has an error of at most $\varepsilon$ if it identifies all separable states correctly as well as all states that have at least a distance $\varepsilon$ to the set of separable states in the chosen norm.
[25] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).
[26] The uniqueness of the probability measure (second part of Ref. [9], Theorem 1) does not hold in general in this formulation because there exist different decompositions of a separable quantum state. The use of the uniqueness of the quantum de Finetti theorem is for the same reason invalid in the proof of the first part of Ref. [9], Theorem 1, the completeness of the hierarchy.
[27] For a permutation $\pi$ of $k$ elements define $U_\pi$ by $U_\pi|i_1\rangle|i_2\rangle\cdots|i_k\rangle = |i_{\pi^{-1}(1)}\rangle|i_{\pi^{-1}(2)}\rangle\cdots|i_{\pi^{-1}(k)}\rangle$. $S^k(A)$ then equals the vector space consisting of all $|\psi\rangle \in A^{\otimes k}$ that satisfy $U_\pi|\psi\rangle = |\psi\rangle$ for all $\pi$.
[28] M. Christandl, N. Schuch, and A. Winter, Phys. Rev. Lett. **104**, 240405 (2010).
[29] W. Matthews, S. Wehner, and A. Winter, Commun. Math. Phys. **291**, 813 (2009).
[30] R. Renner, Nature Phys. **3**, 645 (2007).
[31] S. Beigi, P. Shor, and J. Watrous, Theory Comput. **7**, 101 (2011).
[32] P. Diaconis and D. Freedman, The Annals of Probability **8**, 745 (1980).
[33] B. Toner and M. Christandl, J. Math. Phys. (N.Y.) **50**, 042104 (2009).
[34] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
[35] D. DiVincenzo, D. Leung, and B. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[36] T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).
[37] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[38] S. Virmani, M. Sacchi, M. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001).