

Measurement-base-independent test for genuine multipartite entanglement

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2013 New J. Phys. 15 073033

(<http://iopscience.iop.org/1367-2630/15/7/073033>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 131.130.87.134

This content was downloaded on 18/01/2017 at 13:19

Please note that [terms and conditions apply](#).

You may also be interested in:

[Macroscopic observables detecting genuine multipartite entanglement and partial inseparability in many-body systems](#)

A. Gabriel and B. C. Hiesmayr

[Quantifying entanglement resources](#)

Christopher Eltschka and Jens Siewert

[Open-system dynamics of entanglement: a key issues review](#)

Leandro Aolita, Fernando de Melo and Luiz Davidovich

[Separability criteria for genuine multipartite entanglement](#)

Otfried Gühne and Michael Seevinck

[Proving the generation of genuine multipartite entanglement in a single-neutron interferometer experiment](#)

Daniel Erdösi, Marcus Huber, Beatrix C Hiesmayr et al.

[Relaxations of separability in multipartite systems: Semidefinite programs, witnesses and volumes](#)

Cécilia Lancien, Otfried Gühne, Ritabrata Sengupta et al.

[Efficient k-separability criteria for mixed multipartite quantum states](#)

Ting Gao, Yan Hong, Yao Lu et al.

[Local hidden-variable models for entangled quantum states](#)

R Augusiak, M Demianowicz and A Acín

[Entanglement in continuous-variable systems: recent advances and current perspectives](#)

Gerardo Adesso and Fabrizio Illuminati

Measurement-base-independent test for genuine multipartite entanglement

Andreas Gabriel¹, Łukasz Rudnicki² and Beatrix C Hiesmayr^{1,3}

¹ University of Vienna, Faculty of Physics, Boltzmanngasse 5, A-1090 Vienna, Austria

² Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, PL-02-668 Warsaw, Poland

E-mail: Beatrix.Hiesmayr@univie.ac.at

New Journal of Physics **15** (2013) 073033 (11pp)

Received 24 January 2013

Published 17 July 2013

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/15/7/073033

Abstract. We investigate *a priori* detection probabilities of genuine multipartite entanglement (GME). Even if one does not have knowledge of the basis in which a state is produced by a source, how a channel decoheres it or of the very working of the detectors used, we find that it is possible to detect GME with reasonably high probability in a feasible fashion. We show that by means of certain separability criteria, GME can be detected in a measurement-base-independent way. Our method provides several applications whenever e.g. state tomography is not possible or too demanding, and is a tool to investigate security issues in multi-particle quantum cryptographical protocols.

³ Author to whom any correspondence should be addressed.



Content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](https://creativecommons.org/licenses/by/3.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Contents

1. Introduction	2
2. Genuine multipartite detection criteria	3
3. Measurement-base-independent test for genuine multipartite entanglement	4
4. Examples	5
4.1. No prior knowledge: $U_\alpha \otimes U_\beta \otimes U_\gamma$	5
4.2. Subsystem symmetry: $U^{\otimes 3}$	6
5. Discussion	7
6. Conclusions	10
Acknowledgments	10
References	10

1. Introduction

Entanglement is one of the most intriguing and most fundamentally nonclassical phenomena in quantum physics. One important type of entanglement—both for research concerning the foundations of quantum theory (see e.g. [1, 2]) and for conceivable technological applications such as quantum computers [3–5] or quantum cryptography schemes [6, 7]—is genuine multipartite entanglement (GME). It is even assumed that entanglement (and, particularly, GME) might play significant roles in nature on all scales, ranging from (comparatively) elementary effects such as phase transitions [8] or frustration [9] in crystals to complex mechanisms in lifeforms, e.g. photosynthesis [10] or even geographical orientation of birds [11]. In more and more physical systems, multipartite and high-dimensional entanglement is observed, e.g. in neutron interferometry [12] or for spatially entangled photons (e.g. [13, 14]).

One of the major tasks in entanglement theory is entanglement detection. Given a quantum state, there are many ways of detecting its different entanglement properties—ranging from generic entanglement detection (see e.g. [15–19]) to more specific forms of entanglement, such as GME (see e.g. [20–22]). However, it is much more difficult to make any statement about entanglement in a not (entirely) known state (see e.g. [23]). The aim of this work is to present a method for detecting GME in partially unknown states that can be interpreted as states from a partially unknown source, or as measuring the states with untrusted measurement equipment. The aim of this work is to present a method for detecting GME in partially unknown states that can be interpreted as states from a partially unknown source, or as measuring the states with untrusted measurement equipment, sketched in figure 1.

This work is organized as follows. In the upcoming section, basic definitions on GME will be reviewed and the separability criteria on which our scheme is based are defined. After that, we present our method of *measurement-base-independent* GME detection, which is the main result of this paper and is thoroughly discussed in the following sections, before the paper is concluded. As a measurement-base-independent detection scheme, we shall understand the method that requires no information about local bases in which the state in question has been prepared. This allows one to set the measurement device independently of the state investigated. However still, some extra knowledge could be required in order to be able to implement the test experimentally. For example, to measure a global quantity via local measurements one needs to use two (or more) different bases and know the relationship between them.

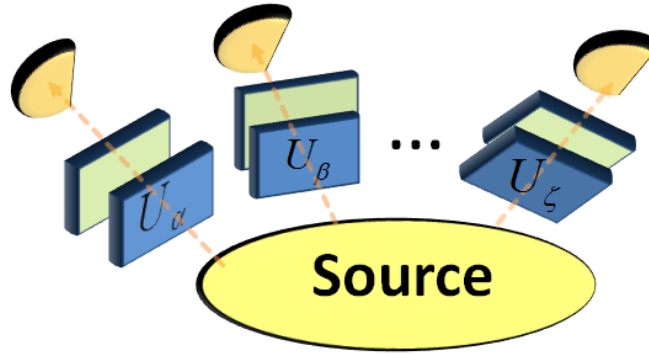


Figure 1. Sketch of our measurement-base-independent test for *a priori* detection probabilities of genuine multipartite entanglement.

2. Genuine multipartite detection criteria

In order to present our results, we need to introduce some basic definitions on multipartite entanglement and its detection first.

A pure multipartite quantum state $|\Psi_2\rangle$ is called biseparable iff it can be written as a nontrivial product: $|\Psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, where the $|\psi_i\rangle$ are states of one or several subsystems. A mixed multipartite state ρ_2 is called biseparable iff it can be written as a mixture of biseparable pure states: $\rho_2 = \sum_i p_i |\Psi_2^i\rangle \langle \Psi_2^i|$, where the $\{p_i\}$ form a probability distribution (i.e. $p_i \geq 0$ and $\sum_i p_i = 1$) and the $|\Psi_2^i\rangle$ may be biseparable under different bipartitions (consequently, the mixed biseparable state is not necessarily separable under a specific bipartition). Any state that is not biseparable is called genuinely multipartite entangled (GME) (figure 1).

Detecting GME in n -partite mixed states can be a rather challenging task, as both biseparable and GME states can be inseparable under all bipartitions and thus hard to distinguish. One way of approaching this problem is by introducing convex detection criteria, which effectively reduce the mixed-state problem to the more simple pure-state problem. A set of such criteria was introduced in [24, 25] via a set of quantities Q_i ($0 \leq i \leq \lfloor \frac{n}{2} \rfloor$) (for a concise summary, consult [26]).

The first criterion for an n -partite state is given by [24]

$$Q_0(\rho) = |\langle 0|^{\otimes n} \rho | 1 \rangle^{\otimes n}| - \sum_{\gamma} \sqrt{\langle 0|^{\otimes n} \langle 1|^{\otimes n} \mathcal{P}_{\gamma A}^{\dagger} \rho^{\otimes 2} \mathcal{P}_{\gamma A} | 0 \rangle^{\otimes n} | 1 \rangle^{\otimes n}}, \quad (1)$$

where the sum runs over all bipartitions $\gamma = \{A, B\}$. The permutation operators $\mathcal{P}_{\gamma A}$ permute the two copies of all subsystems contained in the first part of γ .

A set of other criteria is denoted by [25]

$$Q_m(\rho) = \sum_{\sigma} \left(|\langle d_{\alpha} | \rho | d_{\beta} \rangle| - \sqrt{\langle d_{\alpha} | \langle d_{\beta} | \mathcal{P}_{\alpha}^{\dagger} \rho^{\otimes 2} \mathcal{P}_{\alpha} | d_{\alpha} \rangle | d_{\beta} \rangle} \right) - m(n-m-1) \sum_{\alpha} \langle d_{\alpha} | \rho | d_{\alpha} \rangle, \quad (2)$$

for $1 \leq m \leq \lfloor \frac{n}{2} \rfloor$, where the first sum runs over all sets $\sigma = \{\alpha, \beta\}$ with $\alpha, \beta \subset \{1, 2, \dots, n\}$ such that $|\alpha| = |\beta| = m$ and $|\alpha \cap \beta| = (m-1)$ and, $|d_{\alpha}\rangle$ is the product state vector with $|1\rangle$ in

all subsystems $i \in \alpha$ and $|0\rangle$ otherwise, i.e.

$$|d_\alpha\rangle = \bigotimes_{i \notin \alpha} |0\rangle_i \bigotimes_{i \in \alpha} |1\rangle_i. \quad (3)$$

The permutation operators \mathcal{P}_α permute all subsystems in α with their respective copies in the two copies of ρ .

All these quantities Q_i are, by construction, nonpositive for biseparable states, i.e. any assumed positive value for any ρ implies this ρ to be GME.

As an example, let us consider the Greenberger–Horne–Zeilinger (GHZ)-state for n qubits in the computational basis

$$|\text{GHZ}_n\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \quad (4)$$

and compute the separability criterion Q_0 that yields the maximal value $\frac{1}{2}$ (independently of n), while Q_m is always zero, i.e. does not detect GME. Whereas for a W -state

$$|W_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n \bigotimes_{k \neq i} |0\rangle_k \otimes |1\rangle_i, \\ \text{e.g. } |W_3\rangle = \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle), \quad (5)$$

the criterion $Q_{m=1}$ gives the maximal value 1, but the criterion Q_0 fails to detect GME. In general, the criteria Q_m assume their respective maximal values for the corresponding n -partite Dicke state with m excitations (for more details, consult [26])

$$|D_n^m\rangle = \frac{1}{\sqrt{\binom{n}{m}}} \sum_{\{\beta\}} |d_\beta\rangle, \quad (6)$$

where the set of indices $\{\beta\}$ corresponds to the respective subsystems of excitations and the sum is taken over all inequivalent sets $\{\beta\}$ fulfilling $|\{\beta\}| = m$. In the case of $m = 1$, these states are the W -states.

A characteristic trait of these GME detection criteria is their noninvariance under local unitary transformations, which stems from their formulation via density matrix elements (in contrast to other criteria, which are often based on e.g. eigenvalues). This has the advantage of dramatically reducing the required measurement complexity for their computation and thus experimental feasibility [12], but comes at a price. In order to detect GME in a given state, the basis in which the density matrix elements are computed might need to be adapted to the state in question. We will show, however, that this is surprisingly not necessary in a wide variety of cases.

3. Measurement-base-independent test for genuine multipartite entanglement

Consider the following scenario. A source produces an unknown multipartite state, which is supposed to be GME. The individual parties receiving the particles want to verify the presence of GME without going through the trouble of performing a full quantum state tomography (i.e. by only performing a smaller number of measurements than needed for a state tomography).

Without complete knowledge of the exact state, this problem can, in principle, only be solved with a finite probability $p < 1$, as there is no way to guarantee a choice of observables

yielding a definite answer to the entanglement problem. As the GME detection inequalities Q_i only require small numbers of density matrix elements for computation and have a quite high detection efficiency [24, 25], they offer a good approach to this problem.

By using the Haar measure [27]

$$p_F = \int dU_L |J| \left(\begin{cases} 1 \dots \text{if } F(U_L \cdot \rho \cdot U_L^\dagger) > 0 \\ 0 \dots \text{if } F(U_L \cdot \rho \cdot U_L^\dagger) \leq 0 \end{cases} \right) \quad (7)$$

with e.g. $F(\rho) = Q_i(\rho)$, we obtain the *a priori* probability for the detection criterion Q_i to detect ρ to be GME in a randomly chosen basis, where the integral runs over all local unitary transformations U_L (or, depending on the specific scenario, only a certain subgroup) and $|J|$ is the absolute value of the Jacobi determinant, such that

$$\int dU_L |J| = 1. \quad (8)$$

These integrals can be computed numerically or, in some cases, even analytically (e.g. by means of the composite parameterization from [27]).

If necessary, the detection probability can be increased by combining several Q_i in different measurement bases, i.e. choosing

$$F(\rho) = \max(Q_i(\rho), Q_i(U_x \cdot \rho \cdot U_x^\dagger), Q_j(\rho), \dots), \quad (9)$$

where U_x is e.g. the local unitary rotation to σ_x -eigenstates, i.e. the Hadamard matrix

$$U_x = \left(\begin{array}{cc} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array} \right)^{\otimes n}. \quad (10)$$

Note that the scenario of an unknown state produced by the source is fully equivalent to a known state that is perturbed by the used quantum channels before it can reach the individual parties or the case in which the workings of the detectors are unknown. For the sake of simplicity, in the following we focus for simplicity on the unknown state scenario.

4. Examples

Let us illustrate this approach by means of some simple examples, for which we consider a three-qubit system. Depending on the actual knowledge over the state, the integration in equation (7) may cover different unitary groups. We start with the least favorable case when nothing is known about the local basis in which the state is prepared and proceed with the case when some knowledge about the symmetry is available.

4.1. No prior knowledge: $U_\alpha \otimes U_\beta \otimes U_\gamma$

If there is absolutely no prior knowledge available about the three local bases the state is prepared in, the associated unitary group is $SU(2)^3$. Even in this least favorable case, the probability for detecting GME using a single, randomly guessed measurement basis is surprisingly high. If, for example, the produced state is a GHZ state

$$\rho_U = |\Psi\rangle\langle\Psi| \text{ with } |\Psi\rangle = \frac{U_\alpha \otimes U_\beta \otimes U_\gamma}{\sqrt{2}}(|000\rangle + |111\rangle), \quad (11)$$

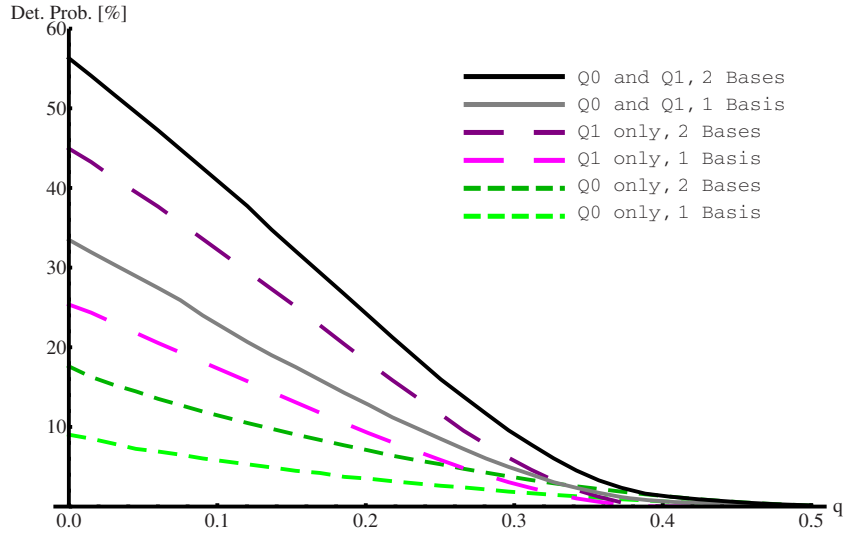


Figure 2. Probability of detecting GME in a GHZ-type isotropic state ($\rho = (1 - q)|\text{GHZ}\rangle\langle\text{GHZ}| + \frac{q}{8}\mathbb{1}$) in a random basis, by means of different separability criteria. The two short-dashed (green) lines correspond to using only Q_0 , the long-dashed (purple) lines to Q_1 and the solid (gray/black) lines to both, where in each case the lower (lighter) line represents measurements in only one basis, while in the upper (darker) line two mutually orthogonal measurement bases are used. Note that for $q = 0.571$ this state becomes biseparable [28].

GME can still be detected in more than 25% of all randomly chosen bases, using only a single separability criterion, namely Q_1 . It is a surprising result here that not the criterion Q_0 , the one designed to detect the GHZ state in the computational basis gives the maximal value. Using Q_0 one detects GME with 18% probability.

If Q_0 and Q_1 are used, as well as a second measurement direction (orthogonal to the first), this ratio increases to more than 56%. Note that this is the highest possible effort using the separability criteria Q_i , as for three qubits there are only two such criteria and only two independent and inequivalent measurement bases. Even if the produced state is not pure, but perturbed by some kind of noise, the detection probability only slowly decreases with the amount of noise, as illustrated in figure 2.

In a similar setup, W -states (5) are detected with only slightly lower efficiency: the corresponding detection probabilities range from 10.7% in the worst case (using only Q_0 in one basis) to 45.9% (for the combination of Q_0 and Q_1 in two mutually orthogonal measurement bases each), as shown in figure 3. Here we do not observe the interchanged roles of the quantities Q_0 and Q_1 .

4.2. Subsystem symmetry: $U^{\otimes 3}$

With the knowledge of the source's output state, the GME detection effectivity increases dramatically. If for example the state is known to be symmetric under particle exchange, only the symmetric subgroup of the group of all local-unitary transformations

$$(SU(2)^3)_{\text{symm}} \cong SU(2) \quad (12)$$

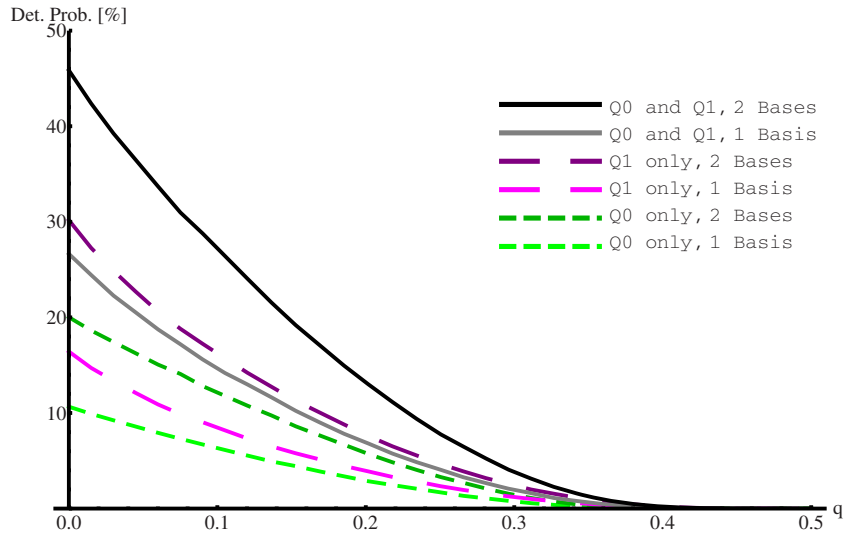


Figure 3. Probability of detecting GME in a W-type isotropic state ($\rho = (1 - q)|W\rangle\langle W| + \frac{q}{8}\mathbb{1}$) in a random basis, by means of different separability criteria. The two short-dashed (green) lines correspond to using only Q_0 , the long-dashed (purple) lines to Q_1 and the solid (gray/black) lines to both, where in each case the lower (lighter) line represents measurements in only one basis, while in the upper (darker) line two mutually orthogonal measurement bases are used. Note that for $q = 0.521$ this state becomes biseparable [28].

has to be integrated over. In this case, the probability of GME detection increases to more than 90%, if both criteria and two measurement bases are used (for both the GHZ- and the W-state). In fact, for the W-state, a detection probability of about 91% can be achieved even using only Q_0 , as illustrated in figure 4.

In cases with a high degree of symmetry, we are even able to obtain analytical expressions for the probabilities in question. For example, for the GHZ-state and only the criterion Q_0 in a single basis, the detection probability computes to (in the following, p_i denotes the probability p_F with $F = Q_i$)

$$p_0 = 1 + \frac{3\sqrt{2}(2K(-\frac{1}{8}) - 3\Pi(-\frac{1}{2}, -\frac{1}{8}))}{2\pi} \approx 0.52966, \quad (13)$$

where $K(x) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-x^2\sin^2(\theta)}}$ is the complete elliptic integral of the first kind and $\Pi(x, y) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{(1-x\sin^2(\theta))\sqrt{1-y^2\sin^2(\theta)}}$ is the complete elliptic integral of the third kind.

5. Discussion

It can be seen from the presented plots (figures 2–4) that the two GME detection criteria (Q_0 and Q_1) in the tripartite case have very different detection behavior. Although Q_0 and Q_1 are specifically designed to detect GHZ- and W-type states, respectively, this is not reflected in the detection probabilities. Instead, Q_0 seems much more suitable for detecting GME in symmetric bases, while Q_1 is much more efficient for nonsymmetric bases. In this context, the two criteria

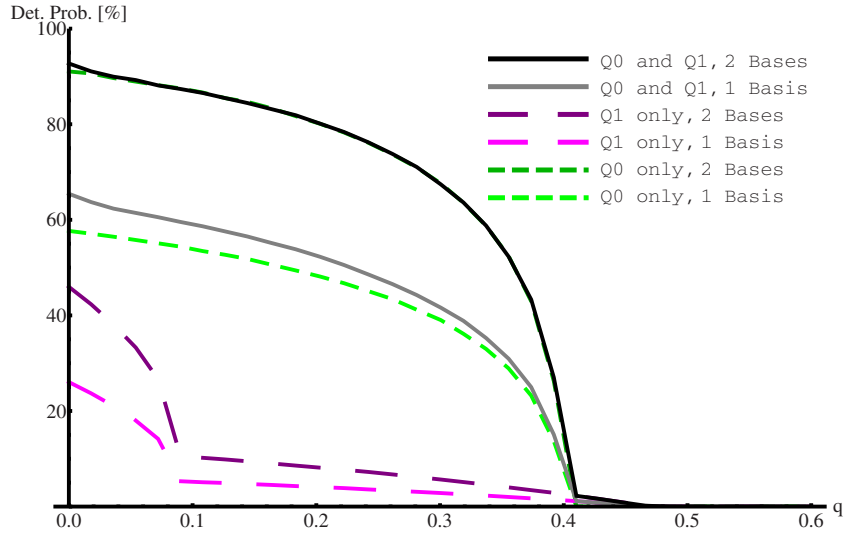


Figure 4. Probability of detecting GME in a W -type isotropic state ($\rho = (1 - q)|W\rangle\langle W| + \frac{q}{8}\mathbb{1}$) in a random symmetric basis, by means of different separability criteria. The two short-dashed (green) lines correspond to using only Q_0 (note that the dark green short-dashed line is mostly below the black one), the long-dashed (purple) lines to Q_1 and the solid (gray/black) lines to both, where in each case the lower (lighter) line represents measurements in only one basis, while in the upper (darker) line two mutually orthogonal measurement bases are used. Note that for $q = 0.521$ this state becomes biseparable [28].

complement each other quite well, such that the combined detection power is highly satisfactory (for both GHZ-type and W -type states).

While all the above results were obtained by numerical methods, the integral (7) can be solved analytically in many cases, even for general numbers n of subsystems (as long as the number of parameters is not too high, i.e. if the degree of symmetry is sufficient). For example, for the n -partite W -state in a symmetric basis, the probability of being detected by Q_1 (using only one basis of measurement) computes to

$$p_1(n) = \frac{1}{n} \left(1 + \sqrt{\frac{n-1}{n-2}} - 2\sqrt{\frac{n-1}{n}} \right), \quad (14)$$

in which case Q_0 yields

$$p_0(n) = \begin{cases} \frac{1}{\sqrt{3}} \approx 57.7\% & \text{for } n = 3, \\ 0 & \text{for } n > 3. \end{cases} \quad (15)$$

Analytic expressions for less symmetric scenarios can often be computed, but as can be recognized from equation (13) are much more cumbersome in general.

It is not surprising that for increasing n individual detection probabilities decrease, as also the number of different types of GME increases (along with the number of detection criteria Q_i). For example, for four qubits there is also the 2-Dicke state (see equation (6))

$$|D_4^2\rangle = \frac{1}{\sqrt{6}} (|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle) \quad (16)$$

and the corresponding detection criterion Q_2 , both of which can straightforwardly be utilized in our base-independent detection scheme. For the 4 qubit 2-Dicke state, the detection probabilities in the symmetric case read

$$\begin{aligned} p_0 &= \frac{1}{\sqrt{3+\sqrt{6}}} \approx 42.8\%, \\ p_1 &= \frac{1}{2}(\sqrt{2}-1) \approx 20.7\%, \\ p_2 &= 1 - \frac{\sqrt{8-2\sqrt{3}}}{3} \approx 29.0\%, \\ p_{012} &= \frac{1}{6} \left(3 + 3\sqrt{2} + 2\sqrt{3(3-\sqrt{6})} - 2\sqrt{4+\sqrt{13}} \right) \approx 71.6\%, \end{aligned} \quad (17)$$

where the p_i are individual detection probabilities using only Q_i , and p_{012} is the detection probability of using Q_0 , Q_1 and Q_2 simultaneously (in a single measurement basis).

An issue of great interest in the context of any device-independent characterization scheme for quantum states is the measurement. The quantities Q_i can be measured comparatively easily, e.g. by decomposing the density-matrix elements into expectation values of Pauli operators (which is particularly efficient for the diagonal elements of the density matrix, as these can all be obtained using only a single measurement setting per used basis).

In particular, for a single neutron propagating through an interferometer the criteria Q_0 and Q_1 were able to prove the generation of genuinely tripartite entangled W -like state families and a GHZ-like state with high fidelity [12]. A single neutron can be entangled in its path-degrees of freedom, its spin-degrees of freedom and its energy-degrees of freedom, thus constituting an effective three-qubit system. In this case, a state tomography is unfeasible for technical reasons (maybe even impossible with today's equipment); thus the criteria, Q_0 and Q_1 , serve as a good experimental test to verify GME. Even if noise was included, the GME between outer and inner degrees of freedom could be witnessed. Our proposed measurement-base-independent test predicts that the detection probabilities would also be high if one was not able to construct a measurement device in the optimal basis choice, but slightly rotated.

Let us also comment on secret sharing protocols. The main idea is to divide a secret into several shares and distribute these shares to n parties such that the secret (or even a part of it) cannot be reconstructed by a subset of parties. Hence, only if all parties work together can the secret be revealed. This scheme was brought to quantum physics in 1999 [29] by exploring the GME of GHZ states. In [7] an experimentally feasible security check was introduced by changing the original protocol and allowing the distributor to choose randomly between the GHZ and a rotated GHZ state. The point is that the unrotated GHZ state maximally violates Q_0 while the rotated GHZ state does not violate Q_0 (in the standard basis). Of course, there exists a $\tilde{Q}_0(\rho) = Q_0(U \cdot \rho \cdot U^\dagger)$ that is maximally violated for the rotated GHZ state while it is not violated for the unrotated one, simply changing the bases. Since an eavesdropper or a dishonest party does not know which state, unrotated or rotated GHZ state, is distributed, there exists no strategy to reveal the secret without being detected (due to the complementary detection properties of the quantities Q_0 and \tilde{Q}_0). Consequently, our proposed base-independent test can be used to analyze the measurement device regarding its reliability probabilistically and, herewith, analyze the security of a given quantum cryptographic protocol.

6. Conclusions

We introduced a method of detecting GME for states in unknown bases, i.e. measurement-base independently. Alternatively, our method applies to the situation when one does not know how a channel decoheres or one has only partial information about the very working of a detector. Measurement-bases independence is achieved by applying certain separability criteria to the (partially unknown) state, which yields decisive results with comparatively high probabilities (which can be increased further by combining several separability criteria and/or several mutually unbiased measurement bases). These probabilities are spread over a wide range of values, depending not only on the actual state but also on the knowledge present about them. Typical values for these probabilities for highly GME states range from several per cent to several tens of per cent.

A rather counter-intuitive result of our work concerns the used GME-criteria Q_i themselves. While Q_0 and Q_1 were designed to detect GME in GHZ- and W -states, respectively, this is not reflected in their *a priori* GME-detection probabilities. Instead, Q_0 seems more suitable for detecting GME in symmetric states (e.g. symmetric bases for either GHZ- or W -states), while Q_1 is more efficient in detecting GME in asymmetric states (such as GHZ- or W -states in random bases).

A possible application of our method are situations where the optimal measurement settings are not available (e.g. due to experimental reasons). In this case, our method allows for an estimation of the probability of success for the setting used.

We also discussed how the criteria used can be experimentally implemented using the fewest possible measurement settings, thus minimizing the experimental complexity. In this way, our scheme can also be understood as an intermediate way of detecting GME: the probability of success increases steadily with the number of used measurements (i.e. the number of used criteria and bases), such that it interpolates between common GME detection criteria and a full quantum state tomography.

Our method may also be applicable to other scenarios, such as analyzing the security of quantum cryptography and secret sharing protocols.

Acknowledgments

We thank Christoph Spengler for his source code for parameterizing unitary groups and the Haar measure. AG gratefully acknowledges the Austrian Research Fund project (FWF-P21947-N16). LR acknowledges the Polish Ministry of Science and Higher Education project no. IP2011 046871. BCH acknowledges gratefully the Austrian Science Fund (FWF-P23627-N16).

References

- [1] Di Domenico A, Gabriel A, Hiesmayr B C, Hipp F, Huber M, Krizek G, Mühlbacher K, Radic S, Spengler Ch and Theussl L 2012 *Found. Phys.* **42** 778
- [2] Hiesmayr B C, Di Domenico A, Curceanu C, Gabriel A, Huber M, Larsson J-A and Moscal P 2012 *Eur. Phys. J. C* **72** 1856
- [3] Jozsa R 2005 arXiv:quant-ph/0508124
- [4] Rossi M, Bruß D and Macchiavello C 2013 *Phys. Rev. A* **87** 022331
- [5] Kampermann H, Gühne O, Wilmott C and Bruß D 2012 *Phys. Rev. A* **86** 032307

- [6] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [7] Schauer S, Huber M and Hiesmayr B C 2010 *Phys. Rev. A* **82** 062311
- [8] de Oliveira T R, Rigolin G and de Oliveira M C 2006 *Phys. Rev. A* **73** 010305
- [9] Giampaolo S M, Gualdi G, Monras A and Illuminati F 2011 *Phys. Rev. Lett.* **107** 260602
- [10] Sarovar M, Ishizaki A, Fleming G R and Whaley K B 2010 *Nature Phys.* **6** 462
- [11] Cai J, Guerreschi G G and Briegel H J 2010 *Phys. Rev. Lett.* **104** 220502
- [12] Erdős D, Huber M, Hiesmayr B C and Hasegawa Y 2013 *New J. Phys.* **15** 023033
- [13] Salakhutdinov V D, Eliel E R and Löffler W 2012 *Phys. Rev. Lett.* **108** 173604
- [14] Löffler W, Euser T G, Eliel E R, Scharrer M, Russell P St. J and Woerdman J P 2011 *Phys. Rev. Lett.* **106** 240505
- [15] Horodecki M, Horodecki P and Horodecki R 1996 *Phys. Lett. A* **223** 1
- [16] Doherty A C, Parrilo P A and Spedalieri F M 2002 *Phys. Rev. Lett.* **88** 187904
- [17] Horodecki M and Horodecki P 1999 *Phys. Rev. A* **59** 4206
- [18] Rudolph O 2000 *J. Phys. A: Math. Gen.* **33** 3951
- [19] Peres A 1996 *Phys. Rev. Lett.* **77** 1413
- [20] Seevinck M and Uffink J 2008 *Phys. Rev. A* **78** 032101
- [21] Gühne O and Seevinck M 2010 *New J. Phys.* **12** 053002
- [22] Gühne O and Toth G 2009 *Phys. Rep.* **474** 1
- [23] Branciard C, Rosset D, Liang Y C and Gisin N 2013 *Phys. Rev. Lett.* **110** 060405
- [24] Huber M, Mintert F, Gabriel A and Hiesmayr B C 2010 *Phys. Rev. Lett.* **104** 210501
- [25] Huber M, Erker P, Schimpf H, Gabriel A and Hiesmayr B C 2011 *Phys. Rev. A* **83** 040301
- [26] Gabriel A 2013 Classification and characterisation of multipartite quantum entanglement *PhD Thesis* Faculty of Physics, University of Vienna arXiv:1305.7401
- [27] Spengler C, Huber M and Hiesmayr B C 2012 *J. Math. Phys.* **53** 013501
- [28] Jungnitsch B, Moroder T and Gühne O 2011 *Phys. Rev. Lett.* **106** 190502
- [29] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829