International Journal of Theoretical Physics, Vol. 42, No. 5, May 2003 (© 2003)

Investigating Three Qubit Entanglement With Local Measurements

Otfried Gühne[1,2] and Philipp Hyllus[1]

Received April 9, 2003

In this paper we describe how three qubit entanglement can be analyzed with local measurements. For this purpose we decompose entanglement witnesses into operators that can be measured locally. Our decompositions are optimized in the number of measurement settings needed for the measurement of one witness. Our method allows to detect true threepartite entanglement and especially GHZ-states with only four measurement settings.

KEY WORDS: entanglement; entanglement witnesses; threepartite systems; local measurements.

1. INTRODUCTION

Entanglement is one of the most puzzling features of quantum theory and of great importance for quantum information theory. It is the resource that makes various quantum protocols possible that perform certain tasks better than it would be possible with purely classical methods (Macchiavello *et al.*, 2000). The investigation and characterization of entanglement with experimental and theoretical methods itself is therefore a task of great importance.

From an experimental point of view it is important to find effective techniques for the production and detection of entanglement. For the detection of entanglement several strategies are known: One can determine the whole density matrix (Thew *et al.*, 2002) and then try to apply one of the necessary or sufficient entanglement criteria, e.g. the PPT criterion (Horodecki *et al.*, 1996; Peres, 1996). One can also look for a violation of Bell inequalities (Werner and Wolf, 2001b). Furthermore, there have been several proposals of detecting entanglement without estimating the whole density matrix (Horodecki, 2001; Horodecki and Ekert, 2002).

However, all these nice ideas have also some disadvantages. Estimating the whole density matrix requires a lot of measurements, and in fact one does not

[1] Institut für Theoretische Physik, Universität Hannover, Hannover, Germany.
[2] To whom correspondence should be addressed at e-mail: guehne@itp.uni-hannover.de.

0020-7748/03/0500-1001/0 © 2003 Plenum Publishing Corporation

need to know the whole matrix in order to check whether it is entangled or not. On the other hand, looking for a violation of Bell inequalities may not suffice for making a decision, since there are entangled states that do not violate any known Bell inequality (Werner and Wolf, 2000, 2001a; Żukowski and Brukner, 2001). It has even been conjectured that entangled states with a positive partial transpose do not violate any Bell inequality at all (Peres, 1999). Finally, the recent proposals of detection require collective measurements on several qubits which makes them hard to implement with the present techniques.

Furthermore, the schemes mentioned above are in some sense too general for many experimental situations. They assume that no a priori information about the state is given. However, in a typical experimental situation one often tries to prepare a certain pure state. Because of imperfections of the experimental apparatus the output state will be a mixture of the desired state and some noise instead. In this case it is desirable to know whether the produced state is still entangled or not.

In Gühne *et al.* (2002a,b), we proposed a general scheme for entanglement detection for the case that some knowledge about the state is given. In this scheme we only want to use local projective measurements, since these measurements can easily be implemented in a lab. In addition, we would like to decrease the number of measurements needed to the minimum, of course.

The scheme relies on the well known concept of witness operators (Horodecki *et al.*, 1996; Terhal, 2000). An hermitean operator W is called a witness operator (or entanglement witness) detecting the entangled state ϱ_e if $Tr(W\varrho_e) < 0$ while $Tr(W\varrho_s) \geq 0$ holds for all separable states ϱ_s. Thus if a measurement yields $Tr(W\varrho) < 0$ then the state ϱ is entangled with certainty. As a consequence of the Hahn-Banach theorem it follows that for every entangied state ϱ_e there exists such an entanglement witness and for many states it is known how to construct such witnesses (Lewenstein *et al.*, 2000). After having constructed the witness, we decompose it into a sum of local measurements, then the expectation value can be measured with simple methods. This decomposition has to be optimized in a certain way since we want to use the smallest number of measurements possible.

Our paper is organized as follows: The first section deals with the decomposition into local measurements because this is the core of our approach. We define there what we understand by an optimized decomposition. We would like to remark here that finding optimized decompositions is in general a hard task, much harder than constructing entanglement witnesses. In the second section we illustrate our approach with an example of a two qubit system. We construct the witness and determine its optimal decomposition. Finally in the third and main part we apply this idea to three qubit systems. We explain how GHZ-type and W-type entanglement can be detected with local measurements. We also determine the minimal number of measurements needed for this.

2. LOCAL DECOMPOSITIONS

Assume that we have an hermitean operator H acting on a tensor product $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots \otimes \mathcal{H}_Z$ of two or more finite dimensional Hilbert spaces. To slenderize the notation we look here at the case that we have a bipartite $N \times N$-system: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with dim $(\mathcal{H}_A) = \dim(\mathcal{H}_B) = N$. But all definitions in this section can be extended to more parties in an obvious manner. To measure the expectation value of this operator locally, we have to decompose it in a sum of tensor products of operators acting on only one system, or, equivalently, we have to decompose it into a sum of projectors onto product vectors:

$$H = \sum_{i=1}^{m} A_i \otimes B_i = \sum_{i=1}^{n} c_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|. \tag{1}$$

By measuring the expectation value of the projectors $|e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|$ and adding the results with the weights c_i this decomposition (1) can be measured locally. There are, of course, many possibilities of finding a decomposition like (1). So we have to optimize the decomposition in a certain sense. But there are even several possibilities of defining an optimized decomposition.

On the first sight one might try to minimize the number of product vectors corresponding to minimizing n in (1). This optimization procedure is already known from the literature, it was considered in Sanpera *et al.* (1998). There it was shown that for a general operator acting on two qubits one needs five product vectors and also a constructive way of computing these product vectors was given.

However, since we want to construct an experimentally accessible scheme for entanglement detection it is natural to look for a decomposition where Alice and Bob have to perform the smallest number of measurements possible. By "measurements" we understand here von Neumann (or projective) measurements, since they can be easily implemented. Such a measurement for Alice corresponds to a choice of an orthonormal basis of $\mathcal{H}_A$, and Bob has to choose an orthonormal basis $\mathcal{H}_B$, too. So any operator of the form

$$M = \sum_{k,l=1}^{N} c_{kl} |e_k\rangle\langle e_k| \otimes |f_l\rangle\langle f_l| \tag{2}$$

with $\langle e_s|e_t\rangle = \langle f_s|f_t\rangle = \delta_{st}$ can be measured with only one collective setting of measurement devices of Alice and Bob. Alice and Bob can distinguish the states $|e_k f_l\rangle$, measure the probabilities of these states and add their results with the weights c_{kl} to measure M. We call an operator which can be measured with one measurement setting (like M in Eq. (2)) a *local von Neumann measurement* (LvNM).

Having understood what can be realized with one measurement setting, we can state another optimization strategy. We want to find a decomposition of the form

$$H = \sum_{i=1}^{K} \sum_{k,l=1}^{N} c_{kl}^{i} |e_k^i\rangle\langle e_k^i| \otimes |f_l^i\rangle\langle f_l^i| \tag{3}$$

with $\langle e_s^i \mid e_t^i \rangle = \langle f_s^i \mid f_t^i \rangle = \delta_{st}$ and a minimal K. This K is the number of collective measurement settings Alice and Bob have to use in order to measure H. This optimization strategy is the aim we are considering in this paper when we talk about "optimized" decompositions.

The reader should note that minimizing m in (1) is not the same as our optimization strategy. However, for systems of dimension N greater than 2 it might be more suitable to decompose the witness as $W = \sum_i^m A_i \otimes B_i$. As shown in (Horodecki, 2002), the expectation values of operators A_i or B_i can be measured by a POVM with a single qubit as ancilla instead of counting clicks for all possible N outcomes of the operator. Also minimizing the number of product vectors (i.e. minimizing n in (1)) is not the same. This will become clear in a few seconds, when we study two qubits.

3. TWO QUBITS

We illustrate the method by considering an experiment that aims at producing a certain 2-qubit state $|\Psi\rangle = a|01\rangle + b|10\rangle$ written in the Schmidt decomposition, i.e. $a, b \geq 0, a^2 + b^2 = 1$. Because of imperfections, the produced state will rather be

$$\varrho_{p,d} = p|\Psi\rangle\langle\Psi| + (1-p)\sigma, \tag{4}$$

where we assume that the noise state σ lies inside a separable ball of radius d around the totally mixed state, i.e. $\|\sigma - \mathbb{1}/4\| \leq d$ for some norm. Our aim is to provide a local experimental method to tell whether the produced state is entangled or not, based on witness operators.

Since we only want to explain our basic idea, we assume here that we have white noise, this means $d = 0$. The case $d > 0$ is studied in greater detail in (Gühne *et al.*, 2002b). We would like to stress that our assumption $d = 0$ is in some sense artificial. By this we mean that if $d = 0$ there is a simple way of determining whether ϱ_p, 0 is entangled or not: One can just measure *any* operator A (which fulfills $Tr(A) \neq 4Tr(A|\Psi\rangle\langle\Psi|)$) and compute p from the expectation value of this operator. With this information the density matrix $\varrho_{p,0}$ can be constructed and the PPT criterion can be used to decide whether it is entangled or not. This is not possible for obvious reasons if $d > 0$.

To reach our goal we first have to construct a proper entanglement witness. For NPPT entangled states, i.e. entangled states with a nonpositive partial transpose, the construction of a witness is relatively easy: The partial transpose of a projector onto an eigenvector of ϱ^{T_B} with negative eigenvalue does the job. Here T_B denotes the partial transposition with respect to subsystem B.

The state $\varrho_{p,0}$ has one possible negative eigenvalue, namely $\lambda_{-} = (1-p)/4 - abp$, with the corresponding eigenvector

$$|\psi_{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{5}$$

that is independent of a and p. Then $W_0 = |\psi_{-}\rangle\langle\psi_{-}|^{T_B}$ is an entanglement witness detecting $\varrho_{p,0}$ since

$$Tr((|\psi_{-}\rangle\langle\psi_{-}|^{T_B})\varrho_{p,0}) = Tr\left(|\psi_{-}\rangle\langle\psi_{-}|\left(\varrho_{p,0}^{T_B}\right)\right) = \lambda_{-} < 0. \tag{6}$$

Having constructed the witness, all that remains is to decompose it. Defining $|z^{\pm}\rangle = |0,1\rangle$, $|x^{\pm}\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|y^{\pm}\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$ we can decompose the more general witness $|\phi\rangle\langle\phi|^{T_B}$ for $|\phi\rangle = \alpha|00\rangle + \beta|11\rangle$ as follows:

$$\begin{aligned}|\phi\rangle\langle\phi|^{T_B} &= \alpha^2|00\rangle\langle 00| + \beta^2|11\rangle\langle 11| + \alpha\beta(|01\rangle\langle 10|) + |10\rangle\langle 01|) \\ &= \alpha^2|z^+z^+\rangle\langle z^+z^+| + \beta^2|z^-z^-\rangle\langle z^-z^-| + \alpha\beta(|x^+x^+\rangle\langle x^+x^+| \\ &\quad + |x^-x^-\rangle\langle x^-x^-| - |y^+y^-\rangle\langle y^+y^-| - |y^-y^+\rangle\langle y^-y^+|) \\ &= \frac{1}{4}(\mathbb{1}\otimes\mathbb{1} + \sigma_z\otimes\sigma_z + (\alpha^2-\beta^2)(\sigma_z\otimes\mathbb{1} + \mathbb{1}\otimes\sigma_z) \\ &\quad + 2\alpha\beta(\sigma_x\otimes\sigma_x + \sigma_y\otimes\sigma_y)),\end{aligned} \tag{7}$$

where the σ_i are the Pauli matrices. This way of decomposing a witness can be used for higher dimensions and for systems of more than two parties by using

$$\begin{aligned}|01\rangle\langle 10| + |10\rangle\langle 01| = |x^+x^+\rangle\langle x^+x^+| + |x^-x^-\rangle\langle x^-x^-| \\ - |y^+y^-\rangle\langle y^+y^-| - |y^-y^+\rangle\langle y^-y^+|.\end{aligned} \tag{8}$$

The local measurement of the general witness of Eq. (7) requires three measurements of Alice and of Bob in the $x, y,$ and z direction. This is also true for the special case $\alpha = -\beta = 1/\sqrt{2}$ corresponding to W_0. It is not possible to evaluate the witness with less than three LvNMs:

Proposition 3.1. *The witness W_0 can not be decomposed into less than three LvNMs, therefore the decomposition (7) is optimal.*

Proof: The proof was first given in (Gühne *et al.*, 2002a), we repeat it here because we extend it later to three qubit systems. Consider a decomposition requiring two measurements:

$$|\psi\rangle\langle\psi|^{T_B} = \sum_{i,j=0}^{1} c_{ij}^1|A_i^1\rangle\langle A_i^1| \otimes |B_j^1\rangle\langle B_j^1| + \sum_{i,j=0}^{1} c_{ij}^2|A_i^2\rangle\langle A_i^2| \otimes |B_j^2\rangle\langle B_j^2|, \tag{9}$$

where $\{|A_i\rangle\}$ and $\{|B_i\rangle\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. With the help of a Schmidt decomposition as above we can write $|\psi\rangle\langle\psi|^{T_B} = \sum_{i,j=0}^{3} \lambda_{ij}\sigma_i \otimes \sigma_j$ with

$$(\lambda_{ij}) = \begin{pmatrix} \frac{1}{4} & 0 & 0 & \frac{\alpha^2-\beta^2}{4} \\ 0 & \frac{\alpha\beta}{2} & 0 & 0 \\ 0 & 0 & \frac{\alpha\beta}{2} & 0 \\ \frac{\alpha^2-\beta^2}{4} & 0 & 0 & \frac{1}{4} \end{pmatrix}. \tag{10}$$

Note that the 3×3 submatrix in the right bottom corner is of rank 3. Now we write any projector on the rhs of (9) as a vector in the Bloch sphere: $|A_0^1\rangle\langle A_0^1| = \sum_{i=0}^{3} s_i^A \sigma_i$ is represented by the vector $s^{A_0^1} = (1/2, s_1^A, s_2^A, s_3^A)$ and $|A_1^1\rangle\langle A_1^1|$ by $s^{A_1^1} = (1/2, -s_1^A, -s_2^A, -s_3^A)$; $|B_0^1\rangle\langle B_0^1|$ can be written similarly. If we expand the first sum on the rhs of (9) in the $(\sigma_i \otimes \sigma_j)$ basis, the 3×3 submatrix in the right bottom corner is given by $(c_{00}^1 - c_{01}^1 - c_{10}^1 + c_{11}^1)(s_1^A, s_2^A, s_3^A)^T(s_1^B, s_2^B, s_3^B)$. This matrix is of rank 1. The corresponding submatrix from the second LvNM on the rhs of (9) is also of rank 1 and we arrive at a contradiction: No matrix of rank 3 can be written as a sum of two matrices of rank 1. □

Note that the decomposition (7) requires six projectors onto product vectors (PPV). By applying the method of Sanpera *et al.* (1998) it is possible to decompose the witness using only five PPVs

$$|\psi\rangle\langle\psi|^{T_B} = \frac{(\alpha+\beta)^2}{3} \sum_{i=1}^{3} |A_i' A_i'\rangle\langle A_i' A_i'| - \alpha\beta(|01\rangle\langle 01| + |10\rangle\langle 10|), \tag{11}$$

where we have used the definitions

$$\begin{aligned} |A_1'\rangle &= e^{i\frac{\pi}{3}} \cos(\theta)|0\rangle + e^{-i\frac{\pi}{3}} \sin(\theta)|1\rangle \\ |A_2'\rangle &= e^{-i\frac{\pi}{3}} \cos(\theta)|0\rangle + e^{i\frac{\pi}{3}} \sin(\theta)|1\rangle \qquad (12) \\ |A_2'\rangle &= |A_1'\rangle + |A_2'\rangle \\ \cos(\theta) &= \sqrt{\alpha/(\alpha+\beta)} \\ \sin(\theta) &= \sqrt{\beta/(\alpha+\beta)}. \qquad (13) \end{aligned}$$

However, with this decomposition the measurement of the witness would require four local correlated measurement settings, hence the two optimization strategies are really different.

4. THREE QUBITS

The state space for three qubits has a much richer structure concerning entanglement than the space of two qubits. Let us briefly remind the reader of some well known facts about three qubits. We first consider pure states. There are two classes of states that are not genuine threepartite entangled: The fully separable states, which can be written as

$$|\phi_{fs}\rangle_{ABC} = |\alpha\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C, \tag{14}$$

and the biseparable states which can be written as a product state in the bipartite system, which is created, if two of the three qubits are grouped together to one party. One example is

$$|\phi_{bs}\rangle_{A-BC} = |\alpha\rangle_A \otimes |\delta\rangle_{BC}. \tag{15}$$

There are three possibilities of grouping two qubits together, hence there are three classes of biseparable states. The genuine threepartite entangled states are the states that are neither fully separable nor biseparable. Given two threepartite states, $|\phi\rangle$ and $|\psi\rangle$, one can ask whether it is possible to transform $|\phi\rangle$ into $|\psi\rangle$ with local operations and classical communication, without requiring that this can be done with probability 1. These operations are called stochastic local operations and classical communication (SLOCC). It turns out (Dür *et al.*, 2000) that $|\phi\rangle$ can be transformed into $|\psi\rangle$ iff there exist operators A, B, C, acting on the space of one qubit with

$$|\psi\rangle = A \otimes B \otimes C|\phi\rangle. \tag{16}$$

Surprisingly, it was proven in (Dür *et al.*, 2000) that there are two classes of genuine threepartite entangled states that cannot be transformed into another by SLOCC. One class, the class of GHZ-states can be transformed by SLOCC into

$$|GHZ\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle), \tag{17}$$

the other class, the class of W-states can be converted into

$$|W\rangle = 1/\sqrt{3}(|100\rangle + |010\rangle + |001\rangle. \tag{18}$$

Now we can classify the mixed states according to Acín *et al.* (2001). We define a mixed state ϱ as fully separable if ϱ can be written as a convex combination of fully separable pure states. A state ϱ that is not fully separable is called biseparable if it can be written as a convex combination of biseparable pure states. One can, of course, define three classes of biseparable mixed states with respect of one of the three partitions as well. Finally, ϱ is fully entangled if it is neither biseparable nor fully separable. There are again two classes of fully entangled mixed states, the W-class and the GHZ-class. The state ϱ belongs to the W-class, if it can be written as a convex combination of pure W- states, and to the GHZ-class

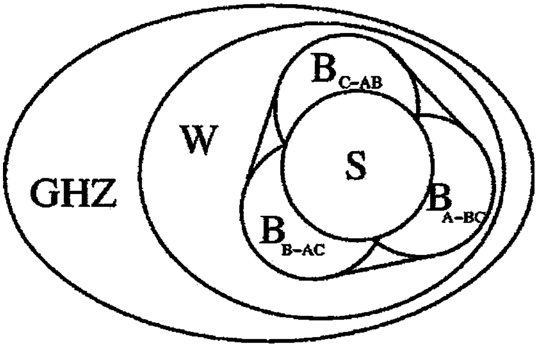

Fig. 1. The structure of the set of three qubit states: They can be (S)eparable, (B)iseparable, (W)-entangled, or (GHZ)-entangled.

otherwise. Taking into account that the set of all states is also a convex set, one obtains an "onion"-structure. This structure is shown in Fig. 1.

In the same reference also witnesses for the detection of GHZ-type and W-type states have been constructed. Here a want to compute the optimized decompositions of these operators.

For the GHZ-class a witness operator is given by

$$W_{GHZ} = \frac{3}{4}\mathbb{1} - |GHZ\rangle\langle GHZ|. \tag{19}$$

If ϱ is a mixed state with $Tr(\varrho W_{GHZ}) < 0$ the state ϱ belongs to the GHZ-class. A decomposition of W_{GHZ} can be computed with similar methods as for the two qubit case, it yields

$$\begin{aligned} W_{GHZ} = \frac{1}{8}(&5 \cdot \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} - \mathbb{1} \otimes \sigma_z \otimes \sigma_z - \sigma_z \otimes \mathbb{1} \otimes \sigma_z - \sigma_z \otimes \sigma_z \otimes \mathbb{1} \\ &- 2 \cdot \sigma_x \otimes \sigma_x \otimes \sigma_x + 1/2 \cdot (\sigma_x + \sigma_y) \otimes (\sigma_x + \sigma_x) \otimes (\sigma_x + \sigma_y) \\ &+ 1/2 \cdot (\sigma_x - \sigma_y) \otimes (\sigma_x - \sigma_y) \otimes (\sigma_x - \sigma_y)). \end{aligned} \tag{20}$$

This witness can be measured with four collective measurment settings. Now we have to show that this decomposition is optimal.

Proposition 4.2. *The witness (19) cannot be measured with three LvNMs, i.e. the decomposition (20) is optimal.*

Proof: The proof is an extension of the two qubit case. First, we write the witness in the $\sigma_i \otimes \sigma_j \otimes \sigma_k$ basis: $W_{GHZ} = 1/8 \sum_{i,j,k=0}^{3} \lambda_{ijk} \sigma_i \otimes \sigma_j \otimes \sigma_k$, and from (20) we obtain:

$$\lambda_{ij0} = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} =: A^{(0)} \qquad \lambda_{ij1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} =: A^{(1)}$$

$$\lambda_{ij2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} =: A^{(2)} \qquad \lambda_{ij3} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} =: A^{(3)}.$$

We denote by $A^{(\nu),\text{red}}$ the reduced 3×3 matrices that appear when the first row and the first column of $A^{(\nu)}$ is dropped: $(A^{(\nu),\text{red}})_{i,j} := (A^{(\nu)})_{i,j=1,..,3}$. In the same sense one can define a reduced tensor $(\lambda^{\text{red}}_{ijk})_{i,j,k} := (\lambda_{ijk})_{i,j,k} = 1,..,3$.

Let us now investigate what can be achieved with one measurement setting. One measurement setting is of the form

$$\begin{aligned} M &= \sum_{r,s,t=0}^{1} c_{rst} |A_r\rangle\langle A_r| \otimes |B_s\rangle\langle B_s| \otimes |C_t\rangle\langle C_t| \\ &= \sum_{i,j,k=0}^{3} \mu_{ijk} \sigma_i \otimes \sigma_j \otimes \sigma_k, \end{aligned} \tag{21}$$

Defining s^A as the Bloch vector of $|A_0\rangle\langle A_0|$ (and similarly s^B and s^C for $|B_0\rangle\langle B_0|$ and $|C_0\rangle\langle C_0|$ and using the same argumentation as in the two qubit case, it is easy to see that the reduced $3 \times 3 \times 3$ tensor μ^{red}_{ijk} is given by

$$\mu^{\text{red}}_{ijk} = \sum_{r,s,t=0}^{1} c_{rst} (-1)^{r+s+t} s^A_i s^B_j s^C_k. \tag{22}$$

Therefore for all k the matrices $(\mu^{\text{red}}_{ijk})_{i,j}$ are of rank 1.

In order to show that W_{GHZ} cannot be measured with three measurement settings, it suffices to show that it is not possible to find three 3×3 matrices B_i, $i \in \{0, \ldots, 2\}$ of rank 1 such that $A^{(0),\text{red}}$, $A^{(1),\text{red}}$ and $A^{(2),\text{red}}$ can be represented as linear combinations of the B_i. Let us assume the contrary, i.e. that we have three B_i. Since the $A^{(i),\text{red}}$ span a three-dimensional subspace in the space of all 3×3 matrices, the B_i have to be linear independent (as matrices) and have to span the same space. That would imply that any of the B_i could be written as a linear combination of the $A^{(i),\text{red}}$. But a general linear combination of the $A^{(i),\text{red}}$ is of the form:

$$\mathcal{A} = \begin{pmatrix} -\alpha & \beta & 0 \\ \beta & \alpha & 0 \\ 0 & 0 & \gamma \end{pmatrix} \tag{23}$$

This is of rank 1 if and only if $\alpha = \beta = 0$. Thus, we arrive at a contradiction, the B_i cannot be of rank 1 and linear independent. □

For the investigation of W-states two witnesses were constructed in Acín *et al.* (2001). The first one is given by

$$\mathcal{W}_{W1} = \frac{2}{3}\mathbb{1} - |W\rangle\langle W|, \tag{24}$$

This witness detects states belonging to the W-class and the GHZ-class, i.e. its expectation value is positive on all biseparable and fully separable states. The optimized decomposition is given by

$$\begin{aligned}
\mathcal{W}_{W1} = \frac{1}{24}(&17 \cdot \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} + 7 \cdot \sigma_z \otimes \sigma_z \otimes \sigma_z \\
&+ 3 \cdot \sigma_z \otimes \mathbb{1} \otimes \mathbb{1} + 3 \cdot \mathbb{1} \otimes \sigma_z \otimes \mathbb{1} + 3 \cdot \mathbb{1} \otimes \mathbb{1} \otimes \sigma_z \\
&+ 5 \cdot \sigma_z \otimes \sigma_z \otimes \mathbb{1} + 5 \cdot \sigma_z \otimes \mathbb{1} \otimes \sigma_z + 5 \cdot \mathbb{1} \otimes \sigma_z \otimes \sigma_z \\
&- (\mathbb{1} + \sigma_z + \sigma_x) \otimes (\mathbb{1} + \sigma_z + \sigma_x) \otimes (\mathbb{1} + \sigma_z + \sigma_x) \\
&- (\mathbb{1} + \sigma_z - \sigma_x) \otimes (\mathbb{1} + \sigma_z - \sigma_x) \otimes (\mathbb{1} + \sigma_z - \sigma_x) \\
&- (\mathbb{1} + \sigma_z + \sigma_y) \otimes (\mathbb{1} + \sigma_z + \sigma_y) \otimes (\mathbb{1} + \sigma_z + \sigma_y) \\
&-(\mathbb{1} + \sigma_z - \sigma_y) \otimes (\mathbb{1} + \sigma_z - \sigma_y) \otimes (\mathbb{1} + \sigma_z - \sigma_y)).
\end{aligned} \tag{25}$$

Here, only five correlated measurement settings are necessary. This decomposition is also optimal:

Proposition 4.3. *The witness $\mathcal{W}_{W1}$ cannot be measured with four measurement settings, i.e. the decomposition (25) is optimal.*

Proof: The strategy of the proof is the same as for the proof of Proposition 2, so we can make it short. First one computes $\mathcal{W}_{W1} = 1/8 \sum_{i,j,k=0}^{3} \lambda_{ijk} \sigma_i \otimes \sigma_j \otimes \sigma_k$, and the corresponding $A^{(i),\text{red}}$, $i \in 0, .., 3$. This time, it turns out that they span a four-dimensional space.

Again, it suffices to show that we cannot find four matrices B_i, $i \in \{0, \ldots, 3\}$ of rank 1 such that $A^{(0),\text{red}}$, $A^{(1),\text{red}}$, $A^{(2),\text{red}}$, and $A^{(3),\text{red}}$ can be represented as linear combinations of the B_i. Here, the assumption that we have four B_i fails due to similar reasons as above: As above, the B_i have to be linear independent and it has to be possible to write any of the B_i as a linear combination of the $A^{(i),\text{red}}$. A general linear combination of the $A^{(i),\text{red}}$, is now of the form

$$\mathcal{A} = \begin{pmatrix} \alpha & 0 & \beta \\ 0 & \alpha & \gamma \\ \beta & \gamma & \delta \end{pmatrix}, \tag{26}$$

and this is of rank 1 if and only if $\alpha = \beta = \gamma = 0$, hence we arrive at a contradiction. □

The second witness for W-class states is given by

$$W_{W2} = \frac{1}{2}\mathbb{1} - |GHZ\rangle\langle GHZ|. \tag{27}$$

This witness can be measured locally with the same decomposition as (20) substracted by $\mathbb{1}/4$. If $-1/4 \leq Tr(W_{W2\varrho}) \leq 0$, ϱ is threepartite entangled, it is either a W-state or a GHZ-state. If $Tr(W_{W2\varrho}) \leq -1/4$, ϱ is a GHZ-state. It also can serve for the detection of states of the type $(\mathbb{1} - p)1/8 + p|W\rangle\langle W|$, this is explained in Acín *et al.* (2001).

Let us conclude this section with a remark about the relationship between convertability under SLOCC and the number of LvNMs needed for a local measurement. One may interpret our results for two qubits in the following way: A projector $|\phi\rangle\langle\phi|$ can be measured with one or three LvNMs, depending on whether it is a product state or not. These two classes coincide with the two inequivalent (under SLOCC) classes for two qubits (Dür *et al.*, 2000). One may think that SLOCC and LvNM are in this way related. Even our results in Gühne *et al.* (2002b), which state that the number of LvNMs needed strongly depends on the Schmidt rank of $|\phi\rangle$ for $N \times N$-systems may support this conjecture, since for bipartite systems the Schmidt rank classifies inconvertible sets under SLOCC. But our work on three qubits suggests that this coincidence is just by chance. For a general state $|\psi_{GHZ}\rangle$ of the GHZ-class there always exists an orthonormal product basis in which it can be written as

$$|\psi_{GHZ}\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle \tag{28}$$

and for a general W-state $|\psi_W\rangle$ there exists the same description, but with $\lambda_4 = \theta = 0$ (Acín *et al.*, 2000). If one has an optimized decomposition of a general $|\psi_{GHZ}\rangle\langle\psi_{GHZ}|$ it should be possible to derive a decomposition of $|\psi_W\rangle\langle\psi_W|$ by setting $\lambda_4 = \theta = 0$, this decomposition would need less or the same number of LvNMs. In the other direction, this means that for a general $|\psi_W\rangle$ there exists a $|\psi_{GHZ}\rangle$ which needs at least the same number of LvNMs for a local measurement. But as we have shown for $|W\rangle$ there also exists a GHZ-state (namely $|GHZ\rangle$) that needs less LvNMs. Hence, the relation between SLOCC and LvNM seems not to be so simple, if there is a relation at all.

5. CONCLUSION

We have studied how three qubit entanglement can be investigated with local measurements. For this purpose we decomposed already known entanglement witnesses into local measurements. We have shown that these decompositions are optimal. By this, we have shown that four measurement settings suffice for the detection of true threepartite entanglement and especially GHZ-type entanglement.

ACKNOWLEDGMENTS

We thank Dagmar Bruß, Artur Ekert, Maciej Lewenstein, Chiara Macchiavello, and Anna Sanpera for helpful discussions. O.G. thanks Ofer Biham and Karol Życzkowski for the discussions in Ustroń, the organizers for their work, and last but not least for their financial support. This work has further been supported by the DFG (Graduiertenkolleg 282 and Schwerpunkt "Quanteninformationsverarbeitung").

REFERENCES

Acín, A., Andrianov, A., Costa, L., Jane, E., Latorre, J., and Tarrach, R. (2000). Generalized Schmidt decomposition and classification of three-quantum-bit states. *Physical Review Letters* **85**, 1560. *Preprint* quant-ph/0003050.

Acín, A., Bruß, D., Lewenstein, M., and Sanpera, A. (2001). Classification of mixed three-qubit states. *Physical Review Letters* **87**, 040401.

Dür, W., Vidal, G., and Cirac, J. (2000). Three qubits can be entangled in two inequivalent ways. *Physical Review A* **62**, 062314. *Preprint* quant-ph/0005115.

Gühne, O., Hyllus, P., Bruß, D., Ekert, A., Lewenstein, M., Macchiavello, C., and Sanpera, A. (2002a). Detection of entanglement with few local measurements. *Physical Review A* **66**, 062305. *Preprint* quant-ph/0205089.

Gühne, O., Hyllus, P., Bruß, D., Ekert, A., Lewenstein, M., Macchiavello, C., and Sanpera, A. (2002b). Experimental detection of entanglement via witness operators and local measurements. *Preprint* quant-ph/0210134, to be published in a special issue of Journal of Modern Optics.

Horodecki, P. (2001). Measuring quantum entanglement without prior state reconstruction. *Preprint* quant-ph/0111082.

Horodecki, P. (2002). Mean of continuous variables observable via measurement on single qubit. *Preprint* quant-ph/0210163.

Horodecki, P. and Ekert, A. (2002). Method for direct detection of quantum entanglement. *Physical Review Letters* **89**, 127902. *Preprint* quant-ph/0111064.

Horodecki, M., Horodecki, P., and Horodecki, R. (1996). Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A* **232**, 1.

Lewenstein, M., Kraus, B., Cirac, J., and Horodecki, P. (2000). Optimization of entanglement witnesses. *Physical Review A* **62**, 052310.

Macchiavello, C., Palma, G., and Zeilinger, A. (eds.) (2000). *Quantum Computation and Quantum Information Theory*, World Scientific, Singapore.

Peres, A. (1996). Separability criterion for density matrices. *Physical Review Letters* **77**, 1413.

Peres, A. (1999). All the Bell inequalities. *Foundations of Physics* **29**, 589.

Sanpera, A., Tarrach, R., and Vidal, G. (1998). Local description of quantum inseparability. *Physical Review A* **58**, 826.

Terhal, B. (2000). Bell inequalities and the separability criterion. *Physics Letters A* **271**, 319.

Thew, R., Nemoto, K., White, A., and Munro, W. (2002). Qudit quantum-state tomorgraphy. *Physical Review A* **66**, 012303.

Werner, R. and Wolf, M. (2000). Bell's inequalities for states with positive partial transpose. *Physical Review A* **61**, 062102. *Preprint* quant-ph/9910063.

Werner, R. and Wolf, M. (2001a). All multipartite Beil-correlation inequalities for two dichotomic observables per site. *Physical Review A* **64**, 032112. *Preprint* quant-ph/0102024.

Werner, R. and Wolf, M. (2001b). Bell inequalities and entanglement. *Quantum Information and Computation Journal* **1**, 1. *Preprint* quant-ph/0107093.

Zukowski, M. and Brukner, C. (2001). Bell's theorem and general N-qubit states. *Physical Review Letters* **88**, 210401. *Preprint* quant-ph/0102039.