

## Entanglement detection in the stabilizer formalism

Géza Tóth<sup>1,\*</sup> and Otfried Gühne<sup>2,†</sup>

<sup>1</sup>*Theoretical Division, Max Planck Institute for Quantum Optics, Hans-Kopfermann-Strasse 1, D-85748 Garching, Germany*

<sup>2</sup>*Institut für Quantenoptik und Quanteninformatik, Österreichische Akademie der Wissenschaften, A-6020 Innsbruck, Austria*

(Received 7 January 2005; published 29 August 2005)

We investigate how stabilizer theory can be used for constructing sufficient conditions for entanglement. First, we show how entanglement witnesses can be derived for a given state, provided some stabilizing operators of the state are known. These witnesses require only a small effort for an experimental implementation and are robust against noise. Second, we demonstrate that also nonlinear criteria based on uncertainty relations can be derived from stabilizing operators. These criteria can sometimes improve the witnesses by adding nonlinear correction terms. All our criteria detect states close to Greenberger-Horne-Zeilinger states, cluster and graph states. We show that similar ideas can be used to derive entanglement conditions for states which do not fit the stabilizer formalism, such as the three-qubit  $W$  state. We also discuss connections between the witnesses and some Bell inequalities.

DOI: [10.1103/PhysRevA.72.022340](https://doi.org/10.1103/PhysRevA.72.022340)

PACS number(s): 03.67.Mn, 03.65.Ud

### I. INTRODUCTION

Entanglement lies at the heart of quantum mechanics and plays also a crucial role in quantum information theory. While the properties of bipartite entanglement are still not fully understood, the situation for multipartite entanglement is even more unclear, since in the multipartite setting several inequivalent types of entanglement occur. However, entangled states of many qubits are needed for quantum information tasks such as measurement based quantum computation [1], error correction [2,3] or quantum cryptography [4], to mention only a few. Thus it is important both theoretically and experimentally to study multipartite entanglement and to provide efficient methods to verify that in a given experiment entanglement is really present.

In this paper we will apply the stabilizer theory [2,3] for entanglement detection. This theory already plays a determining role in quantum information science. Its key idea is describing the quantum state by its so-called stabilizing operators rather than the state vector. This works as follows: An observable  $S_k$  is a stabilizing operator of an  $N$ -qubit state  $|\psi\rangle$  if the state  $|\psi\rangle$  is an eigenstate of  $S_k$  with eigenvalue 1,

$$S_k|\psi\rangle = |\psi\rangle. \quad (1)$$

Many highly entangled  $N$ -qubit states can be uniquely defined by  $N$  stabilizing operators which are locally measurable, i.e., they are products of Pauli matrices.

The main result of the present paper can be formulated as follows: If one has a given state  $|\psi\rangle$  and has identified some of its stabilizing operators, then it is easy to derive entanglement conditions which detect states in the proximity of  $|\psi\rangle$ . So looking for stabilizing operators should be the first step in order to detect entanglement. All the conditions presented are easy to implement in experiments and are robust against noise. We mainly consider criteria detecting entanglement

close to Greenberger-Horne-Zeilinger (GHZ) [5], cluster [6], and graph states [7]. We use different types of entanglement conditions, they may be linear criteria, such as entanglement witnesses, or nonlinear criteria, based on uncertainty relations. In this way we complete our results of Ref. [8], where witnesses for the detection of multipartite entanglement in the vicinity of GHZ and cluster states were derived. Note that the stabilizer formalism also allows to derive Bell inequalities, this has been recently investigated in Ref. [9]. We do not aim to derive Bell inequalities here, since they are used to rule out local hidden variable models, a notion independent of quantum physics. However, some of our constructions exhibit close connections to Bell inequalities, and this will also be discussed.

Our paper is organized as follows. Since GHZ states are the most studied stabilizer states, we use mainly them to explain our ideas, the generalization to other stabilizer states is then usually straightforward. So we start in Sec. II by recalling the basic facts about the stabilizing operators of GHZ states. Then we present a method for obtaining a family of entanglement witnesses for detecting entanglement close to GHZ states. First we present witnesses detecting any (i.e., even partial or biseparable) entanglement. Then we present witnesses which detect only genuine multiqubit entanglement. We discuss some interesting connections to Bell inequalities. In Sec. III we present witnesses for cluster and graph states. We also consider detecting entanglement close to given mixed states. Finally, we present entanglement witnesses for a  $W$  state. It is of interest since the  $W$  state does not fit the stabilizer framework. We show that our ideas can still be generalized for this case. In Sec. IV we present nonlinear entanglement conditions in the form of variance based uncertainty relations. It turns out that they can often improve the witnesses by adding nonlinear terms. In Sec. V we present entanglement conditions which are based on entropic uncertainty relations. Finally, in the Appendices we collect some basic facts about the stabilizer formalism and present some technical calculations in detail.

\*Electronic address: toth@alumni.nd.edu

†Electronic address: otfried.guehne@uibk.ac.at

## II. GHZ STATES AS EXAMPLES OF STABILIZER STATES

Let us start by introducing the stabilizer formalism using the example of GHZ states. An  $N$ -qubit GHZ state is given by

$$|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (2)$$

Besides this explicit definition one may define the GHZ state also in the following way: Let us look at the observables,

$$S_1^{(\text{GHZ}_N)} := \prod_{k=1}^N X^{(k)},$$

$$S_k^{(\text{GHZ}_N)} := Z^{(k-1)}Z^{(k)} \text{ for } k = 2, 3, \dots, N, \quad (3)$$

where  $X^{(k)}$ ,  $Y^{(k)}$ , and  $Z^{(k)}$  denote the Pauli matrices acting on the  $k$ th qubit. Now we can define the GHZ state as the state  $|\text{GHZ}_N\rangle$  which fulfills

$$S_k^{(\text{GHZ}_N)}|\text{GHZ}_N\rangle = |\text{GHZ}_N\rangle \quad (4)$$

for  $k=1, 2, \dots, N$ . One can straightforwardly calculate that these definitions are equivalent and the GHZ state is uniquely defined by the Eqs. (4). From a physical point of view the definition via Eqs. (4) stresses that the GHZ state is uniquely determined by the fact that it exhibits perfect correlations for the observables  $S_k^{(\text{GHZ}_N)}$ .

Note that  $|\text{GHZ}_N\rangle$  is stabilized not only by  $S_k^{(\text{GHZ}_N)}$ , but also by their products. These operators, all having perfect correlations for a GHZ state, form a group called stabilizer [2]. This  $2^N$ -element group of operators will be denoted by  $\mathcal{S}^{(\text{GHZ}_N)}$ .  $S_k^{(\text{GHZ}_N)}$  are the generators of this group which we will denote as  $\mathcal{S}^{(\text{GHZ}_N)} = \langle S_1^{(\text{GHZ}_N)}, S_2^{(\text{GHZ}_N)}, \dots, S_N^{(\text{GHZ}_N)} \rangle$ . For more details on the stabilizer please see Appendix A.

### A. Witnesses for stabilizer states

In order to show that a given state contains some entanglement, we must exclude the possibility that the state is fully separable, i.e., it can be written as

$$\varrho = \sum_i p_i \varrho_i^{(1)} \otimes \varrho_i^{(2)} \otimes \dots \otimes \varrho_i^{(N)} \quad (5)$$

with  $p_i \geq 0$ ,  $\sum_i p_i = 1$ .

Before presenting entanglement witness operators, let us shortly recall their definition. An entanglement witness  $\mathcal{W}$  is an observable which has a positive or zero expectation value for all separable states, and a negative one on some entangled states [10],

$$\text{Tr}(\mathcal{W}\varrho) \begin{cases} \geq 0 & \text{for all separable states } \varrho_s, \\ < 0 & \text{for some entangled states } \varrho_e. \end{cases} \quad (6)$$

Thus a negative expectation value in an experiment signals the presence of entanglement.

In this paper we will construct a family of entanglement witnesses using the elements of the stabilizer. We will call these stabilizer witnesses.

### B. Ruling out full separability

In the following stabilizer witnesses will be used to detect entanglement close to GHZ states. We will construct witnesses of the form

$$\mathcal{W} := c_0 \mathbb{1} - \tilde{S}_k^{(\text{GHZ}_N)} - \tilde{S}_l^{(\text{GHZ}_N)}, \quad (7)$$

where  $\tilde{S}_{k/l}^{(\text{GHZ}_N)}$  are elements of the stabilizer group,

$$c_0 := \max_{\varrho \in \mathcal{P}} (\langle \tilde{S}_k^{(\text{GHZ}_N)} + \tilde{S}_l^{(\text{GHZ}_N)} \rangle_{\varrho}), \quad (8)$$

and  $\mathcal{P}$  denotes the set of product states. Since the set of separable states is convex,  $c_0$  is also the maximum for mixed separable states of the form Eq. (5).

Clearly, if we want to detect entangled states with  $\mathcal{W}$ , we must choose  $\tilde{S}_k^{(\text{GHZ}_N)}$  and  $\tilde{S}_l^{(\text{GHZ}_N)}$  such that the maximum of  $\langle \tilde{S}_k^{(\text{GHZ}_N)} + \tilde{S}_l^{(\text{GHZ}_N)} \rangle$  for entangled quantum states is larger than the maximum for separable states. Whether this condition holds depends on the question whether the  $\tilde{S}_k^{(\text{GHZ}_N)}$  and  $\tilde{S}_l^{(\text{GHZ}_N)}$  commute locally.

**Definition 1:** Two correlation operators of the form

$$K = K^{(1)} \otimes K^{(2)} \otimes \dots \otimes K^{(N)},$$

$$L = L^{(1)} \otimes L^{(2)} \otimes \dots \otimes L^{(N)}, \quad (9)$$

commute locally if

$$\text{for every } n \in \{1, 2, \dots, N\}: K^{(n)}L^{(n)} = L^{(n)}K^{(n)}. \quad (10)$$

Using Definition 1, we can make the following statement.

**Observation 1:** Two multiqubit correlation operators,  $K$  and  $L$ , commute locally iff there is a pure product state among their common eigenstates.

*Proof:*  $K$  and  $L$  commute locally iff for all  $n \in \{1, 2, \dots, N\}$  there are two vectors,  $|\phi_n\rangle$  and  $|\phi_n^\perp\rangle$ , which are common eigenstates of  $K^{(n)}$  and  $L^{(n)}$ . Thus  $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_N\rangle$  is a common eigenstate of  $K$  and  $L$ .  $\square$  Hence it follows that if  $\tilde{S}_k^{(\text{GHZ}_N)}$  and  $\tilde{S}_l^{(\text{GHZ}_N)}$  commute locally then the maximum of  $\langle \tilde{S}_k^{(\text{GHZ}_N)} + \tilde{S}_l^{(\text{GHZ}_N)} \rangle$  for separable and entangled states coincide.

After these considerations, we construct our witness from two locally noncommuting stabilizing operators.

**Theorem 1:** A witness detecting entanglement around an  $N$ -qubit GHZ state is

$$\mathcal{W}_m^{(\text{GHZ}_N)} := \mathbb{1} - S_1^{(\text{GHZ}_N)} - S_m^{(\text{GHZ}_N)}, \quad (11)$$

where  $m=2, 3, \dots, N$ .

*Proof:* The proof is based on the Cauchy-Schwarz inequality. Using this and  $\langle X^{(i)} \rangle^2 + \langle Z^{(i)} \rangle^2 \leq 1$ , for pure product states we obtain

$$\begin{aligned} & \langle S_1^{(\text{GHZ}_N)} \rangle + \langle S_m^{(\text{GHZ}_N)} \rangle \\ &= \langle X^{(1)} \rangle \langle X^{(2)} \rangle \dots \langle X^{(N)} \rangle + \langle Z^{(m-1)} \rangle \langle Z^{(m)} \rangle \\ &\leq |\langle X^{(m-1)} \rangle| |\langle X^{(m)} \rangle| + |\langle Z^{(m-1)} \rangle| |\langle Z^{(m)} \rangle| \\ &\leq \sqrt{\langle X^{(m-1)} \rangle^2 + \langle Z^{(m-1)} \rangle^2} \sqrt{\langle X^{(m)} \rangle^2 + \langle Z^{(m)} \rangle^2} \leq 1. \end{aligned} \quad (12)$$

It is easy to see that the bound is also valid for mixed separable states. This proof can straightforwardly be generalized for arbitrary two locally noncommuting elements of the stabilizer.  $\square$

Witnesses can be constructed with more than two elements of the stabilizer as

$$\hat{\mathcal{W}}_m^{(\text{GHZ}_N)} := 1 - S_1^{(\text{GHZ}_N)} - S_m^{(\text{GHZ}_N)} - S_1^{(\text{GHZ}_N)} S_m^{(\text{GHZ}_N)} \quad (13)$$

for  $m=2,3,\dots,N$  rule out full separability. This can be proved in a similar calculation as in Theorem 1, using the fact that  $\langle X^{(i)} \rangle^2 + \langle Y^{(i)} \rangle^2 + \langle Z^{(i)} \rangle^2 \leq 1$ . Later, in Sec. IV we will see how these conditions can be improved by adding refinement terms which are quadratic in the expectation values.

### C. Criteria for witnesses

Having derived the first entanglement witnesses, it is now time to ask, whether they are really useful witnesses. In fact, there are, for a given state, always infinitely many witnesses allowing the detection of this state. However, some of them are more useful than others. Two criteria for the usefulness of witnesses are of interest: First, it is important to characterize how much a witness tolerates noise. Second, it is crucial to know, how much experimental effort is needed to measure the witness.

Witnesses are usually designed to detect entangled states close to a given pure state  $|\Psi\rangle$ . From a practical point of view it is very important to know, how large neighborhood of  $|\Psi\rangle$  is detected as entangled. This can be characterized in the following way.

**Definition 2:** Let the density matrix of the state obtained after mixing with white noise be given by

$$\varrho(p_{\text{noise}}) := p_{\text{noise}} \frac{1}{2^N} + (1 - p_{\text{noise}}) |\Psi\rangle\langle\Psi|. \quad (14)$$

Here  $p_{\text{noise}}$  determines the ratio of white noise in the mixture. Then, the robustness to noise for a witness  $\mathcal{W}$  is determined by the maximal noise ratio for which it still detects  $\varrho(p_{\text{noise}})$  as entangled.

It is easy to see that witness  $\mathcal{W}$  detects  $\varrho(p_{\text{noise}})$  as entangled if  $p_{\text{noise}} < p_{\text{limit}}$  where

$$p_{\text{limit}} := \frac{-\langle \text{GHZ}_N | \mathcal{W} | \text{GHZ}_N \rangle}{2^{-N} \text{Tr}(\mathcal{W}) - \langle \text{GHZ}_N | \mathcal{W} | \text{GHZ}_N \rangle}. \quad (15)$$

To give an example, for witnesses of the form Eq. (7) we have  $p_{\text{limit}} = (\gamma - 1) / \gamma$  where

$$\gamma := \frac{\langle \text{GHZ}_N | S_k^{(\text{GHZ}_N)} + S_l^{(\text{GHZ}_N)} | \text{GHZ}_N \rangle}{\max_{\varrho \in \mathcal{P}} [\langle S_k^{(\text{GHZ}_N)} + S_l^{(\text{GHZ}_N)} \rangle_{\varrho}]}. \quad (16)$$

Clearly, the maximum of the numerator is 2, while the minimum of the denominator is 1. Thus the maximum noise tolerance achievable by a witness of the form Eq. (7) is given by  $p_{\text{limit}} = 1/2$ . Witnesses  $\mathcal{W}_m^{(\text{GHZ}_N)}$  from Eq. (11) have exactly this noise tolerance thus they are optimal among stabilizer witnesses with two correlation terms. Witnesses  $\tilde{\mathcal{W}}_m^{(\text{GHZ}_N)}$  from Eq. (13) detect  $\varrho(p_{\text{noise}})$  as entangled if  $p_{\text{noise}} < 2/3$ , thus, they are more robust against noise. It can be proved that

Eq. (13) is optimal among stabilizer witnesses with three correlations terms from the point of view of noise tolerance.

The experimental effort needed for measuring a witness can be characterized by the number of local measurement settings needed for its implementation [11].

**Definition 3:** The local decomposition of a witness is defined as follows: Any witness can be decomposed into a sum  $\mathcal{W} = \sum_i \mathcal{M}_i$  where each of the terms  $\mathcal{M}_i$  can be measured by a local measurement setting. One local setting  $\{O^{(k)}\}_{k=1}^N$  consists of performing simultaneously the von Neumann measurements  $O^{(k)}$  on the corresponding parties. By repeating the measurements many times one can determine the probabilities of the  $2^N$  different outcomes. Given these probabilities it is possible to compute all two-point correlations  $\langle O^{(k)} O^{(l)} \rangle$ , three-point correlations  $\langle O^{(k)} O^{(l)} O^{(m)} \rangle$ , etc.

It is easy to see that measuring only one setting is not enough for entanglement detection. For measuring all the witnesses  $\mathcal{W}_m^{(\text{GHZ}_N)}$  given Eq. (11) for  $m=2,3,\dots,N$ , two measurement settings are required for an implementation, namely  $\{X^{(1)}, X^{(2)}, \dots, X^{(N)}\}$  and  $\{Z^{(1)}, Z^{(2)}, \dots, Z^{(N)}\}$ . The witnesses  $\tilde{\mathcal{W}}_m^{(\text{GHZ}_N)}$  from Eq. (13) require a measurement of three settings,  $\{X^{(1)}, X^{(2)}, \dots, X^{(N)}\}$ ,  $\{Y^{(1)}, Y^{(2)}, \dots, Y^{(N)}\}$ , and  $\{Z^{(1)}, Z^{(2)}, \dots, Z^{(N)}\}$ .

### D. Detecting genuine multipartite entanglement

Up to now we considered witnesses which detect any (even partial) entanglement. However, for multipartite systems there are several classes of entanglement. The most interesting class of entangled states are the genuine multipartite entangled states. These are defined as follows. Let us assume that a pure state  $|\psi\rangle$  on an  $N$ -qubit system is given. If we can find a partition of the  $N$  qubits into two groups  $\mathcal{A}$  and  $\mathcal{B}$  such that  $|\psi\rangle$  is a product state with respect to this partition,

$$|\psi\rangle = |\phi\rangle_{\mathcal{A}} |\chi\rangle_{\mathcal{B}} \quad (17)$$

then we call the state  $|\psi\rangle$  biseparable (with respect to the given partition). Note that the states  $|\phi\rangle_{\mathcal{A}}$  and  $|\chi\rangle_{\mathcal{B}}$  may be entangled, thus the state  $|\psi\rangle$  is not necessarily fully separable. According to the usual definition a mixed state is called biseparable iff it can be written as a convex combination of pure biseparable states,

$$\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad (18)$$

where the  $|\psi_i\rangle$  may be biseparable with respect to different partitions. If a state is not biseparable then it is called genuine multipartite entangled. In experiments dealing with the generation of entanglement in multiqubit systems it is necessary to generate and verify genuine multipartite entanglement, since the simple statement ‘‘The state is entangled’’ would still allow that only two of the qubits are entangled while the rest is in a product state.

Witnesses for the detection of genuine multipartite entanglement have already been used experimentally for entanglement detection close to three-qubit  $W$  states and four-qubit singlet states [12]. They used the projector on the state

to be detected as an observable to detect entanglement. For GHZ states, the projector-based witness reads

$$\widetilde{\mathcal{W}}^{(\text{GHZ}_N)} := \frac{1}{2} \mathbb{1} - |\text{GHZ}_N\rangle\langle\text{GHZ}_N|, \quad (19)$$

which has also been used in an experiment [13]. This witness detects genuine  $N$ -qubit entanglement around an  $N$ -qubit GHZ state. The constant  $1/2$  corresponds to the maximal squared overlap between the GHZ state and the pure biseparable states, this can be calculated using the methods presented in Ref. [12].

Witness Eq. (19) can be interpreted in the following way.  $\langle\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}\rangle$  is  $-1/2$  only for the GHZ state. For any other state it is larger. In general, the more negative  $\langle\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}\rangle_{|\Psi\rangle}$  is, the closer state  $|\Psi\rangle$  is to the GHZ state. It is known that in the proximity of the GHZ state there are only states with genuine  $N$ -qubit entanglement, so the constant in Eq. (19) is chosen such that if  $\langle\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}\rangle < 0$  then the state is in this neighborhood and is detected as entangled.

Now we will show that the projector-based witness Eq. (19) can be constructed as a sum of elements of the stabilizer. First, note that the generators of the stabilizer  $S_k^{(\text{GHZ}_N)}$  can be used to define a very convenient basis for calculations, namely their common eigenvectors.  $|\text{GHZ}_N\rangle$  is one of them giving a  $+1$  eigenvalue for all  $S_k^{(\text{GHZ}_N)}$ 's. Allowing both  $+1$  and  $-1$  eigenvalues in Eq. (1),  $2^N$   $N$ -qubit states can be defined which are orthogonal to each other and form a complete basis. These are all GHZ states, but in different bases, i.e., they are of the form  $(|x^{(1)}\dots x^{(N)}\rangle \pm |\bar{x}^{(1)}\dots\bar{x}^{(N)}\rangle)/\sqrt{2}$  with  $x^{(l)} \in \{0, 1\}$  and  $\bar{x}^{(l)} = 1 - x^{(l)}$ . We will refer to this basis as the GHZ state basis. This basis will turn out to be extremely useful since all operators of the stabilizer are diagonal in this basis.

Now, the projector onto a GHZ state can be written with the stabilizing operators [14]

$$|\text{GHZ}_N\rangle\langle\text{GHZ}_N| = \prod_{k=1}^N \frac{S_k^{(\text{GHZ}_N)} + \mathbb{1}}{2}. \quad (20)$$

This can be directly seen in the GHZ basis. From Eq. (20) it follows that the projector-based witness can also be decomposed into the sum of stabilizing terms, i.e.,  $\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}$  is a stabilizer witness. This decomposition can be used to measure the witness locally. However, the number of settings needed seems to increase exponentially with the number of qubits [15]. Thus we must find other stabilizer witnesses for which measuring them is more feasible.

For detecting biseparable entanglement it was enough to use two stabilizing operators for the witness. For the detection of  $N$ -qubit entanglement we must make measurements on all qubits and must measure a full set of generators. This is because we need that the expectation value of the witness is minimal only for the GHZ state. If the witness does not contain a full set of generators then there are at least two of the elements of the GHZ basis giving the minimum. There is, however, always a superposition of two basis vectors of the GHZ basis which is biseparable. This biseparable state

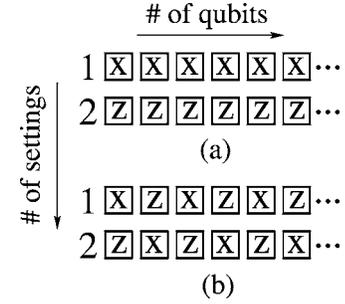


FIG. 1. (a) Measurement settings needed for the approach presented in this paper for detecting entangled states close to GHZ states and (b) cluster states. For each qubit the measured spin component is indicated.

would also give a minimum for our witness. Thus this witness could not be used for detecting genuine  $N$ -qubit entanglement.

The main idea of detecting genuine multiqubit entanglement with the stabilizing operators is the following.

**Observation 2:** Let us consider some of the stabilizing operators. If this set of operators contains a complete set of generators and for a given state the expectation values of these correlation operators are close enough to the values for a GHZ state, then this state must be close to a GHZ state and is therefore multiqubit entangled.

Now we can derive the first entanglement witness.

**Theorem 2:** The witness

$$\mathcal{W} := (N - 1)\mathbb{1} - \sum_{k=1}^N S_k^{(\text{GHZ}_N)} \quad (21)$$

detects only states with genuine  $N$ -qubit entanglement.

*Proof:* In Eq. (21) the constant term,  $c_0 = N - 1$ , was chosen such that the observable

$$X_\alpha := \mathcal{W} - \alpha \widetilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0 \quad (22)$$

for some  $\alpha > 0$  is positive semidefinite. Then we have for any state  $\varrho$  the inequality  $\alpha \text{Tr}(\varrho \widetilde{\mathcal{W}}^{(\text{GHZ}_N)}) \leq \text{Tr}(\varrho \mathcal{W})$  which implies that  $\text{Tr}(\varrho \mathcal{W}) < 0$  can only happen if  $\text{Tr}(\varrho \widetilde{\mathcal{W}}^{(\text{GHZ}_N)}) < 0$ . Thus all states detected with  $\mathcal{W}$  are also detected by  $\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}$  and  $\mathcal{W}$  is a multiqubit witness. Clearly, we would like to have  $c_0$  as small as possible, since the smaller  $c_0$  is, the more entangled states  $\mathcal{W}$  detects. Simple calculation leads to  $c_0 = N - 1$ . One can check that with this choice  $\mathcal{W} - 2\widetilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0$ .  $\square$

Both witnesses  $\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}$  and  $\mathcal{W}$  detect entangled states close to GHZ states. The main advantage of  $\mathcal{W}$  in comparison with  $\widetilde{\mathcal{W}}^{(\text{GHZ}_N)}$  lies in the fact that for implementing it only two measurement settings are needed, namely the ones shown in Fig. 1(a). The first setting,  $\{X^{(1)}, X^{(2)}, \dots, X^{(N)}\}$ , is needed to measure  $\langle S_1^{(\text{GHZ}_N)} \rangle$ , the second one,  $\{Z^{(1)}, Z^{(2)}, \dots, Z^{(N)}\}$ , is to measure the expectation values for the other generators. The other characteristic to check is the noise tolerance of the witness. The witness  $\mathcal{W}$  detects states

mixed with noise of the form Eq. (14) if  $p_{\text{noise}} < 1/N$ . Thus the noise tolerance decreases as the number of qubits increases.

However, using a similar construction it is also possible to derive a witness which is robust against noise even for many qubits and still requires only two measurement settings.

**Theorem 3:** The following entanglement witness detects genuine  $N$ -qubit entanglement for states close to an  $N$ -qubit GHZ state,

$$\mathcal{W}^{(\text{GHZ}_N)} := 3\mathbb{1} - 2 \left( \frac{S_1^{(\text{GHZ}_N)} + 1}{2} + \prod_{k=2}^N \frac{S_k^{(\text{GHZ}_N)} + 1}{2} \right). \quad (23)$$

This witness has the best noise tolerance among stabilizer witnesses which need only two measurement settings and have the property  $\mathcal{W}^{(\text{GHZ}_N)} - \alpha \tilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0$  for some  $\alpha > 0$ .

*Proof:* To prove the first statement, one can show by direct calculation that  $\mathcal{W}^{(\text{GHZ}_N)} - 2\tilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0$ . Thus  $\mathcal{W}^{(\text{GHZ}_N)}$  is a multiqubit witness. For the proof of optimality see Appendix B.

To give an example, for the simple case of three qubits the witness is

$$\mathcal{W}^{(\text{GHZ}_3)} := \frac{3}{2}\mathbb{1} - X^{(1)}X^{(2)}X^{(3)} - \frac{1}{2}(Z^{(1)}Z^{(2)} + Z^{(2)}Z^{(3)} + Z^{(1)}Z^{(3)}). \quad (24)$$

Three-qubit genuine multiqubit entangled states can belong to the so-called  $W$  class or to the GHZ class [16]. Knowing that  $\tilde{\mathcal{W}}^{(\text{GHZ}_3)} + 1/4$  detects GHZ-class entanglement [16], we obtain that  $\mathcal{W}^{(\text{GHZ}_3)} + 1/2$  detects also only GHZ-class entanglement.

The witness  $\mathcal{W}^{(\text{GHZ}_N)}$  is quite robust against noise. It detects states mixed with white noise as true multipartite entangled for

$$p_{\text{noise}} < \frac{1}{3 - 2^{(2-N)}}. \quad (25)$$

Thus it tolerates at least 33% noise, independently from the number of qubits. Again, only two measurement settings are necessary for an implementation [see Fig. 1(a)].

The expression for the witness  $\mathcal{W}^{(\text{GHZ}_N)}$  can be simplified using the fact that

$$\prod_{k=2}^N \frac{S_k^{(\text{GHZ}_N)} + 1}{2} = |00 \cdots 0\rangle\langle 00 \cdots 0| + |11 \cdots 1\rangle\langle 11 \cdots 1|, \quad (26)$$

where  $|11 \cdots 1\rangle\langle 11 \cdots 1|$  is the projector on the state with all spins down and  $|00 \cdots 0\rangle\langle 00 \cdots 0|$  is the projector on the state with all spins up. Using this one obtains

$$\begin{aligned} \mathcal{W}^{(\text{GHZ}_N)} &= 2\mathbb{1} - X^{(1)}X^{(2)}X^{(3)} \cdots X^{(N)} - 2|00 \cdots 0\rangle\langle 00 \cdots 0| \\ &\quad - 2|11 \cdots 1\rangle\langle 11 \cdots 1|. \end{aligned} \quad (27)$$

### E. Bell inequalities for GHZ states

As a sidestep we will discuss now a very surprising feature of the stabilizer witnesses, namely that they are closely

related to Mermin-type Bell inequalities [17,18]. As we will see, this relationship sheds light on the question whether and when Bell inequalities [19–21] can detect genuine multipartite entanglement.

First note that witnesses different from the previous ones can be obtained by including further terms of the stabilizer and using more than two measurement settings. For instance, following the lines of the preceding section it is easy to see that the observable:

$$\begin{aligned} \mathcal{W}_{\text{Mermin}} &:= 2\mathbb{1} - S_1^{(\text{GHZ}_3)}(1 + S_2^{(\text{GHZ}_3)})(1 + S_3^{(\text{GHZ}_3)}) \\ &= 2\mathbb{1} + Y^{(1)}Y^{(2)}X^{(3)} + X^{(1)}Y^{(2)}Y^{(3)} \\ &\quad + Y^{(1)}X^{(2)}Y^{(3)} - X^{(1)}X^{(2)}X^{(3)} \end{aligned} \quad (28)$$

detects genuine three-party entanglement around a GHZ state. It detects a GHZ state mixed with white noise if  $p_{\text{noise}} < 1/2$ . The witness  $\mathcal{W}_{\text{Mermin}}$  is equivalent to Mermin's inequality [18],

$$\begin{aligned} \langle X^{(1)}X^{(2)}X^{(3)} \rangle - \langle X^{(1)}Y^{(2)}Y^{(3)} \rangle - \langle Y^{(1)}X^{(2)}Y^{(3)} \rangle - \langle Y^{(1)}Y^{(2)}X^{(3)} \rangle \\ \leq 2. \end{aligned} \quad (29)$$

In Ref. [22] the condition given in Eq. (29) was used for detecting entanglement in a three-qubit photonic system and a measurement result equivalent to  $\langle \mathcal{W}_{\text{Mermin}} \rangle \approx -0.83 \pm 0.09$  was obtained, thus the created state was genuine three-qubit entangled.

For  $N > 3$  the Bell operator in Mermin's inequality contains also only stabilizing terms.

**Theorem 4:** For the Bell operator of the Mermin's inequality [23,24]

$$\begin{aligned} M_N &:= \frac{1}{2^{N-1}}(X^{(1)}X^{(2)}X^{(3)}X^{(4)} \cdots X^{(N-1)}X^{(N)} \\ &\quad - Y^{(1)}Y^{(2)}X^{(3)}X^{(4)} \cdots X^{(N-1)}X^{(N)} \\ &\quad + Y^{(1)}Y^{(2)}Y^{(3)}Y^{(4)} \cdots X^{(N-1)}X^{(N)} - \dots) \end{aligned} \quad (30)$$

the operator expectation value for biseparable states is bounded by

$$\langle M_N \rangle \leq \frac{1}{2}, \quad (31)$$

while the quantum maximum is 1. Note that a term in Eq. (30) represents the sum of all its possible permutations.

*Proof:*  $M_N$  can alternatively written as

$$\begin{aligned} M_N &= S_1^{(\text{GHZ}_N)} \prod_{k=2}^N \frac{S_k^{(\text{GHZ}_N)} + 1}{2} \\ &= |00 \cdots 0\rangle\langle 11 \cdots 1| + |11 \cdots 1\rangle\langle 00 \cdots 0|. \end{aligned} \quad (32)$$

The maximum for  $\langle M_N \rangle$  for biseparable states can be obtained knowing

$$|\text{GHZ}_N\rangle\langle \text{GHZ}_N| - M_N = |\text{GHZ}_N^-\rangle\langle \text{GHZ}_N^-| \geq 0, \quad (33)$$

where  $|\text{GHZ}_N^-\rangle = (|0000 \cdots\rangle - |1111 \cdots\rangle) / \sqrt{2}$ . Hence for biseparable states  $\varrho$ ,

$$\langle M_N \rangle_{\rho} \leq \langle |\text{GHZ}_N\rangle\langle \text{GHZ}_N| \rangle_{\rho} \leq \frac{1}{2}. \quad (34)$$

For fully separable states the bound is lower and is given in Ref. [25].  $\square$

### III. WITNESSES FOR CLUSTER, GRAPH AND W STATES

#### A. Witnesses for cluster states

Let us turn now to cluster states. These are a family of multiqubit states which have attracted increasing attention in the last years. A cluster state  $|C_N\rangle$  is defined to be the state fulfilling the equations  $|C_N\rangle = S_k^{(C_N)}|C_N\rangle$  with the following stabilizing operators:

$$S_1^{(C_N)} := X^{(1)}Z^{(2)},$$

$$S_k^{(C_N)} := Z^{(k-1)}X^{(k)}Z^{(k+1)}, \quad k = 2, 3, \dots, N-1,$$

$$S_N^{(C_N)} := Z^{(N-1)}X^{(N)}. \quad (35)$$

Witnesses similar to Eq. (11) which rule out full separability can be constructed with two locally noncommuting operators as [26]

$$\mathcal{W}_k^{(C_N)} := \mathbb{1} - S_k^{(C_N)} - S_{k+1}^{(C_N)} \quad \text{for } k = 1, 2, \dots, N-1. \quad (36)$$

This witness detects biseparable states close to an  $N$ -qubit cluster state. The proof is essentially the same as the one for Eq. (11).

Note that  $\mathcal{W}_k^{(C_N)}$  involves only two generators which act on at most four-qubits. This witness detects whether the reduced density matrix of the qubit quadruplet corresponding to qubits  $(k-1)$ ,  $(k)$ ,  $(k+1)$ , and  $(k+2)$  is entangled. The state of the rest of the qubits does not influence  $\langle \mathcal{W}_k^{(C_N)} \rangle$ . The witness  $\mathcal{W}_k^{(C_N)}$  tolerates noise if  $p_{\text{noise}} < 1/2$ .

The following witnesses have a better noise tolerance:

$$\hat{\mathcal{W}}_k^{(C_N)} := \mathbb{1} - S_k^{(C_N)} - S_{k+1}^{(C_N)} - S_k^{(C_N)}S_{k+1}^{(C_N)} \quad (37)$$

$$\text{for } k = 1, 2, \dots, N-1.$$

This witness still involves only the qubits of a quadruplet and tolerates noise if  $p_{\text{noise}} < 2/3$ .

Using witnesses  $\hat{\mathcal{W}}_k^{(C_N)}$ , one can construct a ‘‘composite’’ entanglement witness for which the noise tolerance increases with the number of qubits.

**Theorem 5:** The following entanglement witness detects entangled states close to a cluster state

$$\mathcal{W}_{\text{comp}}^{(C_N)} := \prod_{k=0}^{K-1} \mathbb{1} - S_{4k+1}^{(C_N)} - S_{4k+2}^{(C_N)} - S_{4k+1}^{(C_N)}S_{4k+2}^{(C_N)}, \quad (38)$$

where  $K := \lfloor (N+2)/4 \rfloor$  and  $\lfloor x \rfloor$  denotes the integer part of  $x$ . The witness Eq. (38) tolerates noise if

$$p_{\text{noise}} < \frac{2^K}{2^K + 1}. \quad (39)$$

*Proof:* The noise tolerance comes from direct calculation

along the lines of Eq. (15). Note that all the terms in the product in Eq. (38) act on disjoint sets of qubits. This is the reason that such a composite witness can be constructed.  $\square$

One can also construct witnesses for the detection of genuine multipartite entanglement close to cluster states, similar as for the case of GHZ states.

**Theorem 6:** The witnesses

$$\tilde{\mathcal{W}}^{(C_N)} := \frac{1}{2} - |C_N\rangle\langle C_N|, \quad (40)$$

$$\mathcal{W}^{(C_N)} := 3\mathbb{1} - 2 \left( \prod_{\text{odd } k} \frac{S_k^{(C_N)} + \mathbb{1}}{2} + \prod_{\text{even } k} \frac{S_k^{(C_N)} + \mathbb{1}}{2} \right) \quad (41)$$

detect genuine  $N$ -party entanglement close to a cluster state.  $\mathcal{W}^{(C_N)}$  is optimal from the point of view of noise tolerance among the stabilizer witnesses which need only two measurement settings and have the property  $\mathcal{W}^{(C_N)} - \alpha \tilde{\mathcal{W}}^{(C_N)} \geq 0$  for some  $\alpha > 0$ .

*Proof:* First we must prove that Eq. (40) is a multiqubit witness. For that we must use that from a cluster state one can generate a singlet between arbitrary qubits by local operations [6]. Using the results of Ref. [27] this implies that the maximal Schmidt coefficient of a cluster state when making a Schmidt decomposition with respect to an arbitrary bipartite split does not exceed the maximal Schmidt coefficient of the singlet, which equals  $1/\sqrt{2}$ . Then, from the methods of Ref. [12] it follows that  $\tilde{\mathcal{W}}^{(C_N)}$  is a witness for multiqubit entanglement. After that we have to prove that Eq. (41) is a multiqubit witness. This can be proved similarly as it has been done for Theorem 3 using that  $\mathcal{W}^{(C_N)} - 2\tilde{\mathcal{W}}^{(C_N)} \geq 0$ . Concerning the optimality, see Appendix B.  $\square$

The stabilizing operators in  $\mathcal{W}^{(C_N)}$  are again divided into two groups corresponding to the two settings  $\{X^{(1)}, Z^{(2)}, X^{(3)}, Z^{(4)}, \dots\}$  and  $\{Z^{(1)}, X^{(2)}, Z^{(3)}, X^{(4)}, \dots\}$  as shown in Fig. 1(b). Witness  $\mathcal{W}^{(C_N)}$  tolerates mixing with noise if

$$p_{\text{noise}} < \begin{cases} (4 - 4/2^{N/2})^{-1} & \text{for even } N, \\ [4 - 2(1/2^{(N+1)/2} + 1/2^{(N-1)/2})]^{-1} & \text{for odd } N. \end{cases} \quad (42)$$

Thus, for any number of qubits at least 25% noise is tolerated.

#### B. Witnesses for graph states

Results similar to the ones derived before hold also for graph states [7,28]. These states are defined in the following way: One takes a graph, i.e., a set of  $N$  vertices and some edges connecting them. Edges of this graph are described by the adjacency matrix  $\Gamma$ .  $\Gamma_{kl} = 1(0)$  if the vertices  $k$  and  $l$  are connected (not connected). Based on that one can define the stabilizing operators

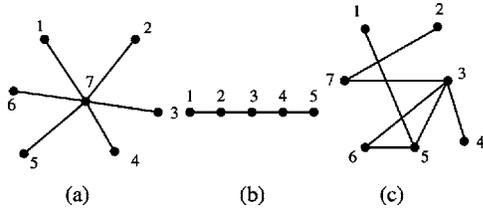


FIG. 2. Graphs corresponding to different graph states. (a) Star graph and (b) cluster state graph. A graph state corresponding to a star graph is equivalent to a GHZ state under local unitaries. (c) A seven-vertex graph which has a triangle. Due to this it is not a two-colorable graph.

$$S_k^{(G_N)} := X^{(k)} \prod_{\substack{\text{Neighbors} \\ l \text{ of } k}} Z^{(l)} = X^{(k)} \prod_{l \neq k} (Z^{(l)})^{\Gamma_{kl}}. \quad (43)$$

Then, the graph state  $|G_N\rangle$  is defined as the  $N$ -qubit state fulfilling  $|G_N\rangle = S_k^{(G_N)} |G_N\rangle$ . Physically, the graph provides also a possible generation method. The graph state can be created from a fully separable state by using Ising interactions between the connected qubits. In fact, many useful multiqubit states can be treated in the graph state formalism, for instance also GHZ states and cluster states. The corresponding graphs are shown in Fig. 2.

**Theorem 7:** A witness detecting biseparable entanglement close to graph states can be given as

$$\mathcal{W}_{kl}^{(G_N)} := \mathbb{1} - S_k^{(G_N)} - S_l^{(G_N)}, \quad (44)$$

where the spins  $(k)$  and  $(l)$  are neighbors, and a witness detecting genuine  $N$ -party entanglement can be defined as

$$\mathcal{W}^{(G_N)} := (N-1)\mathbb{1} - \sum_k S_k^{(G_N)}. \quad (45)$$

*Proof:* The proofs are essentially the same as before. First one must show that  $\mathbb{1}/2 - |G_N\rangle\langle G_N|$  is a witness for true multipartite entanglement. Then one can prove that witnesses Eq. (44) and Eq. (45) detect also only genuine multipartite entanglement.  $\square$

Now the number of settings needed for measuring  $\mathcal{W}^{(G_N)}$  depends on the graph corresponding to the graph state to be detected. For this we need the notion of colorability of graphs. A graph is  $M$ -colorable, if one can divide the vertices into  $M$  groups and assign to the vertices of each group a color, such that neighboring vertices have different colors (see Fig. 2). For two-colorable graphs, only two settings are needed. In this case the  $S_k^{(G_N)}$  operators can be divided into two groups corresponding to the two settings. In general, for  $M$ -colorable graphs  $M$  settings are needed for measuring the witness  $\mathcal{W}^{(G_N)}$ . In this sense, the most settings ( $M=N$ ) are needed for the complete graph [29].

It is, however, important to note at this point that the colorability of the graph is not an intrinsic and physical property of the graph state. Usually, a graph state can be represented by different graphs up to local unitaries, i.e., different graphs  $G_1$  and  $G_2$  can result in two graph states  $|G_1\rangle$  and  $|G_2\rangle$  which are the same up to a local change of the basis. Here,  $G_1$  and  $G_2$  may have different colorability properties, e.g.,  $G_1$

may be two colorable and  $G_2$   $N$  colorable. The question, which graphs give the same graph state is still an open and challenging problem in stabilizer theory. Recently, much progress has been achieved concerning a subclass of local unitary transformations, the so-called local Clifford transformations [30]. Efficient algorithms have been developed which allow the determination of all graphs which are equivalent within this subclass of local unitary transformations. These methods can readily be used to find witnesses with a small number of measurement settings.

### C. Obtaining the fidelity of the prepared state

Let us say that in an experiment we intend to create a GHZ state. Beside knowing that the prepared state  $\rho$  is entangled, we would also like to know how good its fidelity is. The fidelity could be measured by measuring the projector on the GHZ state

$$F := \text{Tr}(|\text{GHZ}_N\rangle\langle\text{GHZ}_N| \rho). \quad (46)$$

However, we would encounter the same problem as with witnesses: The number of local settings needed for measuring the projector increases rapidly with the size.

Fortunately it is possible to obtain a lower bound on the fidelity from the expectation value of our witnesses. For example, for our GHZ witness defined in Theorem 3 we have  $\mathcal{W}^{(\text{GHZ}_N)} - 2\tilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0$ . Hence

$$|\text{GHZ}_N\rangle\langle\text{GHZ}_N| \geq \frac{1}{2} - \frac{1}{2}\mathcal{W}^{(\text{GHZ}_N)}, \quad (47)$$

where  $\mathcal{W}^{(\text{GHZ}_N)}$  is defined in Eq. (23). Now a lower bound on the fidelity  $F := \text{Tr}(|\text{GHZ}_N\rangle\langle\text{GHZ}_N| \rho)$  can be obtained as  $F' := \text{Tr}(P' \rho)$ , where

$$P' := \frac{1}{2} - \frac{1}{2}\mathcal{W}^{(\text{GHZ}_N)} = \frac{S_1^{(\text{GHZ}_N)} + \mathbb{1}}{2} + \prod_{k=2}^N \frac{S_k^{(\text{GHZ}_N)} + \mathbb{1}}{2} - \mathbb{1}. \quad (48)$$

Note that for measuring  $P'$  only two local measurement settings are needed.

Let us see how good this lower bound is for the noisy GHZ state  $\varrho(p_{\text{noise}})$  defined in Eq. (15). For this state we have

$$F(p_{\text{noise}}) = 1 - p_{\text{noise}}(1 - 2^{-N}),$$

$$F'(p_{\text{noise}}) = 1 - p_{\text{noise}}(3/2 - 2^{-(N-1)}). \quad (49)$$

The difference is  $\Delta F \approx p_{\text{noise}}/2$  for large  $N$ . Bounds can be obtained similarly for the fidelity with respect to the cluster state based on

$$|C_N\rangle\langle C_N| \geq \frac{1}{2} - \frac{1}{2}\mathcal{W}^{(C_N)} \quad (50)$$

### D. Witnesses for mixed states

In an experiment, after detecting entanglement in the prepared state, one might be interested to measure and drop one of the qubits and investigate the state obtained this way. Here we assume that we do not know the measurement result thus

the system is in a mixed state corresponding to the reduced density matrix of the remaining qubits. We will show with an example that witnesses can easily be derived also for this mixed state.

Let us consider a concrete example, namely, measuring a qubit of the four-qubit cluster state.

**Example 1:** The witness,

$$\mathcal{W}^{(\varrho_3)} := \mathbb{1} - Z^{(1)}Z^{(2)} - X^{(1)}X^{(2)}Z^{(3)} \quad (51)$$

detects entanglement around the state  $\varrho_3$  which is obtained from the four-qubit cluster state

$$|C'_4\rangle := |0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle \quad (52)$$

after the fourth qubit is measured. Note that for  $|C'_4\rangle$  we used a local transformation in order to be able to present the cluster state in a convenient form in the  $Z$  basis.

*Proof:* After measuring the fourth qubit, the three-qubit mixed state is

$$\begin{aligned} \varrho_3 &:= \frac{1}{2}(|\xi^+\rangle\langle\xi^+| + |\xi^-\rangle\langle\xi^-|), \\ |\xi^+\rangle &:= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle, \\ |\xi^-\rangle &:= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes |1\rangle. \end{aligned} \quad (53)$$

Note that  $\varrho_3$  is biseparable, i.e., the third qubit is unentangled from the first two.

Now we will determine the stabilizer of  $\varrho_3$ . The stabilizers of states  $|\xi^\pm\rangle$ , given with their generators, are  $\mathcal{S}^{(\xi^\pm)} := \langle Z^{(1)}Z^{(2)}, X^{(1)}X^{(2)}Z^{(3)}, \mp Z^{(3)} \rangle$ . We would like to detect entangled states close to a particular mixture of these two states. Any mixture of states  $|\xi^\pm\rangle$  is stabilized by the common elements of  $\mathcal{S}^{(\xi^\pm)}$ : The stabilizer of these mixed states is  $\mathcal{S}^{(\varrho_3)} = \langle Z^{(1)}Z^{(2)}, X^{(1)}X^{(2)}Z^{(3)} \rangle$ .

Based on that, a stabilizer witness Eq. (51) can now be constructed. The constant in Eq. (51) was determined such that  $\mathcal{W}^{(\varrho_3)}$  detects indeed entangled states only. This can be proved similarly to the derivation of Theorem 1. Witness  $\mathcal{W}^{(\varrho_3)}$  needs two measurement settings and tolerates noise if  $p_{\text{noise}} < 1/2$ .  $\square$

### E. Entanglement witnesses with nonlocal stabilizing operators

There are states which do not fit the stabilizer formalism, however, it is still possible to find a simpler witness than the one obtained by decomposing the projector. As an example let us look at the  $W$  state  $|W_3\rangle = (|100\rangle + |010\rangle + |001\rangle)/\sqrt{3}$ . For this state, the projector-based witness is known to be

$$\tilde{\mathcal{W}}^{(W_3)} = \frac{2}{3}\mathbb{1} - |W_3\rangle\langle W_3|. \quad (54)$$

It tolerates noise if  $p_{\text{noise}} < 8/21 \approx 0.38$  and measuring a local decomposition of this witness requires five measurement settings [15]. In this section we will present witnesses for the  $|W_3\rangle$  state which need only three and two measurement settings, respectively.

What is new with the stabilizing operators of  $|W_3\rangle$ ? Clearly, we must leave the requirement that these operators should be a tensor product of single-qubit operators. Now the stabilizing operators must be allowed to be the sum of several such locally measurable terms.

A set of stabilizing operators with simple local decomposition can be found in the following way. Let us assume that we create the  $|W_3\rangle$  state from state  $|000\rangle$  using a unitary dynamics  $U$ . The generators of the stabilizer for  $|000\rangle$  are

$$S_k^{(000)} := Z^{(k)} \quad \text{for } k = 1, 2, 3. \quad (55)$$

Hence one can get the generators for a group of operators which stabilize  $|W_3\rangle$ ,

$$S_k^{(W_3)} = US_k^{(000)}U^\dagger. \quad (56)$$

Let us try to find  $U$ . It must fulfill  $|W_3\rangle = U|000\rangle$ , i.e., written in the  $Z^{(k)}$  product basis we must have

$$\frac{1}{\sqrt{3}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = [u_1 u_2 \cdots u_8] \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \quad (57)$$

Hence,  $u_1$  can be obtained. The other columns of  $U$  are not determined by Eq. (57) and constrained only by requiring that  $U$  is unitary (i.e., the columns of the matrix must be orthonormal to each other). Thus  $U$  is not unique. A possible choice for a  $U$  fulfilling Eq. (57) is

$$U := \frac{1}{\sqrt{3}}(X^{(1)}Z^{(2)} + X^{(2)}Z^{(3)} + Z^{(1)}X^{(3)}). \quad (58)$$

The generators of a group of stabilizing operators can be obtained based on Eq. (56),

$$S_1^{(W_3)} := \frac{1}{3}(Z^{(1)} + 2Y^{(1)}Y^{(2)}Z^{(3)} + 2X^{(1)}Z^{(2)}X^{(3)}),$$

$$S_2^{(W_3)} := \frac{1}{3}(Z^{(2)} + 2Z^{(1)}Y^{(2)}Y^{(3)} + 2X^{(1)}X^{(2)}Z^{(3)}),$$

$$S_3^{(W_3)} := \frac{1}{3}(Z^{(3)} + 2Y^{(1)}Z^{(2)}Y^{(3)} + 2Z^{(1)}X^{(2)}X^{(3)}). \quad (59)$$

These three stabilizing operators uniquely define the  $W$  state. Again, by multiplying them with each other, other stabilizing operators can be found. However, with the exception of  $S_1^{(W_3)}S_2^{(W_3)}S_3^{(W_3)} = -Z^{(1)}Z^{(2)}Z^{(3)}$ , they are all nonlocal.

Now let us try to create an entanglement witness which detects genuine multi party entanglement, but is still easier to measure than the projector-based witness  $\tilde{\mathcal{W}}^{(W_3)}$ . Consider the following witness constructed from some of the elements of the group generated by  $S_k^{(W_3)}$ ,

$$\begin{aligned} \mathcal{W} = & c_0 \mathbb{1} - S_1^{(W_3)} S_2^{(W_3)} - S_2^{(W_3)} S_3^{(W_3)} - S_1^{(W_3)} S_3^{(W_3)} \\ & - c_1 S_1^{(W_3)} S_2^{(W_3)} S_3^{(W_3)}, \end{aligned} \quad (60)$$

where  $c_0$  and  $c_1$  are positive constants. The expectation value of  $\mathcal{W}$  is minimal for the  $W$  state. Constants  $c_0$  and  $c_1$  must be determined such that for some  $\alpha > 0$  we have  $\mathcal{W} - \alpha \tilde{\mathcal{W}}^{(W_3)} \geq 0$ , and also we have the possible best noise tolerance. Thus we have the following.

**Theorem 8:** A witness detecting genuine three-qubit entanglement around a  $|W_3\rangle$ -state is

$$\begin{aligned} \mathcal{W}^{(W_3)} := & \frac{11}{3} \mathbb{1} + 2Z^{(1)}Z^{(2)}Z^{(3)} - \frac{1}{3} \sum_{k \neq l} (2X^{(k)}X^{(l)} + 2Y^{(k)}Y^{(l)} \\ & - Z^{(k)}Z^{(l)}). \end{aligned} \quad (61)$$

It requires three measurement settings and tolerates noise if  $p_{\text{noise}} < 4/15 \approx 0.27$ .

One can also leave out the  $Z^{(k)}$  terms. The following entanglement witness detects genuine three-qubit entanglement close to a  $|W_3\rangle$ -state:

$$\begin{aligned} \mathcal{W}' := & (1 + \sqrt{5}) \mathbb{1} - X^{(1)}X^{(2)} - X^{(2)}X^{(3)} - X^{(1)}X^{(3)} - Y^{(1)}Y^{(2)} \\ & - Y^{(2)}Y^{(3)} - Y^{(1)}Y^{(3)}. \end{aligned} \quad (62)$$

This witness requires the measurement of two settings and tolerates noise if  $p_{\text{noise}} < (3 - \sqrt{5})/4 \approx 0.19$ . The proof is given in Appendix C.

#### IV. CRITERIA USING VARIANCES AND UNCERTAINTY RELATIONS

Let us now explain, how criteria in terms of variances can be derived, using uncertainty relations [31–33]. In Ref. [32] the following recipe was presented for the derivation of such criteria, called the local uncertainty relations (LURs). Consider a bipartite quantum system and let  $A_i$  be some observables on one party, fulfilling a bound

$$\sum_i \delta^2(A_i) \geq U_A \quad (63)$$

for all states on this party. Here,  $\delta^2(A_i) = \langle A^2 \rangle - \langle A \rangle^2$  denotes the variance of the state. This inequality is an uncertainty relation for the  $A_i$ , with  $U_A > 0$  iff the observables  $A_i$  have no common eigenstates. Let us assume that we have also observables  $B_i$  on the second system, fulfilling a similar bound  $\sum_i \delta^2(B_i) \geq U_B$ . Then, we may look at the observables  $M_i = A_i \otimes \mathbb{1} + \mathbb{1} \otimes B_i$  on the composite system. As it was shown in Ref. [32] for separable states

$$\sum_i \delta^2(M_i) \geq U_A + U_B \quad (64)$$

must hold, and a violation of this bound implies that the state is entangled.

Now we show how the witness  $\mathcal{W}_m^{(\text{GHZ}_N)}$  in Eq. (11) for GHZ states can be improved using nonlinear terms.

**Theorem 9:** Let us define

$$A_1 = X^{(1)}X^{(2)} \dots X^{(k)},$$

$$A_2 = Z^{(k)},$$

$$B_1 = -X^{(k+1)}X^{(k+2)} \dots X^{(N)},$$

$$B_2 = -Z^{(k+1)}, \quad (65)$$

for  $k=1, 2, \dots, N-1$ . Using these operators, the following necessary condition for separability can be given

$$1 - \langle S_1^{(\text{GHZ}_N)} \rangle - \langle S_{k+1}^{(\text{GHZ}_N)} \rangle - \frac{1}{2} (\langle A_1 + B_1 \rangle^2 + \langle A_2 + B_2 \rangle^2) \geq 0. \quad (66)$$

*Proof:* For the uncertainties of observables  $A_k$  and  $B_k$ , one has the bounds

$$\delta^2(A_1) + \delta^2(A_2) \geq 1,$$

$$\delta^2(B_1) + \delta^2(B_2) \geq 1. \quad (67)$$

Knowing that  $\langle X^{(k)} \rangle^2 + \langle Z^{(k)} \rangle^2 \leq 1$ , which implies that  $\delta^2(X^{(k)}) + \delta^2(Z^{(k)}) \geq 1$  these bounds should not be a surprise. A detailed proof which relies on the fact that  $A_1$  and  $A_2$  anticommute, is given in Appendix C. From this and the method of the LURs Eq. (66) follows.  $\square$

Equation (66) is a nonlinear necessary condition for separability. It can be considered as a nonlinear ‘‘refinement’’ of  $\mathcal{W}_m^{(\text{GHZ}_N)}$  in Eq. (11), which improves the witness by subtracting the squares of some expectation values. The fact that LURs can sometimes improve entanglement witnesses was, for bipartite systems, first observed in Ref. [34]. There, the magnitude of the improvement for a special case was also investigated numerically. In the given case for GHZ states it is important to note that the LUR does not improve the noise tolerance, when the GHZ state is mixed with white noise. This is due to the fact that for the totally mixed state as well as for the GHZ state the squared mean values in Eq. (66) vanish. However, there are many states which are not of this form and which are detected by the LUR and not by the witness.

In fact, many of the witnesses from the preceding sections can be improved via the method presented above. For instance, one may add the extra observables  $A_3 = X^{(1)}X^{(2)} \dots X^{(k-1)}Y^{(k)}$ ,  $B_3 = -Y^{(k+1)}X^{(k+2)} \dots X^{(N)}$  to the observables  $A_1, \dots, B_2$  from above. Then  $\delta^2(A_1) + \delta^2(A_2) + \delta^2(A_3) \geq 2$  and the same bound holds for the  $B_i$ . This leads to the separability criterion

$$\begin{aligned} 1 - \langle S_1^{(\text{GHZ}_N)} \rangle - \langle S_m^{(\text{GHZ}_N)} \rangle - \langle S_1^{(\text{GHZ}_N)} S_m^{(\text{GHZ}_N)} \rangle - \frac{1}{2} (\langle A_1 + B_1 \rangle^2 \\ + \langle A_2 + B_2 \rangle^2 + \langle A_3 + B_3 \rangle^2) \geq 0 \end{aligned} \quad (68)$$

which improves the witness of Eq. (13). Also the witness in Eq. (36) can be improved using the same methods, leading to the separability condition

$$1 - \langle S_k^{(C_N)} \rangle - \langle S_{k+1}^{(C_N)} \rangle - \frac{1}{2} \langle Z^{(k-1)} X^{(k)} - Z^{(k+1)} \rangle^2 - \frac{1}{2} \langle Z^{(k)} - X^{(k+1)} Z^{(k+2)} \rangle^2 \geq 0, \quad (69)$$

and the witness for graph states can be improved in a similar manner.

To conclude, it turned out that LURs can improve the presented witnesses which were designed for ruling out full separability. The witnesses for the detection of genuine multipartite entanglement cannot be so simply improved, mainly for two reasons. First, LURs are specially designed for bipartite systems, and no generalization to multipartite systems is known so far. Second, according to our definition of multipartite entanglement a state which is a convex combination of states which are biseparable with respect to different partitions is also biseparable. This implies that it is not enough to show that a state is biseparable with respect to each partition in order to show that it is multipartite entangled. However, if one defines a state to be multipartite entangled if it is not biseparable with respect to any partition (as it is done sometimes in the literature, see, e.g., Ref. [35]) then LURs can be used to detect multipartite entanglement by ruling out biseparability for every bipartite split (as proposed in Ref. [32]).

## V. CRITERIA USING ENTROPIC UNCERTAINTY RELATIONS

Let us now discuss another possibility of deriving separability criteria in terms of uncertainty relations, namely criteria based on entropic uncertainty relations. As we will see, the stabilizer formalism allows us to formulate easily such criteria, however, they are not as strong as the witnesses or the variance based criteria.

The recipe to derive such criteria was described in Ref. [33] and goes as follows: If we have an observable  $M$  we can define  $\mathcal{P}(M)_\varrho = (p_1, \dots, p_n)$  as the probability distribution of the different outcomes for measuring  $M$  in the state  $\varrho$ . One can characterize the uncertainty of this measurement by taking the entropy of this probability distribution, i.e., by defining  $H(M) := H(\mathcal{P}(M)_\varrho)$ . Here, we only consider the entropy to be the standard Shannon entropy  $H(\mathcal{P}) := -\sum_k p_k \ln(p_k)$ , however, a more general entropy like the Tsallis entropy may also be used. Given two observables  $M$  and  $N$  which do not share a common eigenstate, there must exist a strictly positive constant  $C$  such that  $H(M) + H(N) \geq C$  holds. The difficulty in this so-called entropic uncertainty relation (EURs) lies in the determination of  $C$ . For results on this problem see Refs. [36,37]. For the detection of entanglement, the following result has been proved [33]: Let  $A_1, A_2$  and  $B_1, B_2$  be observables with nonzero eigenvalues on Alice's (respectively, Bob's) space obeying an EUR of the type

$$H(A_1) + H(A_2) \geq C \quad (70)$$

or the same bound for  $B_1, B_2$ . If  $\varrho$  is separable, then

$$H(A_1 \otimes B_1)_\varrho + H(A_2 \otimes B_2)_\varrho \geq C \quad (71)$$

holds. For entangled states this bound can be violated, since  $A_1 \otimes B_1$  and  $A_2 \otimes B_2$  might be degenerate and have a common entangled eigenstate.

In order to apply this scheme to the detection of entanglement in the stabilizer formalism we must recall some more facts. Assume that we have two observables of the form  $M = \sum \mu_i P_i$  and  $N = \sum \nu_j Q_j$  where the  $P_i, Q_j$  are the projectors on the eigenspaces. Here, we do not require  $M$  and  $N$  to be nondegenerate, i.e., the  $P_i$  and  $Q_j$  may have ranks larger than one. In this situation, it was shown in Ref. [37] that for these observables the EUR,

$$H(M) + H(N) \geq -\ln \max_{ij} Z_{ij} \quad (72)$$

holds, where  $Z_{ij} = \|P_i Q_j\| = \max_{|\psi\rangle} \sqrt{\langle \psi | (P_i Q_j)^\dagger (P_i Q_j) | \psi \rangle}$  is the norm of the operator  $P_i Q_j$ . This has two consequences. First, it follows immediately that for one qubit

$$H(X) + H(Y) \geq \ln(2), \quad (73)$$

holds, and similar relations hold for  $Y, Z$  etc. Second, if  $A$  is an observable consisting of Pauli measurements on  $N$  qubits, e.g.,  $A = X^{(1)} Y^{(2)} \dots Z^{(N)}$ , then for  $N+1$  qubits the EUR

$$H(A \otimes X^{(N+1)}) + H(\mathbb{1}_{2N} \otimes Y^{(N+1)}) \geq \ln(2), \quad (74)$$

holds. Here  $\mathbb{1}_{2N}$  denotes the identity on the first  $N$  qubits. Similar result hold also, if the observables on the qubit  $N+1$  are replaced by other Pauli matrices. Equation (74) can directly be proved from Eq. (72) by identifying the corresponding  $P_i$  and  $Q_j$ .

Armed with these insights, we can formulate now entropic criteria for stabilizer states.

**Theorem 10:** For GHZ and cluster states, respectively, the following necessary conditions for biseparability can be given using entropic uncertainties

$$\sum_{k=1}^N H(S_k^{(\text{GHZ}_N)}) \geq \ln(2), \quad (75)$$

$$\sum_{k=1}^N H(S_k^{(C_N)}) \geq \ln(2). \quad (76)$$

Any state violating these conditions is genuine  $N$ -qubit entangled. Note that for GHZ and cluster states the left-hand side of Eq. (75) and Eq. (76), respectively, is zero.

*Proof:* To prove Eq. (75) it suffices to look at pure biseparable states, since the entropy is concave in the state. So let us assume that  $|\psi\rangle = |a\rangle|b\rangle$  is a biseparable state. For definiteness, we assume that  $|a\rangle$  is a state of the qubits  $1, 2, \dots, k$  and  $|b\rangle$  is a state of the qubits  $k+1, k+2, \dots, N$ ; the proof of the other cases is similar. In order to apply the recipe from above, we must show that on the first  $k$  qubits the EUR

$$H(X^{(1)} \dots X^{(k)}) + \sum_{i=2}^k H(S_k^{(\text{GHZ}_N)}) + H(Z^{(k)}) \geq \ln(2) \quad (77)$$

holds. This is easy to see, since  $H(X^{(1)} \dots X^{(k)}) + H(Z^{(k)}) \geq \ln(2)$  is valid, due to Eq. (74). Similar ideas can be used for cluster states. The proof is essentially the same as for the GHZ state. Similar statements can also be derived for arbitrary graph states.  $\square$

As we have seen, it is quite straightforward to formulate entropic criteria for stabilizer states. However, one should

clearly state that the criteria in the presented form are not very strong. For instance, the criterion in Eq. (75) detects states mixed with white noise only for  $p_{\text{noise}} < 0.123$  for  $N=3$  and  $p_{\text{noise}} < 0.083$  for  $N=4$ . The robustness to noise can, as shown for some two-qubit cases in Ref. [33], be improved, if other entropies than the Shannon entropy are used. However, for these entropies no such general bound as in Eq. (72) is known. So only a better understanding of the EURs can help to explore the full power of the entropic criteria.

## VI. CONCLUSIONS

In summary, we have shown that stabilizer theory can be used very efficiently to derive sufficient criteria for entanglement. Knowing some stabilizing operators of a state allows for an easy derivation of a plethora of entanglement criteria which detect states in the vicinity of the state. This holds for linear as well as nonlinear criteria, and for the different types of entanglement in the multipartite setting. We also noted that the resulting criteria exhibit several interesting features: They all are easy to implement in experiments, some of them have interesting connections to Bell inequalities, others are nonlinear improvements of witnesses.

A natural continuation of the present work lies in the systematic extension of the presented ideas to states which do not fit directly in the stabilizer formalism. GHZ, cluster and graph states are not the only multipartite states which are interesting from the viewpoint of quantum information science. As we have shown in the example of the  $W$  state, also for states outside the stabilizer formalism similar ideas can be applied by identifying their nonlocal stabilizing operators. Exploring this direction might help to clarify the structure of multipartite entanglement.

## ACKNOWLEDGMENTS

The authors thank M. Aspelmeyer, H.J. Briegel, D. Bruß, Č. Brukner, J.I. Cirac, T. Cubitt, J. Eisert, J.J. García-Ripoll, P. Hyllus, M. Lewenstein, M. Van den Nest, A. Sanpera, M. Seevinck, J. Uffink, M.M. Wolf, and M. Żukowski for useful discussions. The authors also acknowledge the support of the DFG (Graduiertenkolleg 282), the Marie Curie Individual Fellowship of the European Union (Grant No. MEIF-CT-2003-500183), the EU projects RESQ and QUPRODIS, and the Kompetenznetzwerk Quanteninformationsverarbeitung der Bayerischen Staatsregierung.

## APPENDIX A: THE STABILIZER GROUP

We summarize the properties of the stabilizing operators of a given  $N$ -qubit quantum state  $|\Psi\rangle$ . These are locally measurable operators  $\tilde{S}$  for which  $\tilde{S}|\Psi\rangle=|\Psi\rangle$ . They have  $\pm 1$  eigenvalues. For states considered in this paper (GHZ, cluster and graph states) they are tensor products of Pauli spin matrices.

Let us now list the properties of the set  $\mathcal{S}$  containing the stabilizing operators of  $\Psi$ . For any  $\tilde{S}_1, \tilde{S}_2, \tilde{S} \in \mathcal{S}$ ,

$$\begin{aligned}\tilde{S}_1\tilde{S}_2 &\in \mathcal{S}, \\ [\tilde{S}_1, \tilde{S}_2] &= 0, \\ \tilde{S}^2 &= 1.\end{aligned}\tag{A1}$$

Now it is clear that the elements of  $\mathcal{S}$  form a commutative (Abelian) group. It is called the stabilizer. One of its  $2^N$  elements is given as

$$\tilde{S}_k := \prod_{l=1}^N (S_l)^{\alpha_{kl}},\tag{A2}$$

where  $\alpha_{kl}$  is the  $l$ th digit of the binary number (i.e.,  $N$ -tuple of  $\{0,1\}$ ) corresponding to the number  $k \in \{0, 1, 2, \dots, 2^N - 1\}$ . Operators  $\{S_l\}_{l=1}^N$  are the generators of the group. If  $\alpha_{kl}=1$  then we say that  $\tilde{S}_k$  contains generator  $S_l$  in its definition of the type Eq. (A2).

## APPENDIX B: PROOF OF OPTIMALITY FOR THE GHZ AND CLUSTER STATE WITNESSES

In this section we will prove that the GHZ and cluster state witnesses defined in Eq. (23) and Eq. (41), respectively, are optimal. That is, it is not possible to find a stabilizer witness  $\mathcal{W}$  which needs only two measurement settings, has the property that for some  $\alpha > 0$  we have  $\mathcal{W} - \alpha\tilde{\mathcal{W}} \geq 0$ , and has better noise tolerance than the witnesses presented in this paper. Here  $\tilde{\mathcal{W}}$  denotes a projector-based witness.

Before presenting the proof, let us analyze what we understand on measurement settings. Let us consider operators which can be measured with one measurement setting. These form a group, members of which commute locally (for an explanation of local commuting see Sec. II B). The projector cannot be measured with two settings, since the stabilizing operators cannot be divided into two locally commuting subgroups. So we will find two subgroups, which contain as many stabilizing operators as possible. Let us consider GHZ states first. The largest such subgroup is  $\langle S_2^{(\text{GHZ}_N)}, S_3^{(\text{GHZ}_N)}, \dots, S_N^{(\text{GHZ}_N)} \rangle$ . Here the group is given by the generators. The operators in this group commute locally since they all contain only  $Z^{(k)}$ 's, and neither  $X^{(k)}$ 's nor  $Y^{(k)}$ 's. All the other elements of the stabilizer have the form  $S_1^{(\text{GHZ}_N)} Q$  where  $Q \in \langle S_2^{(\text{GHZ}_N)}, S_3^{(\text{GHZ}_N)}, \dots, S_N^{(\text{GHZ}_N)} \rangle$ . All these operators contain only  $X^{(k)}$ 's and  $Y^{(k)}$ 's, and do not contain  $Z^{(k)}$ 's. None of these commute locally with any other element of the stabilizer, except with the identity. Thus the other subgroup can contain only one such operator and the identity.

Now the two subgroups corresponding to the two local settings are

$$\begin{aligned}\mathcal{L}_1^{(\text{GHZ}_N)} &= \{S_1^{(\text{GHZ}_N)} Q, 1\}, \\ \mathcal{L}_2^{(\text{GHZ}_N)} &= \langle S_2^{(\text{GHZ}_N)}, S_3^{(\text{GHZ}_N)}, \dots, S_N^{(\text{GHZ}_N)} \rangle.\end{aligned}\tag{B1}$$

Any operator which is a linear combination of operators in  $\mathcal{L}_1$  can be measured by the first measurement setting. Simi-

larly, any operator which is linear combination of operators in  $\mathcal{L}_2$  can be measured by the second measurement setting. It is an important question whether there is another choice for  $\mathcal{L}_1$  and  $\mathcal{L}_2$ . In order to answer this, we must remember that we want to detect genuine  $N$ -qubit entanglement. Thus we must find a witness for which  $\langle \mathcal{W} \rangle$  has a unique minimum for GHZ states. For that, we must be able to measure a complete set of generators with the two settings. (For more details, see Sec. II D.) It can be seen that no other two subgroups can be found which fulfill this requirement. For simplicity, in the following we choose  $Q=1$ . The two measurement settings corresponding to this case are shown in Fig. 1(a). Choosing  $Q$  to be not the identity would not change our argument and would not lead to witnesses with better noise tolerance than the ones presented here.

As discussed before, the eigenvectors of the generators  $\{S_k^{(\text{GHZ}_N)}\}_{k=1}^N$  of the stabilizer form a complete basis (GHZ basis). We will use it to represent states of the  $N$ -qubit Hilbert space. Let us use  $N$ -tuples of  $\{0, 1\}$  for labeling the basis states. If the  $k$ th digit is 0 (1) then for the basis state  $\langle S_k^{(\text{GHZ}_N)} \rangle = +1$  ( $\langle S_k^{(\text{GHZ}_N)} \rangle = -1$ ). Now  $[[00 \cdots 0]]$  is the GHZ state. Here square brackets are used in order to draw our attention to the fact that the GHZ basis is not a product basis and the  $N$  digits do not correspond to a physical partitioning of the system.

Next, let us use this labeling to order the  $2^N$  basis states from  $[[00 \cdots 0]]$  to  $[[11 \cdots 1]]$ . What is the matrix form of  $S_1^{(\text{GHZ}_N)}$  in this basis? It is clearly diagonal. Moreover, it must give  $+1$  and  $-1$  expectation values for states of the form  $[[0s_2s_3 \cdots s_N]]$  and  $[[1s_2s_3 \cdots s_N]]$ , respectively. Knowing this, it must have the form  $\text{diag}(+1, -1) \otimes \mathbb{1}_{2^{N-1}}$ . Here  $\text{diag}$  denotes a diagonal matrix and the size of the identity is indicated by a subscript. Note again that the tensor product does not correspond to a physical partitioning of the system. However, the matrix form of  $S_1^{(\text{GHZ}_N)}$  in the GHZ basis is the same as the matrix form of  $Z^{(1)}$  in the product basis. Similarly, the matrix form of  $S_k^{(\text{GHZ}_N)}$  in the GHZ basis is the same as the matrix form of  $Z^{(k)}$  in the product basis.

After these considerations about measurement settings, let us start our proof. Let us find out how operators measurable by the first setting look like in the GHZ basis. Now it is clear that such operators must have the form  $A \otimes \mathbb{1}_{d_2}$  where matrix  $A$  is of size  $d_1=2$  and  $d_2=2^{(N-1)}$ . Operators measurable by the second setting have the form  $\mathbb{1}_{d_1} \otimes B$  in this basis. Here  $B$  is of size  $d_2$ . We construct our witness from two operators corresponding to the two measurement settings as

$$\mathcal{W} := c \mathbb{1}_{d_1} \otimes \mathbb{1}_{d_2} - A \otimes \mathbb{1}_{d_2} - \mathbb{1}_{d_1} \otimes B, \quad (\text{B2})$$

where  $c$  is a constant. Now we will find an operator  $\mathcal{W}$  for which for some  $\alpha > 0$  we have  $\mathcal{W} - \alpha \tilde{\mathcal{W}}^{(\text{GHZ}_N)} \geq 0$  and which is optimal from the point of view of noise tolerance. Without the loss of generality, we set  $\alpha=2$ . Both  $\mathcal{W}$  and the projector witness  $\tilde{\mathcal{W}}^{(\text{GHZ}_N)}$  are diagonal in the GHZ basis. Hence from the condition  $\mathcal{W} \geq 2\tilde{\mathcal{W}}^{(\text{GHZ}_N)}$ , the following constraints on the diagonal elements  $a_k$  and  $b_k$  of  $A$  and  $B$ , respectively, can be obtained

$$c - a_1 - b_1 \geq -1,$$

$$c - a_k - b_l \geq +1, \quad k \geq 2; l \geq 1,$$

$$c - a_k - b_l \geq +1, \quad k \geq 1; l \geq 2. \quad (\text{B3})$$

The maximal noise  $p_{\text{limit}}$  tolerated by our witness can be computed as given in Eq. (15). For this formula we must use

$$\langle \text{GHZ}_N | \mathcal{W} | \text{GHZ}_N \rangle = c - a_1 - b_1,$$

$$2^{-N} \text{Tr}(\mathcal{W}) = c - \frac{1}{d_1} \sum_{k=1}^{d_1} a_k - \frac{1}{d_2} \sum_{k=1}^{d_2} b_k. \quad (\text{B4})$$

In order to find the optimal witness, constant  $c$  and the elements of  $A$  and  $B$  must be chosen such that the noise tolerance  $p_{\text{limit}}$  is maximized, under the constraints Eq. (B3). This is the case if all the three inequalities in Eq. (B3) are saturated. Thus we obtain  $c=3$ ,  $a_1=b_1=2$ ,  $a_k=b_k=0$  for  $k \geq 2$  and

$$p_{\text{limit}} = \frac{1}{4 - 2/d_1 - 2/d_2}. \quad (\text{B5})$$

The witness obtained this way coincides with the witness given in Eq. (23).

Now let us turn to cluster states. We will need the following lemma.

*Lemma 1:* Let us consider the following three subsets of the stabilizer  $\mathcal{S}^{(C_N)}$ :

$$\mathcal{P}_1 := \{A \in \mathcal{S}^{(C_N)} : A \text{ contains } S_l^{(C_N)}\} \quad (\text{B6})$$

and does not contain  $S_{l+1}^{(C_N)}$ ,

$$\mathcal{P}_2 := \{A \in \mathcal{S}^{(C_N)} : A \text{ contains } S_{l+1}^{(C_N)}\} \quad (\text{B7})$$

and does not contain  $S_l^{(C_N)}$ ,

$$\mathcal{P}_3 := \{A \in \mathcal{S}^{(C_N)} : A \text{ contains both } S_{l+1}^{(C_N)} \text{ and } S_l^{(C_N)}\}. \quad (\text{B8})$$

If a local measurement setting makes it possible to measure an operator in  $\mathcal{P}_n$ , then it does not make it possible to measure any operator in  $\mathcal{P}_m$  for  $m \neq n$ .

*Proof:* First let us prove our Lemma for  $l=1$ . In Table I(a) we show for some elements of the stabilizer which measurements on qubits (1) and (2) are needed to measure them. Here for brevity superscript  $C_N$  is omitted. A binary pattern indicates whether a given element of the stabilizer contains or does not contain generators  $S_1$ ,  $S_2$ , and  $S_3$ . For example, entry 100 represents operators which contain  $S_1$  and do not contain  $S_{2/3}$ . Such operators are, for example,  $S_1$ ,  $S_1S_4$  and  $S_1S_4S_6$ . In the second row of the table  $X$ ,  $Y$ , and  $Z$  represent Pauli spin matrices. 1 indicates that no measurement is needed on the given qubit. For example, in the column of 101 entry X1 indicates that for measuring  $S_1S_3=X^{(1)}X^{(3)}Z^{(4)}$  an  $X$  measurement is needed for qubit (1) and no measurements are needed for qubit (2)

The left two columns correspond to operators of set  $\mathcal{P}_1$  which contain  $S_1$  and do not contain  $S_2$ . The middle two

TABLE I. (a) Local measurements needed for measuring some elements of the stabilizer on qubits (1) and (2) for a cluster state. The binary pattern indicates presence or absence of generators  $S_1$ ,  $S_2$  and  $S_3$ . (b) Local measurements needed for qubits  $k$  and  $k+1$  where  $k \geq 2$ . The binary pattern indicates presence or absence of generators  $S_{k-1}$ ,  $S_k$ ,  $S_{k+1}$  and  $S_{k+2}$ . For details see text.

	(a)					
$S_1 S_2 S_3$	100	101	010	011	110	111
$\mathcal{O}^{(1)} \mathcal{O}^{(2)}$	XZ	X1	ZX	ZY	YY	YX
	(b)					
$S_{k-1} S_k S_{k+1} S_{k+2}$	0100	0101	1100	1101		
$\mathcal{O}^{(k)} \mathcal{O}^{(k+1)}$	XZ	X1	YZ	Y1		
$S_{k-1} S_k S_{k+1} S_{k+2}$	0010	0011	1010	1011		
$\mathcal{O}^{(k)} \mathcal{O}^{(k+1)}$	ZX	ZY	1X	1Y		
$S_{k-1} S_k S_{k+1} S_{k+2}$	0110	0111	1110	1111		
$\mathcal{O}^{(k)} \mathcal{O}^{(k+1)}$	YY	YX	XY	XX		

columns correspond to operators of set  $\mathcal{P}_2$  which contain  $S_2$  and do not contain  $S_1$ . The right two columns correspond to operators of set  $\mathcal{P}_3$  which contain both  $S_1$  and  $S_2$ . Based on the table we see that only 100 and 101 have compatible measurements for the first two qubits, XZ and X1, respectively. An operator of  $\mathcal{P}_n$  cannot be measured together with any operator of  $\mathcal{P}_m$  for  $m \neq n$ . Thus Lemma 1 works for  $l = 1$ .

Now let us prove, that if our Lemma is true for  $l = k - 1$ , then it is true for  $l = k$ . In Table I(b) the measurements for qubits  $k$  and  $k+1$  for a particular set of operators are shown. An entry of the table, let us say 0100, represents all operators which contain  $S_k$ , and does not contain  $S_{k-1}$ ,  $S_{k+1}$ , and  $S_{k+2}$ . Now the measurements for qubits  $k$  and  $k+1$  for 0101 seem to be compatible with the measurements for 1010, 1011, 1110, and 1111. However, we assumed that our Lemma is true for  $l = k - 1$ . Thus 0101 and 1010 cannot be measured with the same setting. For the same reason, 0101 and 1011 cannot be measured with the same setting. Taking the other operators having compatible measurements for qubits  $k$  and  $k+1$ , we find that measuring them with the same setting is prohibited by our lemma for  $l = k - 1$ .

Lemma 1 limits the size of the subgroup of the stabilizer of  $|C_N\rangle$  measurable by one measurement setting. Namely, for even  $N$  the largest subgroup can be given with  $N/2$  generators, while for odd  $N$  the maximum is  $(N+1)/2$ . Two subgroups of the stabilizer allowing for the measurement of a complete set of generators are

$$\begin{aligned} \mathcal{L}_1^{(C_N)} &:= \langle S_1^{(C_N)}, S_3^{(C_N)}, S_5^{(C_N)}, \dots \rangle, \\ \mathcal{L}_2^{(C_N)} &:= \langle S_2^{(C_N)}, S_4^{(C_N)}, S_6^{(C_N)}, \dots \rangle. \end{aligned} \quad (\text{B9})$$

Now  $d_1 = d_2 = 2^{N/2}$  for even  $N$  and  $d_{1/2} = 2^{(N \pm 1)/2}$  for odd  $N$ . There are other possibilities for the two measurement settings, however, they do not give a better noise tolerance since the optimal noise tolerance Eq. (B5) depends only on  $d_1$  and  $d_2$ , and does not depend on which elements of the stabilizer are measured by the two settings. Optimization

leads to witness (41) constructed using two projectors, corresponding to the two settings. Thus witness given in Eq. (41) is also optimal.

### APPENDIX C: SOME TECHNICAL CALCULATIONS

*Calculations for the  $W$  state*—Here, we prove that Eq. (62) describes an entanglement witness detecting states with three-qubit entanglement around a  $W$  state. Note that this witness was constructed independently from the stabilizer theory. The proof is also useful in general, since it shows how to find the minimum of an operator expectation value for biseparable states analytically.

Let us first assume (1)(23) biseparability. Then for a state of the form  $\Psi = \Psi_1 \otimes \Psi_{23}$ ,

$$\begin{aligned} \langle \mathcal{W}' \rangle &= (1 + \sqrt{5}) - \langle X^{(1)} \rangle \langle X^{(2)} \rangle - \langle X^{(1)} \rangle \langle X^{(3)} \rangle - \langle X^{(2)} X^{(3)} \rangle \\ &\quad - \langle Y^{(1)} \rangle \langle Y^{(2)} \rangle - \langle Y^{(1)} \rangle \langle Y^{(3)} \rangle - \langle Y^{(2)} Y^{(3)} \rangle \\ &= (1 + \sqrt{5}) - \langle X^{(1)} \rangle_1 [\langle X^{(2)} + X^{(3)} \rangle_{23}] \\ &\quad + \langle Y^{(1)} \rangle_1 [\langle Y^{(2)} + Y^{(3)} \rangle_{23}] + [\langle X^{(2)} X^{(3)} + Y^{(2)} Y^{(3)} \rangle_{23}] \\ &= \langle F(x, y) \rangle_{23}, \end{aligned} \quad (\text{C1})$$

where

$$x := \langle X^{(1)} \rangle_1, \quad y := \langle Y^{(1)} \rangle_1. \quad (\text{C2})$$

Here  $\langle \dots \rangle_1$  and  $\langle \dots \rangle_{23}$ , respectively, denote expectation value computed for  $\Psi_1$  and  $\Psi_{23}$ . To be explicit, matrix  $F$ , as the function of two real parameters, is given

$$\begin{aligned} F(x, y) &:= (1 + \sqrt{5})\mathbb{1} - x[X^{(2)} + X^{(3)}] - y[Y^{(2)} + Y^{(3)}] \\ &\quad - [X^{(2)} X^{(3)} + Y^{(2)} Y^{(3)}]. \end{aligned} \quad (\text{C3})$$

Note that operator  $F$  acts on the second and third qubits while its two parameters depend on the state of the first qubit. The expectation value of  $F(x, y)$  can be bounded from below

$$\langle F(x, y) \rangle_{23} \geq \Lambda_{\min}[F(x, y)] = \sqrt{5} - \sqrt{1 + 4(x^2 + y^2)}, \quad (\text{C4})$$

where  $\Lambda_{\min}(F)$  is the smallest eigenvalue of  $F$ . The right-hand side of Eq. (C4) was obtained by finding the matrix eigenvalues analytically. Using  $\langle X^{(1)} \rangle^2 + \langle Y^{(1)} \rangle^2 \leq 1$ , we obtain that  $\langle \mathcal{W}' \rangle$  is bounded from below by

$$\langle \mathcal{W}' \rangle \geq \min_{x^2 + y^2 \leq 1} \{\Lambda_{\min}[F(x, y)]\} = 0. \quad (\text{C5})$$

Thus our witness has a non-negative expectation value for biseparable pure states with partitioning (1)(23). Due to that  $\mathcal{W}'$  is symmetric under the permutation of qubits,  $\langle \mathcal{W}' \rangle \geq 0$  holds also for pure biseparable states with a partitioning (12)(3) and (13)(2). It is easy to see that the bound is also valid for mixed biseparable states. In contrast, for three-qubit entangled states we have  $\langle \mathcal{W}' \rangle \geq \sqrt{5} - 3$ . Among pure states, the equality holds only for  $|W_3\rangle$  and  $|\overline{W}_3\rangle = (|011\rangle + |101\rangle + |110\rangle)/\sqrt{3}$ , and their superpositions.

*Calculations for the LURs described in Sec. IV*—To com-

pute the bounds required for the derivation of the LURs we show the following. Let  $A_i$ , for  $i=1, 2, \dots, n$  be some observables, which anticommute pairwise (i.e.,  $A_i A_j + A_j A_i = 0$  for all  $i \neq j$ ) and which have all  $\pm 1$  eigenvalues (i.e.,  $A_i^2 = 1$  for all  $i$ ). Then  $\sum_{i=1}^n \delta^2(A_i) \geq n-1$ . To show this, it suffices to show that  $\sum_{i=1}^n \langle A_i \rangle^2 \leq 1$ . This can be proved as follows: We take real coefficients  $\lambda_1, \dots, \lambda_n$  with  $\sum_{i=1}^n \lambda_i^2 = 1$ . Then, using the fact

that the  $A_i$  anticommute, we have  $(\sum_{i=1}^n \lambda_i A_i)^2 = \sum_{i=1}^n \lambda_i^2 A_i^2 = \sum_{i=1}^n \lambda_i^2 = 1$ . So, for all states  $|\langle \sum_{i=1}^n \lambda_i A_i \rangle| = |\sum_{i=1}^n \lambda_i \langle A_i \rangle| \leq 1$  holds. Since the  $\lambda_i$  are arbitrary, this implies that the vector of the mean values  $(\langle A_1 \rangle, \langle A_2 \rangle, \dots, \langle A_n \rangle)$  has a length smaller than 1. Thus,  $\sum_{i=1}^n \langle A_i \rangle^2 \leq 1$  must hold. This method can be used to derive all the bounds in Sec. IV.

- 
- [1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001); R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [2] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
- [3] D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena, CA, 1997.
- [4] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999); M. Curty, M. Lewenstein, and N. Lütkenhaus, *ibid.* **92**, 217903 (2004).
- [5] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
- [6] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
- [7] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [8] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005); AIP Conf. Proc. **734**, 234 (2004).
- [9] For detecting nonlocality using the stabilizer formalism see D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997); V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, *ibid.* **71**, 042325 (2005); O. Gühne, G. Tóth, P. Hyllus and H. J. Briegel, quant-ph/0410059 (unpublished).
- [10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996); B. M. Terhal, *ibid.* **271**, 319 (2000); M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000); D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).
- [11] B. M. Terhal, Theor. Comput. Sci. **287**, 313 (2002); O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).
- [12] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
- [13] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe, Nature (London) **404**, 256 (2000).
- [14] Equivalently,  $|\text{GHZ}_N\rangle\langle\text{GHZ}_N| = 2^{-N} \sum_{k=1}^{2^N} \tilde{S}_k^{(\text{GHZ}_N)}$  also holds.
- [15] O. Gühne and P. Hyllus, Int. J. Theor. Phys. **42**, 1001 (2003).
- [16] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
- [17] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
- [18] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [19] N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).
- [20] M. Seevinck and J. Uffink, Phys. Rev. A **65**, 012107 (2002).
- [21] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, Phys. Rev. Lett. **88**, 170405 (2002).
- [22] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature (London) **403**, 515 (2000); see also p. 209 of D. Bouwmeester, A. Ekert and A. Zeilinger, *The Physics of Quantum Information* (Springer, Berlin, 2000).
- [23] The Mermin inequality presented in this paper is maximally violated by the state  $(|0000\dots\rangle + |1111\dots\rangle)/\sqrt{2}$ . The form presented by Mermin in Ref. [18] is maximally violated by  $(|0000\dots\rangle + i|1111\dots\rangle)/\sqrt{2}$ . The two Bell inequalities are equivalent under simple relabeling of variables.
- [24] In a calculation different from ours, K. Nagata *et al.* also obtained the here presented bound for the Mermin inequality in an unpublished work to be found at <http://www.qci.jst.go.jp/eqis02/program/abstract/poster11.pdf>. The bound, while not explicitly stated, can straightforwardly be obtained from K. Nagata, M. Koashi, and N. Imoto, Phys. Rev. Lett. **89**, 260401 (2002).
- [25] S. M. Roy, Phys. Rev. Lett. **94**, 010402 (2005).
- [26] G. Tóth, Phys. Rev. A **69**, 052327 (2004).
- [27] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [28] W. Dür, H. Aschauer, and H. J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
- [29] H. J. Briegel (private communication).
- [30] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004); **70**, 034302 (2004); Phys. Rev. A **71**, 062323 (2005).
- [31] D. Janzing and Th. Beth, Phys. Rev. A **61**, 052308 (2000); L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, *ibid.* **84**, 2726 (2000); A. Sørensen, L.-M. Duan, J. I. Cirac, and P. Zoller, Nature (London) **409**, 63 (2001); G. Tóth, C. Simon, and J. I. Cirac, *ibid.* **68**, 062310 (2003); O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004); V. Giovannetti, Phys. Rev. A **70**, 012102 (2004).
- [32] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
- [33] O. Gühne and M. Lewenstein, Phys. Rev. A **70**, 022316 (2004).
- [34] O. Gühne and M. Lewenstein, AIP Conf. Proc. **734**, 230 (2004).
- [35] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [36] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983); H. Maassen, and J. B. M. Uffink, *ibid.* **60**, 1103 (1988); G.-C. Ghirardi, L. Marinatto, and R. Romano, Phys. Lett. A **317**, 32 (2003).
- [37] M. Krishna and K. R. Parthasarathy, Sankhya, Ser. A **64**, 842 (2002); also available at quant-ph/0110025 (unpublished).