Optimal entanglement witnesses from limited local measurements

Alberto Riccardi, 1,* Dariusz Chruściński, 2 and Chiara Macchiavello 1, 3, 4

Dipartimento di Fisica, University of Pavia, via Bassi 6, 27100 Pavia, Italy.

Institute of Physics, Faculty of Physics, Astronomy and Informatics,
Nicolaus Copernicus University, Grudziadzka 5/7, 87-100 Torun, Poland.

INFN Sezione di Pavia, via Bassi 6, I-27100, Pavia, Italy.

4 CNR-INO, largo E. Fermi 6, I-50125, Firenze, Italy.

We address the problem of optimising entanglement witnesses when a limited fixed set of local measurements can be performed on a bipartite system, thus providing a procedure, feasible also for experiments, to detect entangled states using only the statistics of these local measurements. We completely characterize the class of entanglement witnesses of the form $W = P^{\Gamma}$, where Γ denotes partial transposition, that can be constructed from the measurements of the bipartite operators $\sigma_x \otimes \sigma_x$, $\sigma_y \otimes \sigma_y$ and $\sigma_z \otimes \sigma_z$ in the case of two-qubit systems. In particular, we consider all possible extremal decomposable witnesses within the considered class that can be defined from this set of measurements. Finally, we discuss possible extensions to higher dimension bipartite systems when the set of available measurements is characterized by the generalized Gell-Mann matrices. We provide several examples of entanglement witnesses, both decomposable and indecomposable, that can be constructed with these limited resources.

Introduction. — Entanglement is one of the unique aspects of quantum physics and nowadays it is recognized as a pivotal resource in many quantum information areas. Hence, testing whether a state of a composite system is separable or entangled is a crucial task. A well-known procedure to accomplish this task, without requiring full tomography of the state, uses the notion of entanglement witnesses (EW) [1–3]. An operator W that acts on a bipartite system living in $\mathcal{H}_A \otimes \mathcal{H}_B$ is an EW if and only if W is a block-positive operator, i.e. $\langle \psi_A \otimes \psi_B | W | \psi_A \otimes \psi_B \rangle \geq 0$, but it is not positive, that is, it has at least one negative eigenvalue. Equivalently, W is an EW iff i) $\text{Tr}[W\rho_{sep}] \geq 0$ for all separable states ρ_{sep} , and ii) there exists at least one entangled state ρ_e such that $\text{Tr}[W\rho_e] < 0$. Moreover, a state is entangled iff it is detected by some EW [1]. Several types of EW have been defined and studied (see e.g. [4, 8] for the review). For example an EW is decomposable if $W = A + B^{\Gamma}$, where $A, B \geq 0$ and B^{Γ} denotes a partial transposition. Witnesses which do not allow such decomposition are called indecomposable. The former cannot detect positive partial transpose (PPT) entangled states, while the latter can and therefore they can be useful to detect bound entangled states. In the case of two-qubit systems, since PPT entangled states do not exist, all entanglement witnesses are decomposable, hence they can be always represented as $W = A + B^{\Gamma}$. Moreover, a witness W is optimal if for any $C \geq 0$ an operator W-C is no longer a witness [6]. Optimal EWs are the best entanglement detectors, that is, W is optimal if and only if there is no other witness that detects more quantum entangled states than W

does [6]. Hence optimality has a direct operational meaning. A witness which is not optimal may be optimized via a suitable optimization procedure [6]. It is therefore clear that knowing all optimal EWs one is able to detect all entangled states. Among optimal witnesses there are extremal ones: an W is extremal if for any block-positive D (not collinear with W) an operator W-D is no longer a witness. Extremal witnesses are fully characterised in the class of decomposable EWs: a decomposable EW is extremal if and only if $W = |\psi\rangle\langle\psi|^{\Gamma}$ for some entangled vector $\psi \in \mathcal{H}_A \otimes \mathcal{H}_B$. Characterization of extremal but indecomposable EWs is much more complicated and still open.

In this Letter we address the problem of defining the most general class of EWs given a limited set of measurements. This work fits within the framework of studying the experimental realization of quantum information tasks when only a limited set of resources is available, as for example the estimation of quantum channel capacities [9, 10]. More specifically, we assume that a full tomography of the state of the system is not available, and our knowledge is represented by the statistics of a set of local measurements \mathcal{M} . The goal is to process the classical measurement outcomes in order to find the most general classes of EWs that can be defined with this set of local measurements.

Two qubits. — In this Letter we provide a complete characterization of EWs of the form $W = P^{\Gamma}$ that can be constructed for a two-qubit system by considering only the statistics of $\mathcal{M} = \{\sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\}$. Any 2-qubit entanglement witness W can be represented as follows:

$$W = \sum_{\mu,\nu=0}^{3} T_{\mu\nu} \sigma_{\mu} \otimes \sigma_{\nu}, \tag{1}$$

 $^{*\} alberto.riccardi 01 @universita dipavia.it \\$

with $\sigma_{\mu} \in \{1, \sigma_x, \sigma_y, \sigma_z\}$, and 16 real parameters $T_{\mu\nu}$. Now, having an access to the limited resources \mathcal{M} we consider witnesses with diagonal correlation tensor $T_{kl} = c_k \delta_{kl}$ (k, l = 1, 2, 3) only, that is,

$$W = \alpha \mathbb{1} \otimes \mathbb{1} + \sum_{k=x,y,z} \left(a_k \mathbb{1} \otimes \sigma_k + b_k \sigma_k \otimes \mathbb{1} \right) + \sum_{k=x,y,z} c_k \sigma_k \otimes \sigma_k,$$
 (2)

with real parameters α, a_k, b_k, c_k . This reduces the number of independent parameters from 6 elements $T_{kl} = T_{lk}$ to 3 real parameters c_k . The above form is justified by the fact that the mean values of single qubit operators $\sigma_k \otimes \mathbb{1}$ and $\mathbb{1} \otimes \sigma_k$ for i = x, y, z can be derived by simply ignoring the statistics on one side. Moreover, all the EWs within the class (2) can be also represented as $W = P^{\Gamma} + Q$, with $P, Q \geq 0$. It should be stressed, that even if P and Q do not belong to \mathcal{M} it may happen that $W = P^{\Gamma} + Q$ does [11, 12]. Hereafter, we consider only witnesses within the class (2) that are of the form

$$W = P^{\Gamma}, \tag{3}$$

where P contains only terms from \mathcal{M} . The canonical example of such a witness is provided by the flip operator

$$\mathbb{F} = \frac{1}{2} \Big(\mathbb{1} \otimes \mathbb{1} + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z \Big). \tag{4}$$

As is well known \mathbb{F} witnesses entanglement within a class of Werner states:

$$\rho_W = \frac{1}{2(2-f)} \Big(\mathbb{1} \otimes \mathbb{1} - f \, \mathbb{F} \Big), \quad -1 \le f \le 1, \quad (5)$$

that is, ρ_W is entangled iff $\text{Tr}(\mathbb{F}\rho_W) < 0$ which is equivalent to $f > \frac{1}{2}$. Another well known example is an isotropic 2-qubit state

$$\rho_{\rm iso} = \frac{1}{4} \mathbb{1} \otimes \mathbb{1} + r |\phi^{+}\rangle \langle \phi^{+}|, \tag{6}$$

where we denote by $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$ the standard Bell states. The corresponding witness has the following form $W_{\rm iso} = |\psi^{-}\rangle\langle\psi^{-}|^{\Gamma}$, and hence it belongs to our class

$$W_{\rm iso} = \frac{1}{2} \Big(\mathbb{1} \otimes \mathbb{1} - \sigma_1 \otimes \sigma_1 + \sigma_2 \otimes \sigma_2 - \sigma_3 \otimes \sigma_3 \Big). \tag{7}$$

Again $\rho_{\rm iso}$ is entangled iff ${\rm Tr}(\rho_{\rm iso}W_{\rm iso})<0$ which implies $r>\frac{1}{3}$. To find EWs compatible with the above structure we find all state vectors $|\varphi\rangle$ such that $|\varphi\rangle\langle\varphi|$ has the structure (2). It is evident that $|\varphi\rangle\langle\varphi|^{\Gamma}$ fits also the structure (3. Our main result states

Theorem 1. There are six 1-parameter families of rank-1 projectors $|\varphi\rangle\langle\varphi|$ of the form (2):

$$|\varphi_{1}\rangle = a |\phi^{+}\rangle + b |\phi^{-}\rangle; |\varphi_{2}\rangle = a |\psi^{+}\rangle + b |\psi^{-}\rangle; |\varphi_{3}\rangle = a |\phi^{+}\rangle + b |\psi^{+}\rangle; |\varphi_{4}\rangle = a |\phi^{-}\rangle + b |\psi^{-}\rangle; |\varphi_{5}\rangle = a |\phi^{+}\rangle + ib |\psi^{-}\rangle; |\varphi_{6}\rangle = a |\phi^{-}\rangle + ib |\psi^{+}\rangle,$$
(8)

where $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$ are the Bell states, and $a, b \in \mathbb{R}$ are such that $a^2 + b^2 = 1$.

Note that $|\varphi_k\rangle$ is entangled if and only if $a \neq \pm \frac{1}{\sqrt{2}}$. The proof of theorem 1 is given in Supplementary Material. Interestingly, the above sets of states are the same as the ones reported in [9] in the context of detection of quantum channel capacities with limited local measurements, where the sets were derived by requiring orthogonality between states in order to have bases of the Hilbert space. Here this condition is relaxed but we arrive at the same result.

It is, therefore, clear that there are six families of extremal EWs belonging to the class (3):

$$W_k = |\varphi_k\rangle\langle\varphi_k|^{\Gamma},\tag{9}$$

for k = 1, ..., 6. For instance the extremal witness $W_1 = |\varphi_1\rangle\langle\varphi_1|^{\Gamma}$ is given by:

$$W_{1} = \frac{1}{4} \left[\mathbb{I} \otimes \mathbb{I} + \sigma_{z} \otimes \sigma_{z} + (a^{2} - b^{2}) \sigma_{x} \otimes \sigma_{x} \right]$$

$$+ (a^{2} - b^{2}) \sigma_{y} \otimes \sigma_{y} + 2ab \left(\sigma_{z} \otimes \mathbb{I} + \mathbb{I} \otimes \sigma_{z} \right),$$

$$(10)$$

where the presence of only measurements from the set \mathcal{M} is manifest. The list of the others EWs is provided in the Supplementary Material. These operators generalize two qubit EWs derived in [13]. Recall that two qubit states of the form $\rho = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sum_k c_k \sigma_k \otimes \sigma_k)$ span so called magic simplex [14, 15].

In the following we show explicitly the performance of the extremal decomposable witnesses on states that emerge from an amplitude-damping channel, with damping parameter $\gamma \in [0,1]$, applied on one of the two qubits. This channel has the form $\mathcal{E}(\rho) = A_0 \rho A_o^{\dagger} + A_1 \rho A_1^{\dagger}$, with $A_0 = |0\rangle \langle 0| + \sqrt{1-\gamma} |1\rangle \langle 1|$ and $A_1 = \sqrt{\gamma} |0\rangle \langle 1|$. If this channel is applied to the second subsystem of a two qubit-system, with the Bell state $|\phi^+\rangle$ as input, the output state $A = \mathbb{I} \otimes \mathcal{E}(|\phi^+\rangle \langle \phi^+|)$ is entangled for $\gamma < 1$. The witness W_2 identifies the state A as entangled for any γ . Indeed, we have: $\text{Tr}[W_2 A] = \frac{1}{4}\left[2\left(-1+2a^2\right)\sqrt{1-\gamma}+\gamma-2a\sqrt{1-a^2\gamma}\right]$ which for $0 \le \gamma < 1$, i.e. all the entangled states, can be negative for some suitable choice of a. For example if $\gamma = 0.9$, then $\text{Tr}[W_2 A] < 0$ for $0.17 < a < \frac{1}{\sqrt{2}}$. While for $\gamma = 0.95$ we have $\text{Tr}[W_2 A] < 0$ for $0.38 < a < \frac{1}{\sqrt{2}}$. It is interesting to note that in

order to detect entangled states for γ close to 1, which are the least entangled, we have to consider witnesses with a different from the extreme points ± 1 and 0. This shows that our ability to detect entangled states increases by considering witnesses W_i characterized by $a, b \neq 0, \pm 1$, in contrast to the use of only the extremal witnesses on the Bell states, which in this case are fail.

Let us now explain how the EWs derived above can be operationally used. Given several copies of an unknown two-qubit quantum state ρ , if we want to determine whether ρ is entangled or not we can perform the local measurements given in \mathcal{M} and collect the statistics of their measurement outcomes. Then, from the statistics, we can evaluate $Tr(W_k \rho)$ for all k. If one of these quantities is below zero, then the state is identified as entangled. A classical optimization of the parameters a, b is required to achieve the best procedure performance, by computing $\min_{k,a,b} \text{Tr}[W_k(a,b)\rho]$. Such a procedure can be easily impremented in an experimental scenario, e.g. quantum optical implementation such as the one considered in [16], where a similar apparatus was used to demonstrate an efficient test to detect quantum channel capacities [9].

Higher dimensions.— In order to extend the above results, our goal is to construct entanglement witnesses for bipartite qudit systems by considering the statistics of only few local measurements. In a d-dimensional Hilbert space a convenient choice of the basis in the space of linear operators is provided by a set of generalized Gell-Mann matrices G_{α} ($\alpha = 1, 2, ..., d^2 - 1$) [19, 20]. These are traceless hermitian matrices that can be divided into three groups: (i) diagonal matrices:

$$G_{l}^{D} = \sqrt{\frac{1}{l(l+1)}} \left(\sum_{j=1}^{l} |j\rangle \langle j| - l |l+1\rangle \langle l+1| \right),$$
(11)

for $1 \le l \le d-1$; (ii) symmetric matrices:

$$G_{jk}^{S} = (|j\rangle \langle k| + |k\rangle \langle j|)/\sqrt{2}, \quad 1 \le j < k \le d \quad (12)$$

and (iii) antisymmetric ones:

$$G_{jk}^{A} = (\left|j\right\rangle \left\langle k\right| - \left|k\right\rangle \left\langle j\right|) / i\sqrt{2}, \quad 1 \leq j < k \leq d. \quad (13)$$

In what follows we enumerate the Gell-Mann matrices as follows $G_{\alpha} = \{G_l^D, G_{ij}^S, G_{ij}^A\}$. The normalization factors guarantiee the following orthogonal relations $\text{Tr}(G_{\alpha}G_{\beta}) = \delta_{\alpha\beta}$ for $\alpha = 0, 1, \ldots, d^2 - 1$, where $G_0 = 1/\sqrt{d}$. Now, any Hermitian operator in $\mathbb{C}^d \otimes \mathbb{C}^d$ may be represented as follows $X = \sum_{\alpha,\beta=0}^{d^2-1} x_{\alpha\beta}G_{\alpha} \otimes G_{\beta}$. Assuming normalization TrX = 1 one has

$$X = \frac{1}{d^2} \Big\{ \mathbb{1} \otimes \mathbb{1} + \sum_{\alpha,\beta=1}^{d^2 - 1} \Big(a_{\alpha} G_{\alpha} \otimes \mathbb{1} + b_{\alpha} \mathbb{1} \otimes G_{\alpha} \Big) + \sum_{\alpha,\beta=1}^{d^2 - 1} C_{\alpha\beta} G_{\alpha} \otimes G_{\beta} \Big\},$$

$$(14)$$

with real generalized Bloch vectors a_{α} , b_{α} , and correlation matrix $C_{\alpha\beta}$. Hence the analog of (2) corresponds to $C_{\alpha\beta} = c_{\alpha}\delta_{\alpha\beta}$, i.e. diagonal correlation matrix.

The *canonical* example of such witnesses is provided by a flip operator:

$$\mathbb{F}_d = \sum_{\alpha=0}^{d^2 - 1} G_\alpha \otimes G_\alpha. \tag{15}$$

As is well known, \mathbb{F}_d witnesses entanglement within the whole class of $d \otimes d$ Werner states, which generalize to two qudits the class (5).

Interestingly, it was proved in [22] that for arbitrary orthogonal matrix $O_{\alpha\beta}$ the following operator

$$W = \mathbb{1} \otimes \mathbb{1} - \sum_{\alpha,\beta=0}^{d^2 - 1} O_{\alpha\beta} G_{\alpha} \otimes G_{\beta}^{\mathrm{T}}$$
 (16)

is block-positive and hence it defines an entanglement witness when W has at least one negative eigenvalue. Clearly, $W^{\Gamma} = \mathbbm{1} \otimes \mathbbm{1} - \sum_{\alpha,\beta=0}^{d^2-1} O_{\alpha\beta} G_{\alpha} \otimes G_{\beta}$ is a witness as well. In particular, $\mathbbm{1} \otimes \mathbbm{1} - \sum_{\alpha=0}^{d^2-1} G_{\alpha} \otimes G_{\alpha}$ defines a witness operator.

In what follows we consider the similar scenario for arbitrary d, that is, we look for EWs of the form (14) that belong to two classes: the class C_0 made by operators with diagonal correlation matrix $C_{\alpha\beta} = c_{\alpha}\delta_{\alpha\beta}$; and the class C_1 with correlation matrix that satisfies the following structure:

$$\sum_{\alpha,\beta} C_{\alpha\beta} G_{\alpha} \otimes G_{\beta} = \sum_{k,l=1}^{d-1} D_{kl} G_k^D \otimes G_l^D + \sum_{i < j} \left(S_{ij} G_{ij}^S \otimes G_{ij}^S + A_{ij} G_{ij}^A \otimes G_{ij}^A \right).$$
 (17)

Both classes coincide for d = 2. A straightforward generalization of Theorem 1 consists in the following:

Theorem 2. The following rank-1 projectors belong

to C_1 :

$$|\varphi_{1}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + b |\phi^{-}\rangle_{jk}$$

$$|\varphi_{2}\rangle_{jk} = a |\psi^{+}\rangle_{jk} + b |\psi^{-}\rangle_{jk}$$

$$|\varphi_{3}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + b |\psi^{+}\rangle_{jk}$$

$$|\varphi_{4}\rangle_{jk} = a |\phi^{-}\rangle_{jk} + b |\psi^{-}\rangle_{jk}$$

$$|\varphi_{5}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + ib |\psi^{-}\rangle_{jk}$$

$$|\varphi_{6}\rangle_{jk} = a |\phi^{-}\rangle_{jk} + ib |\psi^{+}\rangle_{jk}$$

$$(18)$$

where the real a and b satisfy $a^2+b^2=1$. Vectors $|\phi^{\pm}\rangle_{jk}$ and $|\psi^{\pm}\rangle_{jk}$ represent four Bell states defined by $|\phi^{\pm}\rangle_{jk}=(|jj\rangle\pm|kk\rangle)/\sqrt{2}$ and $|\psi^{\pm}\rangle_{jk}=(|jk\rangle\pm|jk\rangle)/\sqrt{2}$.

For the proof see the Supplementary Material. Clearly, the above vectors from $\mathbb{C}^d \otimes \mathbb{C}^d$ have Schmidt rank not greater than two. To go beyond Schmidt rank 2 vectors one has the following:

Proposition 1. A rank-1 projector P_{MC} corresponding to a maximally correlated state $|\psi\rangle_{\text{MC}} = \sum_i x_i |ii\rangle$ with $x_i \in \mathbb{R}$ satisfying $\sum_i x_i^2 = 1$, belongs to \mathcal{C}_1 . Moreover, it belongs to \mathcal{C}_0 iff it is maximally entangled, that is, $x_i = \frac{1}{\sqrt{d}}$.

Indeed, one has

$$P_{\text{MC}} = \sum_{i,j=1}^{d} x_i x_j |i\rangle\langle j| \otimes |i\rangle\langle j|$$

$$= \sum_{i} x_i^2 |i\rangle\langle i| \otimes |i\rangle\langle i| \qquad (19)$$

$$+ \frac{1}{2} \sum_{i < j} x_i x_j \left(G_S^{ij} \otimes G_S^{ij} - G_A^{ij} \otimes G_A^{ij} \right),$$

which proves that it belongs to C_1 . If all $x_i = 1/\sqrt{d}$, then it follows from the fact that $dP_d^+ = \mathbb{F}^{\Gamma}$.

This implies that with projectors (19) we can build the following EWs: extremal decomposable P^{Γ} and W = D - P, where $D = \sum_{i,j=1}^{d} d_{ij} |i\rangle \langle i| \otimes |j\rangle \langle j|$ is a diagonal matrix. Note, that if W is an EW then $W^{\Gamma} = D - P^{\Gamma}$ is an EW as well. In particular, if $D = d1 \otimes 1$, then $W = \lambda \mathbb{I} \otimes \mathbb{I} - |\psi\rangle \langle \psi|$, is an EW iff $1 > \lambda \geq x_{\star} = \max_{i} \{x_{i}\}$. Moreover, such W is always decomposable and it is optimal only if P is maximally entangled. To get non-decomposable EW one needs $D \neq \lambda 1 \otimes 1$.

Example 1. Consider the diagonal part

$$D = \sum_{i=1}^{d} |i\rangle\langle i| \otimes \left((d-k)|i\rangle\langle i| + \sum_{j=1}^{k} |i+j\rangle\langle i+j| \right), (20)$$

with $k \in \{1, ..., d-1\}$. It corresponds to $d_{ii} = d-k$, $d_{i,i+1} = ... = d_{i,i+k} = 1$ and the remaining $d_{ij} = 0$. For k = 1, ..., d-2 it was proved [24] that $W = D - dP_d^+$ defined non-decomposable EW

and for k = d - 1 it reproduces the reduction EW $1 \otimes 1 - dP_d^+$. For d = 3 and k = 1, 2 it gives the celebrated Choi witness which was proved to be also extremal (see also [25] for another analysis of this witness).

Example 2. Consider the diagonal part

$$D = p_0 \sum_{i=1}^{d} |i\rangle\langle i| \otimes \left(p_0|i\rangle\langle i| + p_{i-1}|i-1\rangle\langle i-1|\right), (21)$$

for $p_0, p_1, \dots, p_d > 0$. It defines a non-decomposable EW $W = D - dP_d^+$ iff: $p_0 \in [d-2, d-1)$ and

$$p_1 \dots p_d \ge (d - 1 - p_0)^d$$
.

Interestingly, for d = 3 it was proved that if $p_0 = 1$ and $p_1p_2p_3 = 1$, then W is also extremal [23].

Example 3. Let d = 3 and consider

$$\begin{split} D_{[abc]} &= \sum_{i=1}^{3} |i\rangle\langle i| \otimes \Big(\left(a+1\right)|i\rangle\langle i| \\ &+ b|i+1\rangle\langle i+1| + c|i+2\rangle\langle i+2|\Big). \end{split}$$

where we add $\mod 2$ and $a,b,c \ge 0$. Then, we consider:

$$W_{[abc]} = D_{[abc]} - dP_3^+.$$

The above operator is an EW iff [24]: a < 2, $a + b + c \ge 2$, and if a < 1, then additionally $bc > (1-a)^2$. Note that if a = 0, b = c = 1, then we recover the reduction witness. The class $W_{[abc]}$ contains indecomposable EW and therefore it can be used to detect bound entangled states. A special class is given by the following choice: $0 < a \le 1$, a + b + c = 2 and $bc = (1-a)^2$, indeed it contains only extremal witnesses. Moreover, they are indecomposable iff $b \ne c$.

Conclusions— In this Letter we have proposed a method to construct EWs from a limited set of local measurements. Such a method completely characterized the class of EW of the form $W = P^{\Gamma}$ that can be derived from \mathcal{M} on two-qubit systems. The method relies on an optimization procedure performed by classical means on the measurement results and leads to a possible implementation in various experimental, such as the quantum optical implementation considered in [16]. Possible generalisations to higher dimensional systems have been proposed. It would be also very interesting to provide similar analysis for different observables, such as the ones defined in [26], and in the multipartite case.

Acknowledgements- : We thank O. Gühne for useful discussions and comments.

D.C. was supported by the Polish National Science Centre project 2015/19/B/ST1/03095.

- M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A 223, 1 (1996).
- [2] B.M. Terhal, Phys. Lett. A 271, 319 (2000); Linear Algebr. Appl. 323, 61 (2000).
- [3] B. M. Terhal, Theor. Comput. Sci. 287, 313 (2002).
- [4] O. Gühne and G. Tóth, Phys. Rep. 474, 1 (2009).
- [5] D. Chruscinski and G. Sarbicki, J. Phys. A: Math. Theor. 47, 483001 (2014).
- [6] M. Lewenstein, B. Kraus, J.I. Cirac and P. Horodecki, Phys. Rev. A 62, 052310 (2000).
- [7] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera, Phys. Rev. A 66, 062305 (2002).
- [8] D. Chruściński and G. Sarbicki, J. Phys. A: Math. Theor. 47 (2014).
- [9] C. Macchiavello and M. Sacchi, Phys, Rev. Lett. 116, 140501 (2016).
- [10] C. Macchiavello and M. Sacchi, Phys. Rev. A 94, 052333 (2016).
- [11] O. Gühne, Private communication (2019).
- [12] B. Jungnitsch, T. Moroder and O. Gühne, Phys. Rev. Lett. 106, 190502 (2011).
- [13] R.A. Bertlmann, H. Narnhofer and W. Thirring, Phys. Rev. A 66, 032319 (2002).
- [14] B. Baumgartner, B.C. Hiesmayr and H. Narnhofer, Phys. Rev. A 74, 032327 (2006).
- [15] B. Baumgartner, B.C. Hiesmayr and H. Narnhofer, J. Phys. A: Math. Theor. 40, 7919 (2007).
- [16] A. Cuevas, M. Proietti, M. A. Ciampini, S. Duranti, P. Mataloni, M. F. Sacchi and C. Macchiavello, Phys. Rev. Lett. 119, 100502 (2017).
- [17] N. Ganguly, S. Adhikari, A. S. Majumdar and J. Chatterjee, Phys. Rev. Lett. 107, 270501 (2011).
- [18] F. G. S. L. Brandao, Phis. Rev. A 72, 022310 (2005).
- [19] R. A. Bertlmann and P. Krammer, J. Phys. A: Math.Theor. 41, 235303 (2008).
- [20] G. Kimura, Phys. Lett. A 314, 339 (2003).
- [21] W. J. Munro, D. F. V. James, A. G. White, and P. G. Kwiat, Phys. Rev. A 64, 030302(R) (2001).
- [22] S. Yu and N. Liu, Phys. Rev. Lett. 95, 150504 (2005).
- [23] H. Osaka, Linear Algebr. Appl. 153, 73 (1991).
- [24] K.-C. Ha, Publ. Res. Inst. Math. Sci. 34, 591 (1998).
- [25] M. Lewenstein et al. Phys. Rev. A 93, 042335 (2016).
- [26] A. Asadian et al. Phys. Rev. A 94, 010301(R)(2016).

Appendix A: Extremal entanglement witness for two qubits

The extremal EWs for two-qubit systems derived from the set of local measurements $\sigma_x \otimes \sigma_x$, $\sigma_y \otimes \sigma_y$ and $\sigma_z \otimes \sigma_z$ are given by the following operators:

$$W_{1} = \frac{1}{4} \Big[\mathbb{I} \otimes \mathbb{I} + \sigma_{z} \otimes \sigma_{z} + (a^{2} - b^{2}) \sigma_{x} \otimes \sigma_{x}$$
 (A1)

$$+ (a^{2} - b^{2}) \sigma_{y} \otimes \sigma_{y} + 2ab \left(\sigma_{z} \otimes \mathbb{I} + \mathbb{I} \otimes \sigma_{z} \right) \Big],$$

$$W_2 = \frac{1}{4} \left[\mathbb{I} \otimes \mathbb{I} - \sigma_z \otimes \sigma_z + (a^2 - b^2) \sigma_x \otimes \sigma_x - (A2) - (a^2 - b^2) \sigma_y \otimes \sigma_y + 2ab(\sigma_z \otimes \mathbb{I} - \mathbb{I} \otimes \sigma_z) \right],$$

$$W_{3} = \frac{1}{4} \left[\mathbb{I} \otimes \mathbb{I} + \sigma_{x} \otimes \sigma_{x} + (a^{2} - b^{2}) \sigma_{z} \otimes \sigma_{z} \right]$$

$$+ (a^{2} - b^{2}) \sigma_{y} \otimes \sigma_{y} + 2ab2(\sigma_{x} \otimes \mathbb{I} + \mathbb{I} \otimes \sigma_{x}) ,$$
(A3)

$$W_4 = \frac{1}{4} \Big[\mathbb{I} \otimes \mathbb{I} - \sigma_x \otimes \sigma_x + (a^2 - b^2) \sigma_z \otimes \sigma_z \qquad (A4)$$
$$- (a^2 - b^2) \sigma_y \otimes \sigma_y - 2ab(\sigma_x \otimes \mathbb{I} - \mathbb{I} \otimes \sigma_x) \Big],$$

$$W_5 = \frac{1}{4} \left[\mathbb{I} \otimes \mathbb{I} + \sigma_y \otimes \sigma_y + (a^2 - b^2) \sigma_z \otimes \sigma_z + (a^2 - b^2) \sigma_x \otimes \sigma_x + 2ab(\sigma_y \otimes \mathbb{I} + \mathbb{I} \otimes \sigma_y) \right],$$

$$W_{6} = \frac{1}{4} \Big[\mathbb{I} \otimes \mathbb{I} - \sigma_{y} \otimes \sigma_{y} + (a^{2} - b^{2}) \sigma_{z} \otimes \sigma_{z}$$
 (A6)
$$- (a^{2} - b^{2}) \sigma_{x} \otimes \sigma_{x} - 2ab(\sigma_{y} \otimes \mathbb{I} - \mathbb{I} \otimes \sigma_{y}) \Big],$$

Appendix B: Proof of theorem 1

Theorem 1. There are six 1-parameter families of rank-1 projectors: $|\varphi\rangle\langle\varphi|$ of the form

$$W = \alpha \mathbb{1} \otimes \mathbb{1} + \sum_{k=x,y,z} \left(a_k \mathbb{1} \otimes \sigma_k + b_k \sigma_k \otimes \mathbb{1} \right) + \sum_{k=x,y,z} c_k \sigma_k \otimes \sigma_k,$$
(B1)

which are given by:

$$|\varphi_{1}\rangle = a |\phi^{+}\rangle + b |\phi^{-}\rangle; |\varphi_{2}\rangle = a |\psi^{+}\rangle + b |\psi^{-}\rangle; |\varphi_{3}\rangle = a |\phi^{+}\rangle + b |\psi^{+}\rangle; |\varphi_{4}\rangle = a |\phi^{-}\rangle + b |\psi^{-}\rangle; |\varphi_{5}\rangle = a |\phi^{+}\rangle + ib |\psi^{-}\rangle; |\varphi_{6}\rangle = a |\phi^{-}\rangle + ib |\psi^{+}\rangle,$$
(B2)

where $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$ are the Bell states, and $a, b \in \mathbb{R}$ are such that $a^2 + b^2 = 1$.

Proof. Any 2-qubit entanglement witness W can be represented as follows:

$$W = \sum_{\mu,\nu=0}^{3} T_{\mu\nu} \sigma_{\mu} \otimes \sigma_{\nu}, \tag{B3}$$

with $\sigma_{\mu} \in \{1, \sigma_{x}, \sigma_{y}, \sigma_{z}\}$, and 16 real parameters $T_{\mu\nu}$. Witnesses of the form (B1) have diagonal correlation tensor $T_{ij} = c_{i}\delta_{ij}$ (i, j = 1, 2, 3) We now derive the most general projectors of the form $|\varphi\rangle\langle\varphi|$ that satisfy the conditions $c_{ij} = c_{i}\delta_{ij}$. The state pure state φ can be decomposed as:

$$|\varphi\rangle = e^{i\chi_0} m |00\rangle + e^{i\chi_i} n |01\rangle + e^{i\chi_2} q |10\rangle + t |11\rangle,$$
(B4)

where $m^2 + n^2 + q^2 + t^2 = 1$. The projector $|\varphi\rangle\langle\varphi|$ consists in 16 terms that can be expressed in terms of the single system Pauli operators by using the following equations:

$$|0\rangle\langle 0| = \frac{1}{2} (\mathbb{I} + \sigma_z);$$

$$|0\rangle\langle 1| = \frac{1}{2} (\sigma_x + i\sigma_y);$$

$$|1\rangle\langle 0| = \frac{1}{2} (\sigma_x - i\sigma_y);$$

$$|1\rangle\langle 1| = \frac{1}{2} (\mathbb{I} - \sigma_z).$$
(B5)

Then we can gather the coefficients of each operators and arrive at a projector of the form (B3) . Finally, we impose the conditions $c_{ij}=0$, for $i\neq j$ which implies a six equations system that it can be expressed as:

$$\begin{cases}
mn\cos(\chi_0 - \chi_1) = qt\cos\chi_2 \\
mn\sin(\chi_0 - \chi_1) = qt\sin\chi_2 \\
mq\cos(\chi_0 - \chi_2) = nt\cos\chi_1 \\
mq\sin(\chi_0 - \chi_2) = nt\sin\chi_1 \\
nq\sin(\chi_1 - \chi_2) = 0 \\
mt\sin\chi_0 = 0
\end{cases}$$
(B6)

We remind that another equation is provided by the constraint $m^2 + n^2 + q^2 + t^2 = 1$, that expresse the state normalization.

Let us analyze which are the solutions of (B6). First a class of solutions can be derived by the two last equations by imposing that one of the two parameters that multiply the sine functions vanishes. In this case the solutions are given by the following values:

$$m^2 + t^2 = 1$$
, $n = q = 0$ $\chi_0 = 0, \pi$; (B7)

or

$$n^2 + q^2 = 1$$
, $m = t = 0$ $\chi_2 - \chi_1 = 0, \pi$. (B8)

Note that we cannot have solutions like $q^2 + t^2 = 1$ with $b \neq 0, 1$, indeed if we impose m = n = 0 we would have:

$$\begin{cases} qt\cos\chi_2 = 0\\ qt\sin\chi_2 = 0\\ q^2 + t^2 = 1 \end{cases}$$
 (B9)

which is verified only in the points q = 0, 1 and t = 1, 0. In terms of states the solutions (B7) and (B8) are represented by:

$$|\varphi_m\rangle = m |00\rangle \pm t |11\rangle$$
 (B10)

and

$$|\varphi_n\rangle = n |01\rangle \pm q |10\rangle.$$
 (B11)

Note that they contain the four Bell states, namely $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The remaining solutions can be found by imposing $\sin{(\chi_1 - \chi_2)} = 0$, i.e. $\chi_1 - \chi_2 = 0$, π , in (B6). Besides (B7) and (B8), which can be restored, new solutions are linked to the condition $\sin{(\chi_0)} = 0$, i.e. $\chi_0 = 0$, π .

Let us analyze the solutions for $\chi_1 = \chi_2$ and $\chi_0 = 0$; the other cases produce similar results. We have only one free parameter a and the solutions are:

$$n = \pm \sqrt{\frac{1 - 2m^2}{2}}; q = \pm \sqrt{\frac{1 - 2m^2}{2}};$$

$$t = -\frac{2abc}{2a^2 - 1}; \chi_2 = 0, \pi;$$
(B12)

and

$$n = \pm \sqrt{\frac{1 - 2m^2}{2}}; q = \pm \sqrt{\frac{1 - 2m^2}{2}};$$

$$t = \frac{2abc}{2a^2 - 1}; \chi_2 = \frac{\pi}{2}, \frac{3\pi}{2}.$$
 (B13)

In order to understand which states correspond to the above solution we consider the case $n=q=\sqrt{\frac{1-2m^2}{2}}$, $\chi_2=\frac{\pi}{2}$ and therefore t=-m. Equation (B4) becomes:

$$|\varphi\rangle = m|00\rangle + i\sqrt{\frac{1 - 2m^2}{2}} (|01\rangle + |10\rangle) - m|11\rangle$$

$$= \sqrt{2}m \left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right) + i\sqrt{1 - 2m^2} \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right)$$

$$= \sqrt{2}m|\phi^-\rangle + i\sqrt{1 - 2m^2}|\psi^+\rangle$$

$$= a|\phi^-\rangle + ib|\psi^+\rangle$$

where $a^2 + b^2 = 1$. Similar results can be obtained by considering the others solutions. Finally we arrive at 6 distinct states, which in terms of the Bell states are:

$$|\varphi_{1}\rangle = a |\phi^{+}\rangle + b |\phi^{-}\rangle; |\varphi_{2}\rangle = a |\psi^{+}\rangle + b |\psi^{-}\rangle;$$
(B15)
$$|\varphi_{3}\rangle = a |\phi^{+}\rangle + b |\psi^{+}\rangle; |\varphi_{4}\rangle = a |\phi^{-}\rangle + b |\psi^{-}\rangle;$$
(B16)
$$|\varphi_{5}\rangle = a |\phi^{+}\rangle + ib |\psi^{-}\rangle; |\varphi_{6}\rangle = a |\phi^{-}\rangle + ib |\psi^{+}\rangle;$$
(B17)

Note that we must have $a^2 + b^2 = 1$. Moreover the states $|\varphi_m\rangle$ and $|\varphi_n\rangle$ can be generated from those above. For example $|\varphi_m\rangle$ can be represented in terms of the state $|\varphi_1\rangle$ by redefining the parameters.

Appendix C: Proof of theorem 2

Any Hermitian operator X in $\mathbb{C}^d \otimes \mathbb{C}^d$ may be represented as $X = \sum_{\alpha,\beta=0}^{d^2-1} x_{\alpha\beta} G_{\alpha} \otimes G_{\beta}$, where the $G_{\alpha} = \{G_l^D, G_{ij}^S, G_{ij}^A\}$ are the Generalized Gell-Mann (GGM) matrices, which can be divided into three types defined as follows: (i) diagonal matrices:

$$G_{l}^{D} = \sqrt{\frac{1}{l(l+1)}} \left(\sum_{j=1}^{l} |j\rangle \langle j| - l |l+1\rangle \langle l+1| \right), \tag{C1}$$

for $1 \le l \le d-1$; (ii) symmetric matrices:

$$G_{jk}^{S} = (|j\rangle \langle k| + |k\rangle \langle j|)/\sqrt{2}, \quad 1 \le j < k \le d \quad (C2)$$

and (iii) antisymmetric ones:

$$G_{jk}^A = (|j\rangle \langle k| - |k\rangle \langle j|)/i\sqrt{2}, \quad 1 \le j < k \le d. \quad (C3)$$

Assuming normalization TrX = 1 one has

$$X = \frac{1}{d^2} \Big\{ \mathbb{1} \otimes \mathbb{1} + \sum_{\alpha,\beta=1}^{d^2 - 1} \Big(a_{\alpha} G_{\alpha} \otimes \mathbb{1} + b_{\alpha} \mathbb{1} \otimes G_{\alpha} \Big) + \sum_{\alpha,\beta=1}^{d^2 - 1} C_{\alpha\beta} G_{\alpha} \otimes G_{\beta} \Big\},$$
 (C4)

with real generalized Bloch vectors a_{α} , b_{α} , and correlation matrix $C_{\alpha\beta}$. Hence the analog of (2) corresponds to $C_{\alpha\beta} = c_{\alpha}\delta_{\alpha\beta}$, i.e. diagonal correlation matrix.

Among the operators (C4) we distinguish two classes: first, the class C_0 made by operators with diagonal $C_{\alpha\beta}$; second, the class C_1 of operators that satisfy:

$$\sum_{\alpha,\beta} C_{\alpha\beta} G_{\alpha} \otimes G_{\beta} = \sum_{k,l=1}^{d-1} D_{kl} G_D^k \otimes G_D^l + \sum_{i < j} \left(S_{ij} G_S^{ij} \otimes G_S^{ij} + A_{ij} G_A^{ij} \otimes G_A^{ij} \right). \quad (C5)$$

Theorem 2. The following rank-1 projectors belong

to C_1 :

$$|\varphi_{1}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + b |\phi^{-}\rangle_{jk}$$

$$|\varphi_{2}\rangle_{jk} = a |\psi^{+}\rangle_{jk} + b |\psi^{-}\rangle_{jk}$$

$$|\varphi_{3}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + b |\psi^{+}\rangle_{jk}$$

$$|\varphi_{4}\rangle_{jk} = a |\phi^{-}\rangle_{jk} + b |\psi^{-}\rangle_{jk}$$

$$|\varphi_{5}\rangle_{jk} = a |\phi^{+}\rangle_{jk} + ib |\psi^{-}\rangle_{jk}$$

$$|\varphi_{6}\rangle_{jk} = a |\phi^{-}\rangle_{jk} + ib |\psi^{+}\rangle_{jk}$$
(C6)

where the real A and b satisfy $a^2 + b^2 = 1$. Vectors $|\phi^{\pm}\rangle_{jk}$ and $|\psi^{\pm}\rangle_{jk}$ represent four Bell stare defined by $|\phi^{\pm}\rangle_{jk} = (|jj\rangle \pm |kk\rangle)/\sqrt{2}$ and $|\psi^{\pm}\rangle_{jk} = (|jk\rangle \pm |jk\rangle)/\sqrt{2}$.

Proof. Without loss of generality we consider the state $|\varphi_1\rangle_{ik}$. The projector on $|\varphi_1\rangle_{ik}$ is given by:

$$|\varphi_1\rangle_{jk} \langle \varphi_1|_{jk} = \frac{(1+2ab)}{2} |jj\rangle \langle jj| + \frac{(1-2ab)}{2} |kk\rangle \langle kk| + \frac{(a^2-b^2)}{2} (|jj\rangle \langle kk| + |kk\rangle \langle jj|).$$
(C7)

The projectors $|jj\rangle \langle jj|$ and $|kk\rangle \langle kk|$ contain only terms related to $G_l^D \otimes G_{l'}^D$, $G_l^D \otimes \mathbb{I}$ and $\mathbb{I} \otimes G_{l'}^D$, hence we can focus only on the remaining two projectors. From equations (C2) and (C3) we can see that the single system projector $|j\rangle \langle k|$ can be expressed as:

$$|j\rangle\langle k| = \frac{1}{2} \left(G_{jk}^S + iG_{jk}^A \right),$$
 (C8)

hence $|jj\rangle\langle kk|$ is given by:

$$|jj\rangle\langle kk| = \frac{1}{4} \left(G_{jk}^S \otimes G_{jk}^S + iG_{jk}^S \otimes G_{jk}^A \right)$$
 (C9)

$$\frac{1}{4} \left(iG_{jk}^A \otimes G_{jk}^S - G_{jk}^A \otimes G_{jk}^A \right). \quad (C10)$$

Its complex conjugated is thus given by:

$$|kk\rangle \langle jj| = \frac{1}{4} \left(G_{jk}^S \otimes G_{jk}^S - iG_{jk}^S \otimes G_{jk}^A \right), \quad (C11)$$
$$\frac{1}{4} \left(-iG_{jk}^A \otimes G_{jk}^S - G_{jk}^A \otimes G_{jk}^A \right), \quad (C12)$$

hence their sum is:

$$|jj\rangle\langle kk| + |jj\rangle\langle kk| = \frac{1}{2} \left(G_{jk}^S \otimes G_{jk}^S - G_{jk}^A \otimes G_{jk}^A \right),$$
(C13)

which contains only terms of the form (C5), and so do the projectors on $|\varphi_1\rangle_{jk}$. Note that if we had considered a state of the form $|\varphi_1\rangle_{jk}^{\chi} = a\,|\phi^+\rangle_{jk} + e^{i\chi}b\,|\phi^-\rangle_{jk}$, then its corresponding projector would have been expressed by

$$|\varphi_{1}\rangle_{jk}^{\chi} \langle \varphi_{1}|_{jk}^{\chi} = \frac{(1+2ab)}{2} |jj\rangle \langle jj| + \frac{(1-2ab)}{2} |kk\rangle \langle kk| + \frac{(a^{2}-b^{2}+2iab\sin\chi)}{2} |jj\rangle \langle kk| + \frac{(a^{2}-b^{2}-2iab\sin\chi)}{2} |jj\rangle \langle kk|,$$

$$(C14)$$

which fits in the class C_{∞} if and only if $\chi = 0, \pi$. The same derivation, by using the properties of the GGM matrices, holds for any of the states $|\varphi_m\rangle_{jk}$, m = 0, 1, 2, 3, 4, 5, 6 and $1 \le j < k \le d$.