Optimal entanglement witnesses from limited local measurements

Alberto Riccardi,1 Dariusz Chruściński,2 and Chiara Macchiavello1,3,4
1Dipartimento di Fisica, University of Pavia, via Bassi 6, 27100 Pavia, Italy.
2Institute of Physics, Faculty of Physics, Astronomy and Informatics, Nicolaus Copernicus University, Grudziadzka 5/7, 87-100 Toruń, Poland.
3INFN Sezione di Pavia, via Bassi 6, I-27100, Pavia, Italy.
4CNR-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 that can be constructed from the measurements of the bipartite operators $\sigma_x \otimes \sigma_z$, $\sigma_y \otimes \sigma_z$ and $\sigma_z \otimes \sigma_z$ in the case of two-qubit systems. In particular, we consider all possible extremal decomposable witnesses, which represent the most powerful form of witnesses for a two-qubit system, that can be defined from this set of measurements. Finally, we discuss possible extensions to higher dimension multipartite systems when the set of available measurements is characterized by the generalised 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) \[1\] \[2\]. 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) $\text{Tr}[W \rho_{\text{sep}}] \geq 0$ for all separable states $\rho_{\text{sep}}$, and ii) there exists at least one entangled state $\rho_e$ 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. \[1\] \[4\] for the review). For example an EW is decomposable if $W = A + B^\dagger$, where $A, B \geq 0$ and $B^\dagger$ 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 cannot 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 $W = A + B^\dagger$. 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 \[7\]. 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 $W = |\psi\rangle\langle\psi|^\dagger$ 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 \[10\] \[11\]. 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 that can be constructed for a two-qubit system by considering only the statistics of $\mathcal{M} = \{\sigma_x \otimes \sigma_z, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\}$. Any 2-qubit entanglement witness $W$ can be represented as follows:

$$W = \sum_{\mu,\nu=0}^3 T_{\mu\nu} \sigma_\mu \otimes \sigma_\nu,$$  \hspace{1cm} (1)
with \( \sigma_{il} \in \{1, \sigma_x, \sigma_y, \sigma_z \} \), and 16 real parameters \( T_{kl} \). 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 \( \alpha, a_k, b_k, c_k \). 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. The canonical example of such a witness is provided by the flip operator

\[
F = \frac{1}{2} \left( \mathbb{1} \otimes \mathbb{1} + \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z \right).
\]

(3)

As is well known \( F \) witnesses entanglement within a class of Werner states:

\[
\rho_W = \frac{1}{2(1-f)} \left( \mathbb{1} \otimes \mathbb{1} - f F \right), \quad -1 \leq f \leq 1,
\]

(4)

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

\[
\rho_{iso} = \frac{1}{4} \mathbb{1} \otimes \mathbb{1} + r |\phi^+\rangle \langle \phi^+|,
\]

(5)

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

\[
W_{iso} = \frac{1}{2} \left( \mathbb{1} \otimes \mathbb{1} - \sigma_1 \otimes \sigma_1 + \sigma_2 \otimes \sigma_2 - \sigma_3 \otimes \sigma_3 \right).
\]

(6)

Again \( \rho_{iso} \) is entangled iff \( \text{Tr}(\rho_{iso} W_{iso}) < 0 \) which implies \( r > \frac{1}{2} \). 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 \( |\varphi\rangle \langle \varphi| \) fits the structure (2) as well. Our main result states

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

\[
|\varphi_1\rangle = a |\phi^+\rangle + b |\phi^-\rangle; \quad |\varphi_2\rangle = a |\psi^+\rangle + b |\psi^-\rangle;
|\varphi_3\rangle = a |\phi^+\rangle + b |\psi^+\rangle; \quad |\varphi_4\rangle = a |\phi^-\rangle + b |\psi^-\rangle;
|\varphi_5\rangle = a |\phi^+\rangle + ib |\psi^-\rangle; \quad |\varphi_6\rangle = a |\phi^-\rangle + ib |\psi^+\rangle,
\]

(7)

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 [10] 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 (2).

\[
W_k = |\varphi_k\rangle \langle \varphi_k|,
\]

(8)

for \( k = 1, \ldots, 6 \). For instance the extremal witness \( W_1 = |\varphi_1\rangle \langle \varphi_1| \) is given by:

\[
W_1 = \frac{1}{4} \left( \mathbb{1} \otimes \mathbb{1} + \sigma_2 \otimes \sigma_2 + (a^2 - b^2) \sigma_x \otimes \sigma_x
+ (a^2 - b^2) \sigma_y \otimes \sigma_y + 2ab (\sigma_z \otimes I + I \otimes \sigma_z) \right),
\]

(9)

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 [12]. Recall that two qubit states of the form \( \rho = \frac{1}{2} (\mathbb{1} \otimes \mathbb{1} + \sum_k c_k \sigma_k \otimes \sigma_k) \) span so called magic simplex [13, 14]. It is, therefore, clear that EWs we provided completely characterized entanglement content of the magic simplex states.

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 \( \mathcal{E} (\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger \), 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 \( A = I \otimes \mathcal{E} (|\phi^+\rangle \langle \phi^+|) \) is entangled for \( \gamma < 1 \). The extremal decomposable witness that identifies the state \( A \) as entangled for any \( \gamma \) is \( W_2 \). Indeed we have

\[
\text{Tr} [W_2 A] = \frac{1}{4} \left[ 2 \left( -1 + 2a^2 \right) \sqrt{1-\gamma} + \gamma - 2a \sqrt{1-\gamma} - a^2 \gamma \right]
\]

which for \( 0 \leq \gamma < 1 \), namely 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 \( \gamma \) close to 1, that correspond to the weakest form
of entanglement in this class of states, we have to consider extremal decomposable witnesses with $\alpha$ different from the extreme points $\pm 1$ and $0$. This shows that our ability to detect entangled states increases by considering extremal decomposable 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 $\rho$, if we want to determine whether $\rho$ 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 $\text{Tr}(W_k \rho)$ 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 $\min_{a, b} \text{Tr}(W_k(a, b)\rho)$. Such a procedure can be easily implemented in an experimental scenario, e.g. quantum optical implementation such as the one considered in [13], where a similar apparatus was used to demonstrate an efficient test to detect quantum channel capacities [10].

**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 $G_\alpha$ ($\alpha = 1, 2, \ldots, d^2 - 1$) [18, 19]. These are traceless hermitian matrices that can be divided into three groups: (i) diagonal matrices:

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

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

$$G^S_{jk} = (\langle j | k \rangle + | k \rangle \langle j |)/\sqrt{2}, \quad 1 \leq j < k \leq d \quad (11)$$

and (iii) antisymmetric ones:

$$G^A_{jk} = (\langle j | k \rangle - | k \rangle \langle j |)/i\sqrt{2}, \quad 1 \leq j < k \leq d. \quad (12)$$

In what follows we enumerate the Gell-Mann matrices as follows $G_\alpha = \{ G^D_l, G^S_{ij}, G^A_{ij} \}$. The normalization factors guarantee the following orthogonal relations $\text{Tr}(G_\alpha G_\beta) = \delta_{\alpha \beta}$ for $\alpha = 0, 1, \ldots, d^2 - 1$, where $G_0 = \mathbb{I}/\sqrt{d}$. Now, any Hermitian operator in $\mathbb{C}^d \otimes \mathbb{C}^d$ may be represented as follows

$$X = \sum_{\alpha, \beta = 0}^{d^2 - 1} C_{\alpha \beta} G_\alpha \otimes G_\beta.$$ 

Assuming normalization $\text{Tr}X = 1$ one has

$$X = \frac{1}{d^2} \left\{ \mathbb{I} \otimes \mathbb{I} + \sum_{\alpha, \beta = 1}^{d^2 - 1} \left( a_\alpha G_\alpha \otimes \mathbb{I} + b_\alpha \mathbb{I} \otimes G_\alpha \right) + \sum_{\alpha, \beta = 1}^{d^2 - 1} C_{\alpha \beta} G_\alpha \otimes G_\beta \right\}, \quad (13)$$

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

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

$$F_d = \frac{1}{d} \left( \mathbb{I} \otimes \mathbb{I} + \sum_{\alpha = 1}^{d^2 - 1} G_\alpha \otimes G^T_\alpha \right). \quad (14)$$

As is well known, $F_d$ witnesses entanglement within the whole class of $d \otimes d$ Werner states, which generalize to two qudits the class (4).

Interestingly, it was proved in [21] that for arbitrary orthogonal matrix $O_{\alpha \beta}$ the following operator

$$W = \mathbb{I} \otimes \mathbb{I} - \sum_{\alpha, \beta = 0}^{d^2 - 1} O_{\alpha \beta} G_\alpha \otimes G^T_\beta \quad (15)$$

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

In what follows we consider the similar scenario for arbitrary $d$, that is, we look for EWs of the form (13) that belong to two classes: the class $C_0$ made by operators with diagonal correlation matrix $C_{\alpha \beta} = c_\alpha d_{\alpha \beta}$; and the class $C_1$ with correlation matrix that satisfies the following structure:

$$\sum_{\alpha, \beta} C_{\alpha \beta} G_\alpha \otimes G_\beta = \sum_{k, l=1}^{d-1} D_{kl} G^D_k \otimes G^D_l$$

$$+ \sum_{i<j} \left( S_{ij} G^S_{ij} \otimes G^S_{ij} + A_{ij} G^A_{ij} \otimes G^A_{ij} \right). \quad (16)$$

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 $C_1$:

$$
|\varphi_1\rangle_{jk} = a|\phi^+\rangle_{jk} + b|\phi^-\rangle_{jk} \\
|\varphi_2\rangle_{jk} = a|\psi^+\rangle_{jk} + b|\psi^-\rangle_{jk} \\
|\varphi_3\rangle_{jk} = a|\phi^+\rangle_{jk} + b|\psi^+\rangle_{jk} \\
|\varphi_4\rangle_{jk} = a|\phi^-\rangle_{jk} + b|\psi^-\rangle_{jk} \\
|\varphi_5\rangle_{jk} = a|\phi^+\rangle_{jk} + ib|\psi^-\rangle_{jk} \\
|\varphi_6\rangle_{jk} = a|\phi^-\rangle_{jk} + ib|\psi^+\rangle_{jk}
$$

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 $|\psi^\pm\rangle_{jk} = (|jk\rangle \pm |kj\rangle)/\sqrt{2}$.

For the proof see the Supplementary Material. Clearly, the above vectors from $C^d \otimes C^d$ 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 $|\psi\rangle_{MC} = \sum x_i |ii\rangle$ with $x_i \in \mathbb{R}$ satisfying $\sum x_i^2 = 1$, belongs to $C_1$. Moreover, it belongs to $C_0$ iff it is maximally entangled, that is, $x_i = \frac{1}{\sqrt{d}}$.

Indeed, one has

$$P_{MC} = \sum_{i,j=1}^d x_i x_j |jj\rangle \langle ii| \\
= \sum_i x_i^2 |ii\rangle \langle ii| + \frac{1}{2} \sum_{i<j} x_i x_j \left( G_{S}^{ij} \otimes G_{S}^{ij} - G_{A}^{ij} \otimes G_{A}^{ij} \right),
$$

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

This implies that with projectors $[12]$ we can build the following EWs: extremal decomposable $P^+$ and $W = D - P_+$, where $D = \sum_{i,j=1}^d d_{ij} |ii\rangle \langle jj|$ is a diagonal matrix. Note, that if $W$ is an EW then $W^+ = D - P^r$ is an EW as well. In particular, if $D = d^2 \mathbb{I} \otimes \mathbb{I}$, then $W = \lambda \mathbb{I} \otimes \mathbb{I} - |\psi\rangle \langle \psi|$, is an EW iff $1 > \lambda \geq x_*$, max$_i \{|x_i|\}$. Moreover, such $W$ is always decomposable and it is optimal if $P$ is maximally entangled. To get non-decomposable EW one needs $D \neq \lambda \mathbb{I} \otimes \mathbb{I}$.

**Example 1.** Consider the diagonal part

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

with $k \in \{1,\ldots,d-1\}$. It corresponds to $d_{ii} = d - k$, $d_{i,i+1} = \ldots = d_{i,i+k} = 1$ and the remaining $d_{ij} = 0$. For $k = 1,\ldots,d-2$ it was proved $[23]$ that $W = D - dP_d^+$ defined non-decomposable EW and for $k = d - 1$ it reproduces the reduction EW $\mathbb{I} \otimes \mathbb{I} - dP_d^+$. For $d = 3$ and $k = 1,2$ it gives the celebrated Choi witness which was proved to be also extremal (see also $[24]$ for another analysis of this witness).

**Example 2.** Consider the diagonal part

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

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

Interestingly, for $d = 3$ it was proved that if $p_0 = 1$ and $p_1 p_2 p_3 = 1$, then $W$ is also extremal $[22]$.

**Example 3.** Let $d = 3$ and consider

$$D_{[abc]} = \sum_{i=1}^3 |i\rangle \langle i| \otimes \left( (a + 1)|i\rangle \langle i| + b|i+1\rangle \langle i+1| + c|i+2\rangle \langle i+2| \right),$$

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

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

\[ W_1 = \frac{1}{4} \left[ I \otimes I + \sigma_z \otimes \sigma_z + (a^2 - b^2)\sigma_x \otimes \sigma_x \right. \]
\[ + \left. (a^2 - b^2)\sigma_y \otimes \sigma_y + 2ab(\sigma_z \otimes I + I \otimes \sigma_z) \right], \]

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

\[ W_3 = \frac{1}{4} \left[ I \otimes I + \sigma_z \otimes \sigma_z + (a^2 - b^2)\sigma_x \otimes \sigma_x \right. \]
\[ + \left. (a^2 - b^2)\sigma_y \otimes \sigma_y + 2ab(\sigma_z \otimes I + I \otimes \sigma_z) \right], \]

\[ W_4 = \frac{1}{4} \left[ I \otimes I - \sigma_x \otimes \sigma_x + (a^2 - b^2)\sigma_z \otimes \sigma_z \right. \]
\[ - \left. (a^2 - b^2)\sigma_y \otimes \sigma_y - 2ab(\sigma_x \otimes I - I \otimes \sigma_x) \right], \]

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

\[ W_6 = \frac{1}{4} \left[ I \otimes I - \sigma_y \otimes \sigma_y + (a^2 - b^2)\sigma_z \otimes \sigma_z \right. \]
\[ - \left. (a^2 - b^2)\sigma_x \otimes \sigma_x - 2ab(\sigma_y \otimes I - I \otimes \sigma_y) \right]. \]

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

\[ W = \alpha I \otimes I + \sum_{k=x,y,z} \left( a_k I \otimes \sigma_k + b_k \sigma_k \otimes I \right) \]
\[ + \sum_{k=x,y,z} c_k \sigma_k \otimes \sigma_k, \] (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:

\[ W = \sum_{\mu, \nu=0}^{3} T_{\mu \nu} \sigma_\mu \otimes \sigma_\nu, \] (B3)

with $\sigma_\mu \in \{I, \sigma_x, \sigma_y, \sigma_z\}$, and 16 real parameters $T_{\mu \nu}$.Witnesses of the form $W_1$ 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 \( \varphi \) can be decomposed as:
\[
|\varphi\rangle = e^{i\chi_0} m |00\rangle + e^{i\chi_1} n |01\rangle + e^{i\chi_2} q |10\rangle + t |11\rangle,
\]
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:
\[
\begin{align*}
|0\rangle \langle 0| &= \frac{1}{2} (I + \sigma_z) ;
|0\rangle \langle 1| &= \frac{1}{2} (\sigma_x + i\sigma_y) ;
|1\rangle \langle 0| &= \frac{1}{2} (\sigma_x - i\sigma_y) ;
|1\rangle \langle 1| &= \frac{1}{2} (I - \sigma_z) .
\end{align*}
\]
(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:
\[
\begin{cases}
m n \cos (\chi_0 - \chi_1) = q t \cos \chi_2 \\
m n \sin (\chi_0 - \chi_1) = q t \sin \chi_2 \\
q m \cos (\chi_0 - \chi_2) = n t \cos \chi_1 \\
q m \sin (\chi_0 - \chi_2) = n t \sin \chi_1 \\
n q \sin (\chi_1 - \chi_2) = 0 \\
m n \sin \chi_0 = 0.
\end{cases}
\]
(B6)

We remind that another equation is provided by the constraint \( m^2 + n^2 + q^2 + t^2 = 1 \), that express 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:
\[
m^2 + t^2 = 1, \quad n = q = 0, \quad \chi_0 = 0, \pi; \tag{B7}
\]
or
\[
n^2 + q^2 = 1, \quad m = t = 0, \quad \chi_2 - \chi_1 = 0, \pi. \tag{B8}
\]

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:
\[
\begin{align*}
qt \cos \chi_2 &= 0 \\
qt \sin \chi_2 &= 0 , \\
q^2 + t^2 &= 1
\end{align*}
\]
(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:
\[
|\varphi_m\rangle = m |00\rangle \pm t |11\rangle \quad \text{(B10)}
\]
and
\[
|\varphi_n\rangle = n |01\rangle \pm q |10\rangle . \quad \text{(B11)}
\]

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. \( \chi_1 = \chi_2 = 0, \pi \), in (B6). Besides (B7) and (B8), which can be restored, new solutions are linked to the condition \( \sin (\chi_0) = 0 \), i.e. \( \chi_0 = 0, \pi \).

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:
\[
n = \pm \sqrt{1 - 2m^2} ; q = \pm \sqrt{1 - 2n^2} ; \tag{B12}
\]
\[
t = - \frac{2abc}{2a^2 - 1} ; \chi_2 = 0, \pi; \tag{B13}
\]

In order to understand which states correspond to the above solution we consider the case \( n = q = \sqrt{1 - 2m^2} \), \( \chi_2 = \frac{\pi}{2} \) and therefore \( t = -m \). Equation (B9) becomes:
\[
|\varphi\rangle = m |00\rangle + i \sqrt{1 - 2m^2} (|01\rangle + |10\rangle) - m |11\rangle
\]
\[
= \sqrt{2m} \left( |00\rangle - |11\rangle \right) + i \sqrt{1 - 2m^2} \left( |01\rangle + |10\rangle \right) \tag{B14}
\]
\[
= \sqrt{2m} |\phi^-\rangle + i \sqrt{1 - 2m^2} |\psi^+\rangle
\]
\[
= a |\phi^-\rangle + ib |\psi^+\rangle
\]
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:
\[
|\varphi_1\rangle = a |\phi^+\rangle + b |\phi^-\rangle ; \quad |\varphi_2\rangle = a |\psi^+\rangle + b |\psi^-\rangle ; \tag{B15}
\]
\[
|\varphi_3\rangle = a |\phi^+\rangle + b |\psi^+\rangle ; \quad |\varphi_4\rangle = a |\phi^-\rangle + b |\psi^-\rangle ; \tag{B16}
\]
\[
|\varphi_5\rangle = a |\phi^+\rangle + ib |\psi^-\rangle ; \quad |\varphi_6\rangle = a |\phi^-\rangle + ib |\psi^+\rangle . \tag{B17}
\]

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.

\[
\square
\]

Appendix C: Proof of theorem 2

Any Hermitian operator \( X \) in \( \mathbb{C}^d \otimes \mathbb{C}^d \) may be represented as \( X = \sum_{\alpha, \beta=0}^{d-1} x_{\alpha \beta} G_\alpha \otimes G_\beta \), where the
\[ G_\alpha = \{ G_D^\alpha, G_S^\alpha, G_I^\alpha \} \] are the Generalized Gell-Mann (GGM) matrices, which can be divided into three types defined as follows: (i) diagonal matrices:
\[
G_D^l = \frac{1}{l(l+1)} \left( \sum_{j=1}^{l} |j\rangle \langle j| - l(l+1)|l+1\rangle \langle l+1| \right),
\]
for \(1 \leq l \leq d-1\); (ii) symmetric matrices:
\[
G_S^j_k = (|j\rangle \langle k| + |k\rangle \langle j|)/\sqrt{2}, \quad 1 \leq j < k \leq d
\]
and (iii) antisymmetric ones:
\[
G_A^j_k = (|j\rangle \langle k| - |k\rangle \langle j|)/i\sqrt{2}, \quad 1 \leq j < k \leq d.
\]
Assuming normalization \( Tr(X) = 1 \) one has
\[
X = \frac{1}{d^2} \left\{ \mathbb{I} \otimes \mathbb{I} + \sum_{\alpha,\beta=1}^{d^2-1} (a_\alpha G_\alpha \otimes \mathbb{I} + b_\alpha \mathbb{I} \otimes G_\alpha) + \sum_{\alpha,\beta=1}^{d^2-1} C_{\alpha\beta} G_\alpha \otimes G_\beta \right\},
\]
with real generalized Bloch vectors \( a_\alpha, b_\alpha \), 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:
\[
\sum_{\alpha,\beta} C_{\alpha\beta} G_\alpha \otimes G_\beta = \sum_{k,j=1}^{d-1} D_{kl} G_D^k \otimes G_D^j + \sum_{i<j} \left( S_{ij} G_S^{ij} \otimes G_S^{ij} + A_{ij} G_A^{ij} \otimes G_A^{ij} \right).
\]

**Theorem 2.** The following rank-1 projectors belong to \( C_1 \):
\[
\begin{align*}
|\varphi_1\rangle_j k &= a|\phi^+\rangle_j k + b|\phi^-\rangle_j k \\
|\varphi_2\rangle_j k &= a|\psi^+\rangle_j k + b|\psi^-\rangle_j k \\
|\varphi_3\rangle_j k &= a|\phi^+\rangle_j k + b|\psi^-\rangle_j k \\
|\varphi_4\rangle_j k &= a|\phi^-\rangle_j k + b|\psi^+\rangle_j k \\
|\varphi_5\rangle_j k &= a|\phi^+\rangle_j k + ib|\psi^-\rangle_j k \\
|\varphi_6\rangle_j k &= a|\phi^-\rangle_j k + ib|\psi^+\rangle_j k
\end{align*}
\]
where the real \( A \) and \( b \) satisfy \( a^2 + b^2 = 1 \). Vectors \(|\phi^\pm\rangle_j k\) and \(|\psi^\pm\rangle_j k\) represent four Bell states defined by \(|\phi^\pm\rangle_j k = (|jj\rangle \pm |kk\rangle)/\sqrt{2}\) and \(|\psi^\pm\rangle_j k = (|jj\rangle \pm |kk\rangle)/\sqrt{2}\). 

**Proof.** Without loss of generality we consider the state \(|\varphi_1\rangle_j k\). The projector on \(|\varphi_1\rangle_j k\) is given by:
\[
|\varphi_1\rangle_j k \langle \varphi_1| j k = \frac{1 + 2ab}{2} |jj\rangle \langle jj| + \frac{1 - 2ab}{2} |kk\rangle \langle kk| + \frac{(a^2 - b^2)}{2} (|jj\rangle \langle kk| + |kk\rangle \langle jj|).
\]
The projectors \(|jj\rangle \langle jj|\) and \(|kk\rangle \langle kk|\) contain only terms related to \( G_D^D \otimes G_D^D, G_I^D \otimes \mathbb{I}\) and \( \mathbb{I} \otimes G_D^D \), hence we can focus only on the remaining two projectors. From equations (C2) and (C3) we can see that the single system projector \(|jj\rangle \langle jj|\) can be expressed as:
\[
|jj\rangle \langle jj| = \frac{1}{2} \left( G_S^{jj} + iG_A^{jj} \right),
\]
and hence \(|jj\rangle \langle kk|\) is given by:
\[
|jj\rangle \langle kk| = \frac{1}{4} \left( G_S^{jj} \otimes G_S^{jj} + iG_A^{jj} \otimes G_A^{jj} \right) = \frac{1}{4} \left( iG_A^{jj} \otimes G_A^{jj} - G_S^{jj} \otimes G_S^{jj} \right).
\]
Its complex conjugated is thus given by:
\[
|kk\rangle \langle jj| = \frac{1}{4} \left( G_S^{jj} \otimes G_S^{jj} - iG_A^{jj} \otimes G_A^{jj} \right) = \frac{1}{4} \left( -iG_A^{jj} \otimes G_A^{jj} - G_S^{jj} \otimes G_S^{jj} \right),
\]
and hence their sum is:
\[
|jj\rangle \langle kk| + |jj\rangle \langle jj| = \frac{1}{2} \left( G_S^{jj} \otimes G_S^{jj} - G_A^{jj} \otimes G_A^{jj} \right),
\]
which contains only terms of the form \(|\varphi_1\rangle_j k\), and so do the projectors on \(|\varphi_1\rangle_j k\). Note that if we had considered a state of the form \(|\varphi_1\rangle_j k = a|\phi^+\rangle_j k + e^{ikb}|\phi^-\rangle_j k\), then its corresponding projector would have been expressed by
\[
|\varphi_1\rangle_j k \langle \varphi_1| j k = \frac{1 + 2ab}{2} |jj\rangle \langle jj| + \frac{1 - 2ab}{2} |kk\rangle \langle kk| + \frac{(a^2 - b^2 + 2iab \sin \chi)}{2} (|jj\rangle \langle kk| + |kk\rangle \langle jj|),
\]
which fits in the class \( C_n \) if and only if \( \chi = 0, \pi \). The same derivation, by using the properties of the GGM matrices, holds for any of the states \(|\varphi_m\rangle_j k\), \( m = 0, 1, 2, 3, 4, 5, 6 \) and \( 1 \leq j < k \leq d \).