Proposal of Universal Detection of Two-photon Polarization Entanglement

Karol Bartkiewicz,1, 2 Paweł Horodecki,3, 4 Karel Lerner,2 Adam Miranowicz,1 and Karol Życzkowski5, 6

1Faculty of Physics, Adam Mickiewicz University, PL-61-614 Poznań, Poland
2RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic, 17. listopadu 12, 772 07 Olomouc, Czech Republic
3Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, PL-80-233 Gdańsk, Poland
4National Quantum Information Centre in Gdańsk, 81-824 Sopot, Poland
5Institute of Physics, Jagiellonian University, ul Regensburg 4, PL-30-059 Kraków, Poland
6Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, PL-02-668 Warsaw, Poland

(Dated: December 1, 2014)

Detecting and quantifying quantum entanglement of a given unknown state poses problems that are fundamentally important for quantum information processing. Surprisingly, no direct (i.e., without quantum tomography) universal experimental implementation of a necessary and sufficient test of entanglement has been designed even for a general two-qubit state. Here we propose an experimental method for detecting a collective universal witness, which is a necessary and sufficient test of two-photon polarization entanglement. It allows us to detect entanglement for any two-qubit mixed state, and to establish tight upper and lower bounds on its amount. A novel element of this method is the sequential character of its main components, which allows us to obtain relatively complicated information about quantum correlations with the help of simple linear-optical elements. As such, this proposal is the first to realize a universal two-qubit entanglement test within the present state of the art of quantum optics. We show the optimality of our setup with respect to the minimal number of measured quantities.

PACS numbers: 03.67.Mn, 42.50.Dv

Introduction.— Quantum entanglement [1, 2] is a fascinating phenomenon considered to be one of the main resources in quantum information and quantum engineering (for reviews, see Refs. [3–5]). In general, detecting entanglement in various physical scenarios poses a significant problem. Most widely used methods are based on measuring entanglement witnesses (see Ref. [4]), which is efficient but requires some information about the state prior to its measurement. On the other hand, by performing standard methods of quantum tomography of a given state one obtains complete information about that state. Thus, information concerning its entanglement can be extracted by an explicit calculation, through the post-processing of the complete experimental data. However, full tomography requires measuring a large number of parameters; this number scales with the square of the total dimension of a measured state. Moreover, there remains one conceptually fundamental question, namely what is the minimal number of parameters that are experimentally feasible (in the sense of, e.g., linear optics) that will nevertheless provide complete information about quantum entanglement independently of a general input state. This can be viewed as a question about a quantum processor with a quantum input (state) and a classical output (giving a ‘yes/no’ answer or some quantitative information about entanglement) with minimal processing of classical (incoherent) information inside.

First proposals regarding the detection and quantification of quantum entanglement without state reconstructions were based on the identification of polynomial moments. These methods made it possible to retrieve information on entanglement from the data spectrum of the partial transpose of the two-qubit Wootters concurrence (see Refs. [6–8] for a significant quantum-noise reduction). They enabled sharp two-qubit entanglement tests, but required nonlinear postprocessing of the data to retrieve the original information about entanglement.

Independently of the above-mentioned line of research, the concept of collective entanglement witnesses [9] made it possible to construct collective observables for describing entanglement quantitatively in experiments [10]. Moreover, the analysis of the concurrence of Ref. [11] (see also Ref. [12] for recent developments) eventually led to a quantitative experimental estimation of entanglement in terms of specific two-copy collective witnesses [13, 14].

Another interesting example of collective entanglement witnesses is a two-copy witness based on the geometric intuition of the concept of metric [15]. A number of multipartite tests based on the nonlinear functions of simple multicopy observables were developed [16], and several quantitative methods of detecting entanglement without quantum tomography were proposed. Nevertheless, these techniques, although quite powerful, are not universal and the quality of their results depends on a given state.

Experimental adaptive approaches were also proposed for the case of two-qubits which we shall focus on in this Letter [21, 25]. Although these methods are an elegant
improvement, they do not satisfy the universality requirement.

Let us stress, however, that there exists a universal entanglement witness for a two-qubit state that requires joint measurements on the four copies of the state. This witness, provided in Ref. [20], is an operator the expected value of which is $\det \rho^{T} = \langle W^{(4)}_{\text{univ}} \rangle := \text{tr}(W^{(4)}_{\text{univ}} \rho^{\otimes 4})$

$$= \frac{1}{27}(1 - 6\Pi_1 + 8\Pi_3 - 3\Pi_2^2 - 6\Pi_2),$$  \hspace{1cm} (1)

where $\Pi_n = \text{tr}(\rho^{n})$ are the moments of a partially-transposed (marked by $\Gamma$) two-qubit matrix $\rho$. It follows from the positive partial transpose (PPT) criterion that a two-qubit state is entangled if and only if $\langle W^{(4)}_{\text{univ}} \rangle < 0$.

The explicit form of this witness, which is the mean value of the Hermitian observable $W^{(4)}_{\text{univ}}$ on the four copies $\rho^{\otimes 4}$ of qubit pairs in a given state $\rho$, is explicitly provided in Ref. [20] and constructed from permutation matrices. The main advantage of this universal witness compared to other universal methods of two-qubit entanglement detection is that this is a linear observable that does not require solving ("unfolding") nonlinear polynomial equations, which are more sensitive to errors, to obtain the information about a given state (see Refs. [5,5]).

Another advantage of this witness is that its rescaled value $w := \max_{0, -16(W^{(4)}_{\text{univ}})}$ provides tight upper and lower bounds [20] on the negativity $N(\rho)$ and concurrence $C(\rho)$ of a two-qubit state $\rho$.

$$f(w) \leq N \leq C \leq \sqrt{w},$$  \hspace{1cm} (2)

where $f(w)$ is the inverse of the polynomial $w(C) = C(C + 2)^3/27$ on the interval $C \in [0, 1]$ as given explicitly in the supplement [28].

However, so far no experimental implementation for such a measurement has been proposed. The aim of this letter is to propose a constructive measurement procedure that outputs the mean value $\langle W^{(4)}_{\text{univ}} \rangle$ of the above witness for any two-qubit polarization state of a pair of photons, allowing thereby to detect the arbitrary quantum entanglement of such systems. To our knowledge this is the first experimental proposal of a universal (sharp) entanglement test with (i) elementary (linear) optics and (ii) practically trivial (direct substitution to polynomial) postprocessing of experimental data. To be more specific, the procedure has the unique advantage that it can be (probabilistically) utilized with the help of just linear-optical methods involving only a sequence of beam-splitters and the Hong-Ou-Mandel (HOM) interference. Quite remarkably, no polarizing beam splitters or phase rotators are needed. This is especially important here because we consider only the polarization-encoded qubits.

We start the presentation of our results with the analysis of the symmetries of the observables needed for reproducing the three moments $\Pi_i$ ($i = 2, 3, 4$). Then we shall provide the optical HOM interference methods for reproducing the values of the moments. Having found these values, one just needs to substitute them into the polynomial [1] and to check the sign of the final value.

Theoretical analysis.— To directly determine the witness $\langle W^{(4)}_{\text{univ}} \rangle$, we can measure all the moments $\Pi_n = \text{tr}(\rho^{n})$ separately. We know how to measure $\Pi_2$ (see Ref. [27]), since it is equivalent to the purity of $\rho = \rho_{a_1,b_1}$. The remaining problem is how to measure $\Pi_{3,4}$. As already mentioned, these moments were originally reproduced as the mean values of the observables constructed from permutation operators. However, the direct measurement of the observables seems to be difficult due to their relatively complicated structure. Fortunately, we can express the moments $\Pi_n$ (for $n = 3, 4$) differently, i.e., by decomposing the $n$th cycle into the products of inversions (the swap operations $S$) as follows

$$\Pi_n = \text{tr}(A_n B_n \rho^{\otimes n}),$$  \hspace{1cm} (3)

where $n = 2, 3, 4$ and

$$A_2 = S_{a_1,a_2} \otimes I_{b_1} \otimes I_{b_2},$$

$$B_2 = I_{a_1} \otimes I_{a_2} \otimes S_{b_1,b_2},$$

$$A_3 = S_{a_1,a_2} \otimes I_{a_3} \otimes I_{b_1} \otimes S_{b_2,b_3},$$

$$B_3 = I_{a_1} \otimes S_{a_2,a_3} \otimes S_{b_1,b_2} \otimes I_{b_3},$$

$$A_4 = S_{a_1,a_2} \otimes S_{a_3,a_4} \otimes I_{b_1} \otimes S_{b_2,b_3} \otimes I_{b_4},$$

$$B_4 = I_{a_1} \otimes S_{a_2,a_3} \otimes I_{a_4} \otimes S_{b_1,b_2} \otimes S_{b_3,b_4},$$

(4)

together with the swap operator $S = |HH\rangle\langle HH| + |HV\rangle\langle VH| + |VH\rangle\langle HV| + |VV\rangle\langle VV|$ and the single-qubit identity operator $I$, where $H$ and $V$ are horizontally and vertically polarized photons, respectively. The products $A_n B_n$ are not Hermitian for $n = 3, 4$, so they cannot be measured directly. However, the operators $A_n$ and $B_n$ taken separately are Hermitian and have other useful properties, i.e., $\text{tr}(A_n B_n \rho^{\otimes n}) = \text{tr}(B_n A_n \rho^{\otimes n})$ and $A_2^2 = B_2^2 = I^{\otimes n}$. By applying these properties we can express higher-order moments of the partially-transposed matrix as

$$\Pi_n = \frac{1}{2} \text{tr}[(A_n + B_n)^2 \rho^{\otimes n}] - 1, \hspace{1cm} n = 3, 4.$$  \hspace{1cm} (5)

Note that this method displays some analogy to the method of calculating the collective spin of two parties. Let us denote $X_n = (A_n + B_n)^2$. Then, in order to measure these two moments, we have to perform projections on the eigenspaces of $X_3$ and $X_4$. The implementation of these operations might be difficult for two reasons: (i) the large number of different eigenvalues of the operators $X_n$ (positive-valued measures, POVMs), and (ii) the complicated structure of the corresponding eigenspaces with the eigenvectors corresponding to entangled multi-qubit states. Fortunately, the operator $X_3$ has only two different eigenvalues ($1, 4$), resulting in two eigenspaces; and the operator $X_4$ has only three different eigenvalues ($0, 2, 4$), hence it has three eigenspaces. Therefore,
one has to perform only the measurement of five projections on some of the eigenspaces to measure both $\Pi_3$ and $\Pi_4$. The remaining problem is to find the eigenspaces and associate them with the specific settings of a multithoton interferometer. Measuring the second moment $\Pi_2$ requires two projections. Thus, the complete measurement of $W_{\text{uni}}^{(4)}$ can be decomposed into seven projections (this value may be even lower if some optimization is applied) onto subspaces spanned by highly entangled multiqubit states, which is twice as efficient as a full two-qubit tomography. There is, however, another method of measuring the products of $A_n$ and $B_n$ for $n = 3, 4$ which is better regarding the complexity of these projections. We can express $A_n = P^+_n - P^-_n$ in terms of the projectors onto the symmetric ($P^+_n$) and antisymmetric ($P^-_n$) subspaces. Then, we can show \cite{28} that

$$\Pi_n = \text{tr}[B_n P^+_n \rho^{(n)} P^+_n] - \text{tr}[B_n P^-_n \rho^{(n)} P^-_n] \quad (6)$$

for an arbitrary $\rho$. It is convenient to denote $P^\pm_{m,n} = \frac{1}{2}(I_{m,n} \otimes I_{m,n} \pm S_{m,a,a})$ and $P^\pm_{m,n} = \frac{1}{2}(I_{m,n} \otimes I_{m,n} \pm S_{m,b,b})$. Then the symmetric ($P^+_n$) and antisymmetric ($P^-_n$) projectors for $n = 3, 4$ read as

$$P^\pm_3 = P^\pm_{1,2} \otimes P^\pm_{2,3},$$

$$P^\pm_4 = P^\pm_{1,4} \otimes P^\pm_{3,4}.$$  

(7)  

(8)

For the operator $B_n = \bar{P}^+_n - P^-_n$, we can apply the same procedure but with the subsystems of the multiqubit density matrix swapped as $a \leftrightarrow b$. Then, we have

$$\Pi_n = \text{tr}(\bar{P}^+_n Q \bar{P}^+_n) - \text{tr}(\bar{P}^-_n Q \bar{P}^-_n), \quad (9)$$

where $Q = P^+_n \rho^{(n)} P^+_n - P^-_n \rho^{(n)} P^-_n$, which means that

$$\Pi_n = \sum_{x,y=0} (-1)^x y \text{tr}[\bar{P}^x \bar{P}^y \rho^{(n)} \bar{P}^y \bar{P}^x], \quad (10)$$

where $\bar{P}^0_n = \bar{P}^+_n$ and $\bar{P}^1_n = \bar{P}^-_n$. Thus, it appears to be more convenient to project $\rho^{(n)}$ onto the symmetric or antisymmetric subspace of $A_n$ first, and then to measure $B_n = \bar{P}^+_n - \bar{P}^-_n$, as shown in Fig. 1.

**A proposal of experimental implementation.**—The analyzed projections $P^\pm_n$ are not the products of projections (except $n = 2$), thus they cannot be implemented by local (two-qubit) operations. Let us note that the $P^\pm_n$ projectors split a collective multiqubit state into the states of positive and negative parities. This technique was also applied to, e.g., the cluster-state preparation \cite{30}.

We can, however, measure $B_3 P^\pm_3$ directly as shown in Fig. 2. Note that $B_3$ can be measured using only beam splitters and photon detectors analogously to the methods applied in Refs. \cite{27, 31}. In Figs. 2 and 3 we show a simple implementation of a $B_n$ block (for $n = 3, 4$). To measure the three parameters from Fig. 1 (four parameters without normalization) instead of using the $B_n$ block we can reuse the $P^\pm_n$ part of the relevant scheme to perform a $\bar{P}^\pm_n$ projection (see Ref. \cite{28}).

For any $P^\pm_n$, two qubits $a_1$ and $a_n$ ($b_k$) for even (odd) $n$ can be destroyed in this process. In the most complex case of $P^\pm_4$, we have to perform a nondestructive parity test on six qubits, where two of them can be destroyed before measuring $B_4$. The measurement of $B_4 P^\pm_4$ is more challenging than that of $\Pi_3$. In the comparison to the $\Pi_3$ setup the main difficulty here is the necessity to condition the outcome of nondestructive measurements on $b_2$ and $b_3$. This is because both $b_2$ and $b_3$ are required in the latter part of the $\Pi_4$ measurement. We can solve this problem by using ancillary photons prepared in the polarization singlet state in the modes $c_1$ and $c_2$. The corresponding setup is shown in Fig. 3. In some experimental approaches, this setup can be further simplified by applying, e.g., the time-bin methods \cite{8, 32}. Our alternative proposal is discussed in the Supplement \cite{28}. Finally, note that the relevant moments $\Pi_n$ can be measured with the subblocks of the setup in Fig. 3 if some
the first detection mode and there is a photon in the second detectors $D_3$. Assume that this is done by using photon-number-resolving detectors $D_4$. Here we assume that the measurement multiplied by $1$ (Ref. [28]). If the even (odd) number of photons is passed to the detection mode of the second BS, the output state becomes $\rho_{a,b}^P \rho_{a,b}^P$. However, if there is no photon in the first detection mode and there is a photon in the second detection mode, the output state becomes $\rho_{a,b}^P \rho_{a,b}^P$. The setup works if both the detectors $D_1$ and $D_2$ register a photon, and it is unknown from where the photons have arrived. The $B_3$ part is implemented by distinguishing between $P^+$ and $P^-$ by means of detecting bunching and antibunching, respectively. The information about parities of individual photon pairs can be erased as described in Ref. [28]. Here we assume that this is done by using photon-number-resolving detectors $D_4^{(a)}$, but this can also be done probabilistically using bucket detectors [8, 27]. Thus, assuming perfect detectors, one needs two measurements to determine $\Pi_3$. Finally, neutral density filters $F$ of the transmittance $1/2$ ensure that the setup works with probability $1/16$.

The setup works if both the detectors $D_1$ and $D_2$ register a photon, and it is unknown from where the photons have arrived. The $B_3$ part is implemented by distinguishing between $P^+$ and $P^-$ by means of detecting bunching and antibunching, respectively. The information about parities of individual photon pairs can be erased as described in Ref. [28]. Here we assume that this is done by using photon-number-resolving detectors $D_4^{(a)}$, but this can also be done probabilistically using bucket detectors [8, 27]. Thus, assuming perfect detectors, one needs two measurements to determine $\Pi_3$. Finally, neutral density filters $F$ of the transmittance $1/2$ ensure that the setup works with probability $1/16$.

The setup works if both the detectors $D_1$ and $D_2$ register a photon, and it is unknown from where the photons have arrived. The $B_3$ part is implemented by distinguishing between $P^+$ and $P^-$ by means of detecting bunching and antibunching, respectively. The information about parities of individual photon pairs can be erased as described in Ref. [28]. Here we assume that this is done by using photon-number-resolving detectors $D_4^{(a)}$, but this can also be done probabilistically using bucket detectors [8, 27]. Thus, assuming perfect detectors, one needs two measurements to determine $\Pi_3$. Finally, neutral density filters $F$ of the transmittance $1/2$ ensure that the setup works with probability $1/16$.

Note that local qubit unitary operations have three relevant independent real parameters (excluding global phase). Thus, number of parameters of $U_A \otimes U_B$ is six while the total number of parameters of a mixed two qubit state is 15. The resulting $9 = 15 - 6$ parameters are exactly all the relevant ones after introducing the $U_A \otimes U_B$ invariant equivalence classes, and they correspond to the nine fundamental invariants. This number of parameters can be further reduced by swapping the subsystems of $\rho$.

This is probably the reason behind the minimalistic character of this method. Indeed, it requires no unitary operations, which may reflect the symmetry of the problem under local unitary operations. Because of its simplicity, we believe that the presented setup paves the way for the first experimental realization of a necessary and sufficient universal test of entanglement.

Finally, let us underscore that the key feature responsible for the success of the proposed approach is the sequential character of measurements. It seems that this property of the setup reframes the paradigm for entanglement, correlations and any other nonlocal (i.e., not depending solely on the reduced density matrices of subsystems) property of quantum-state detection and/or estimation in practice. As a result a more general problem can be conceived of. Given only very specific measurement modules (analogous to a beam-splitter in the Hong-Ou-Mandel interference experiment) which can be
repeated in different subsystems, is it possible to estimate nonlocal quantities and, if so, what setup would minimize the number of required measurements?

We gratefully acknowledge the financial support of the Polish National Science Centre under grants DEC-2011/03/B/ST2/01903 (AM), DEC-2013/11/D/ST2/02638 (KB), and DEC-2011/02/A/ST2/00305 (KZ), the Czech Science Foundation (Grant No. 13-31000P) (KL), as well as the support by the Czech Ministry of Education under grant No. LO1305 (KB) and the Quasar: Era-Net Chist-Era 7FP UE (PH).

* Electronic address: bark@amu.edu.pl

---

[28] For our other proposals of experimental setups and for more detailed technical information, see Supplemental Material.
Supplementary material:

In this supplement we present explicitly the tight lower bound $f(w)$ for the two-qubit negativity and concurrence in terms of the universal witness value $w$. We also propose alternative setups for measuring the moments $\Pi_4$ and $B_{3(4)}$. Finally, we give the more technical details on deriving some expressions used in the main text.

UNIVERSAL WITNESS AND BOUNDS ON NEGATIVITY AND CONCURRENCE

The lower bound $f(w)$, in Eq. (2), can be given explicitly in terms of the universal witness value $w$ as follows

$$f(w) = \frac{1}{2} \left( -3 + \sqrt{z} + \sqrt{3 - z + \frac{2}{\sqrt{z}}} \right),$$

where $z = 1 + x - y$, $y = 36w/x$, and

$$x = 3^\frac{3}{2}\left(2\sqrt{w^2(16w+1)} - 2w\right).$$

This lower bound, together with the upper bound, are shown in Fig. 4.

ALTERNATIVE SETUP FOR MEASURING $\Pi_4$

The setup depicted in Fig. 3 of the Letter is fairly efficient and experimentally not overly demanding. Unfortunately, it requires the photon-number parity measurement, which (i) is experimentally challenging and (ii) photon losses in the setup can result in incorrect measurement outcome. Especially the second limitation hinders the implementation of the method since photon losses and imperfect detection efficiencies are unavoidable in real experiments.

To overcome this problem, in addition to the time-bin approach mentioned in the Letter, we have devised another setup, as shown in Fig. 5 for the direct measurement of the $B_4P_4^\pm$ term. In contrast to the previous setup, shown in Fig. 3, no parity measurement is required. On the other hand, the new setup is much more complex and requires interferometric stability (at some places). The idea behind the method is to use two quantum gates: the controlled-NOT (CNOT) gate [1–4] and the exclusive OR (XOR) gate [5]. In order to join two CNOT gates, it is also required to introduce the nonde- moliotion photon presence detection gate, which uses two additional ancillae in a Bell state [6,7]. By heralding the presence of a qubit, this gate informs that the preceding CNOT operation was successful. The entire measurement method is successful if two photons are detected by each detector pair among $D_1$, $D_3$ and $D_4$, while one photon is detected by either of the $D_2$ detectors and the presence detection gate also heralds a photon. Further, if the detector $D_2^b$ fires, the method performs the $B_4P_4^+$ measurement, while if the photon impinges on the $D_2^b$ detector, the setup implements the $B_4P_4^-$ measurement.

ALTERNATIVE IMPLEMENTATION OF THE $B_{3(4)}$ BLOCK

If we take a look at the $B_n$ blocks with $n = 3, 4$ in Figs. 2 and 3, respectively, we will discover that we check for bunching and antibunching separately for each photon pair. Additionally to the information about the outcome of the $\bar{D}_n^\pm$ projections, we obtain the information about which of the photon pairs is bunched or antibunched. We do not use the which-pair information in any way (we just need to know how many pairs bunched or antibunched) and this measurement is not difficult to implement. However, one may argue that we gain more knowledge from our measurement that it is necessary to measure $\Pi_n$.

To perform the $B_n$ measurement and not to distinguish between the pairs of photons one would have to use the same block as for the $P_n^\pm$ measurement and to swap the modes $a \leftrightarrow b$ to perform the $P_n^\pm$ projections. This procedure would result in the following four separate detection events: $P_n^+P_n^+, P_n^+P_n^-, P_n^-P_n^+$, and $P_n^-P_n^-$ [see Eq. (10) in the main text] associated with the single observable $\Pi_n$. This number of the detection events is now smaller that in the case of analyzing bunching and antibunching for each pair at the original $B_n$ blocks. The drawback of this method is that it is more experimentally challenging. However, by using the time-bin approach, analogously to that applied in Ref. [8], we could reuse the same physical $P_n^\pm$ setup to measure $P_n^\pm$ at a later moment of time. To summarize, we may iterate the block measuring $P_n^\pm$ to get exactly the statistics corresponding only to four exclusive events.
In order to derive Eq. (6) of the main text, let us start by noting that

\[ \text{tr}(B_n A_n \rho^{\circ n}) = \text{tr} \left[ B_n A_n (\rho^{\circ n})' \right], \]

where the statistical operator

\[ \rho^{\circ n}' = \frac{1}{2} (\rho^{\circ n} + A_n \rho^{\circ n} A_n), \]

can be implemented by alternating between the input state \( \rho^{\circ n} \) and \( A_n \rho^{\circ n} A_n \) (qubits are swapped according to the definition of \( A_n \)). The newly obtained density matrix \( \rho^{\circ n}' \) has a very important property, i.e., it commutes with the operator \( A_n \):

\[ [A_n, (\rho^{\circ n})'] = \frac{1}{2} \left( [A_n, \rho^{\circ n}] + [\rho^{\circ n}, A_n] \right) = 0. \]

Thus, the two operators have a common set of eigenvectors \( |\psi_m^{(n)}\rangle \) for \( m = 1, 2, \ldots, 4^n \), i.e., they are both diagonal in the same basis. Let us expand the expression \( \text{tr}[B_n A_n (\rho^{\circ n})'] \) using the following diagonal representations of the operators \( A_n = \sum_{k,l,m} a_k^{(n)} |\psi_k^{(n)}\rangle \langle \psi_l^{(n)}| \) and \( B_n = \sum_{k,l,m} b_k^{(n)} |\phi_l^{(n)}\rangle \langle \phi_l^{(n)}| \) and \( (\rho^{\circ n})' = \sum_{m} \psi_m^{(n)} \langle \psi_m^{(n)}| \langle \psi_m^{(n)}| \).

By doing so, we arrive at

\[ \text{tr} [B_n A_n (\rho^{\circ n})'] = \sum_{k,l,m} \text{tr}(a_k^{(n)} b_l^{(n)} \psi_m^{(n)} \langle \phi_l^{(n)}| \langle \psi_m^{(n)}| \langle \psi_l^{(n)}| \langle \phi_l^{(n)}| \rangle) \]

\[ = \sum_{k,l} a_k^{(n)} b_l^{(n)} r_k^{(n)} |\langle \phi_l^{(n)}| \langle \psi_l^{(n)}| \rangle|^2. \]

This is equivalent to a measurement strategy consisting of measuring \( A_n \) first, and then measuring \( B_n \), which can be expressed as

\[ \sum_{k} \text{tr} \left[ B_n a_k^{(n)} |\psi_k^{(n)}\rangle \langle \psi_k^{(n)}| (\rho^{\circ n})'| \langle \psi_k^{(n)}| \langle \psi_k^{(n)}| \right) \]

\[ = \sum_{k,l} a_k^{(n)} b_l^{(n)} r_k^{(n)} |\langle \phi_l^{(n)}| \langle \psi_l^{(n)}| \rangle|^2. \]

The operator \( A_n \) has degenerated eigenvalues, which makes its set of eigenvectors not unique, i.e., any linear combination of two eigenvectors associated with the same eigenvalue is an eigenvector itself. Thus, finding the basis \( \{ \psi_k^{(n)} \} \), in which both \( A_n \) and \( (\rho^{\circ n})' \) are diagonal, seems to be a difficult problem that depends on the particular form of \( \rho \). So, this approach is not universal. However, now we can express \( A_n = P_n^+ - P_n^- \) in terms of the projectors onto the symmetric \( (P_n^+) \) and antisymmetric \( (P_n^-) \) subspaces. From the above, it follows that

\[ \Pi_n = \text{tr}[B_n P_n^+ (\rho^{\circ n})' P_n^+] - \text{tr}[B_n P_n^- (\rho^{\circ n})' P_n^-]. \]
Moreover we can see that
\[ P_n^\pm (\rho^{(n)})' P_n^\pm = P_n^\pm \rho^{(n)} P_n^\pm. \] (19)

Therefore, we derive Eq. (6) of the main text, i.e.,
\[ \Pi_n = \text{tr}[B_n P_n^+ \rho^{(n)} P_n^+] - \text{tr}[B_n P_n^- \rho^{(n)} P_n^-]. \] (20)

MAKHLIN'S INVARIANTS AND THE MINIMAL NUMBER OF INDEPENDENT MEASUREMENTS

The moments \( \Pi_{1,2,3,4} \) are not independent quantities. In order to demonstrate this property, let us express the two-qubit density matrix \( \rho \) in terms of the Pauli matrices \( \sigma_i \) for \( i = 1, 2, 3 \) and the single-qubit identity matrix \( \sigma_0 \). The resulting matrix reads
\[ \rho = \frac{1}{2} \sigma_0 \otimes \sigma_0 + \frac{1}{2} s_i \sigma_i \otimes \sigma_0 + \frac{1}{2} p_j \sigma_0 \otimes \sigma_j + \beta_{ij} \sigma_i \otimes \sigma_j, \] (21)

where the elements of the correlation matrix \( \beta \) are \( \beta_{ij} = \text{tr}[(\sigma_i \otimes \sigma_j)\rho] \) and the Bloch vectors \( s \) and \( p \) have the following elements of \( s_i = \text{tr}[(\sigma_i \otimes \sigma_0)\rho] \) and \( p_j = \text{tr}[(\sigma_0 \otimes \sigma_j)\rho] \), respectively. It can be directly shown, after tedious calculations, that
\[ \Pi_1 = 1, \]
\[ 4\Pi_2 = 1 + x_1, \]
\[ 16\Pi_3 = 1 + 3x_1 + 6x_2, \]
\[ 64\Pi_4 = 1 + 6x_1 + 24x_2 + x_1^2 + 2x_3 + 4x_4, \] (22)

where
\[ x_1 = I_2 + I_4 + I_7, \quad x_2 = I_1 + I_{12}, \]
\[ x_3 = I_2^2 - I_3, \quad x_4 = I_5 + I_8 + I_{14} + I_4 I_7. \] (23)

are functions of nine local invariants of the two-qubit matrix \( \rho \) as defined by Makhlin in Ref. [9], i.e., \( I_1 = \text{det} \hat{\beta}, I_2 = \text{tr}(\hat{\beta}^T \hat{\beta}), I_3 = \text{tr}(\hat{\beta}^T \hat{\beta})^2, I_4 = s^2, I_5 = [s \hat{\beta}]^2, I_7 = p^2, I_8 = [\hat{\beta}p]^2, I_{12} = s \hat{\beta} p, \) and \( I_{14} = e_{ijk} e_{lmn} s_i p_j \beta_{jm} \beta_{kn} \), where \( e_{ijk} \) is the Levi-Civita symbol. It is apparent that only six (instead of nine) linear combinations of Makhlin’s invariants need to be measured to estimate the values of \( x_n \) for \( n = 1, 4 \). These invariants read
\[ y_1 = I_2, \quad y_2 = I_8, \quad y_3 = I_4, \quad y_4 = I_7, \]
\[ y_5 = I_1 + I_{12}, \quad y_6 = I_5 + I_8 + I_{14}. \] (24)

Thus, in order to detect the entanglement via \( \text{det} \rho^\Gamma \), one needs to measure exactly six instead of nine independent linear combinations of fundamental invariants. It also happens that this is also the minimal number of independent fundamental quantities describing negativity of an arbitrary two-qubit state [10].

* Electronic address: bark@amu.edu.pl