9-6-2011

Extracting an Entanglement Signature from Only Classical Mutual Information

David J. Starling
University of Rochester

Curtis J. Broadbent
University of Rochester

John C. Howell
Chapman University, johhowell@chapman.edu

Extracting an Entanglement Signature from Only Classical Mutual Information

Comments

This article was originally published in *Physical Review A*, volume 84, issue 3, in 2011. https://doi.org/10.1103/PhysRevA.84.032305

Copyright

Extracting an entanglement signature from only classical mutual information

David J. Starling,[1] Curtis J. Broadbent,[1,2] and John C. Howell[1]
[1]*Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627, USA*
[2]*Rochester Theory Center, University of Rochester, Rochester, New York 14627, USA*
(Received 26 April 2011; published 6 September 2011)

We introduce a quantity which is formed using classical notions of mutual information and which is computed using the results of projective measurements. This quantity constitutes a sufficient condition for entanglement and represents the amount of information that can be extracted from a bipartite system for spacelike separated observers. In addition to discussion, we provide simulations as well as experimental results for the singlet and maximally correlated mixed states.

DOI: 10.1103/PhysRevA.84.032305 PACS number(s): 03.67.Bg, 42.65.Lm, 42.50.Ex

I. INTRODUCTION

Mutual information and the Shannon entropy were first laid out in Shannon's seminal 1948 paper [1] and have since fueled research in many areas of classical [2] and quantum information theory [3–5]. Although quantum information theory has many analogies to its classical counterpart, it relies upon the density matrix formalism and von Neumann entropy, rather than on probabilities and the Shannon entropy. It is for this reason that the information capacity of quantum systems can exceed that of classical systems in some practical applications, such as dense coding [6,7]. Quantifying quantum correlations is therefore critical to understanding when and how they may be used advantageously in information processing tasks.

To determine the extent to which a system exhibits quantum correlations, one can consider the "quantum excess" expressed as the quantum discord [8–10]. The quantum discord can be understood as follows. There exist two, classically equivalent definitions of mutual information: I, which is based upon joint measurements, and J, which is based upon conditional measurements. In the quantum framework, these two definitions are *not* equivalent. The excess of mutual information predicted by I relative to J is what is known as the quantum discord δ. A nonzero value of δ is an indication of nonclassicality, but not an indication of entanglement [10,11]. For this reason, it is clear that the quantity J—in both the classical and quantum frameworks—represents only the classical part of the correlations between two parties. It has also been shown that a nonzero discord (not entanglement) is sufficient for quantum speedup [9] and sophisticated quantum searches [12,13]; we therefore consider the effect of entanglement on classical mutual information.

In what follows, we show how to identify nonclassical correlations in a quantum state using *only Shannon entropy*. In Sec. II, we summarize the various descriptions of mutual information from a measurement point of view and then show how to extract an entanglement signature by summing J taken from measurements (see Fig. 1) in three mutually unbiased bases. This sum constitutes a sufficient condition for the entanglement of a state. This recently defined quantity bears some resemblance to Ref. [14], where the use of six states offers an improvement over the so-called Bennett and Brassard 1984 (BB84) quantum cryptographic protocol [15]. Similarly, there has been related work on the geometry of spin vectors to quantify the entanglement of a large number of photons [16,17]. In Sec. III, we compare a variety of entangled states by correlating concurrence [18], an entanglement measure, with the aforementioned sum. In Sec. IV, we provide experimental data from spontaneous parametric down conversion (SPDC).

II. THEORY

Mutual information is a measure of how much information a random variable A, with probability distribution $p(a)$, has in common with another random variable B with probability distribution $p(b)$; the joint probability distribution is written as $p(a,b)$. The classical mutual information can then be expressed by

$$I_C(A,B) = H(A) + H(B) - H(A,B), \tag{1}$$

where

$$H(A) = -\sum_{a\in A} p(a)\log p(a) \tag{2}$$

is the marginal Shannon entropy of the random variable A and

$$H(A,B) = -\sum_{a\in A}\sum_{b\in B} p(a,b)\log p(a,b) \tag{3}$$

is the joint Shannon entropy of A and B. All logarithms are taken base 2 so that H is measured in units of bits. A classically equivalent definition of I_C follows from Baye's rule [2]:

$$J_C(A,B) = H(A) - H(A|B), \tag{4}$$

where $H(A|B)$ is the conditional entropy, computed as

$$H(A|B) = -\sum_{a\in A, b\in B} p(a,b)\log \frac{p(a,b)}{\sum_{a\in A} p(a,b)}. \tag{5}$$

The conditional entropy is an average measure of how uncertain we are about the random variable A given the knowledge of random variable B. In the context of optics, the random variables may represent the results of polarization measurements, say $a \in A = \{h,v\}$, for horizontal and vertical directions, respectively.

The *quantum* mutual information is given by

$$I(\rho) = S(\rho^A) + S(\rho^B) - S(\rho), \tag{6}$$

where $S(\rho) = -\mathrm{Tr}(\rho\log\rho)$ is the von Neumann entropy, $\rho = \rho^{AB}$ is the composite density matrix of the two subsystems, and, e.g., ρ^A is the density matrix for subsystem A found by

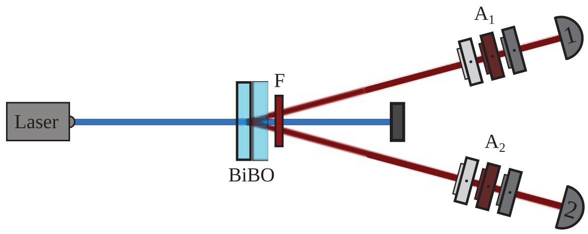

FIG. 1. (Color online) Entangled photons are generated by two bismuth borate (BiBO) nonlinear crystals in two spatial modes (1 and 2). The down-converted photons are frequency filtered (F) and then analyzed in polarization (A_1 and A_2) before detection and correlation. The physical design employs collinear down conversion and a 50:50 beam splitter to separate the two photons.

tracing over the states of subsystem B. Due to the subadditivity of S, the entropy of the joint density matrix ρ is always less than or equal to the sum of the marginal entropies, $S(\rho^{A,B})$ [19].

To motivate the quantum and classical forms of *conditional* mutual information [11], consider a complete projective measurement $\{\Pi_b^B\}$ performed on subsystem B of the quantum state ρ. The expression for the measured state is simply

$$\rho' = \sum_b \Pi_b^B \rho\, \Pi_b^B, \tag{7}$$

where the sum extends over the whole space of subsystem B. Since the von Neumann entropy reduces to the Shannon entropy after projective measurements on ρ, it is straightforward to verify that

$$I(\rho') = J(\rho)_{\{\Pi_b^B\}} := S(\rho^A) - S\big(\rho\big|\{\Pi_b^B\}\big), \tag{8}$$

where we define the conditional entropy as

$$S\big(\rho\big|\{\Pi_b^B\}\big) = \sum_b p(b) S(\rho_b), \tag{9}$$

$$\rho_b = \frac{\Pi_b^B \rho\, \Pi_b^B}{\mathrm{Tr}\big[\rho\, \Pi_b^B\big]}, \tag{10}$$

and $p(b) = \mathrm{Tr}[\Pi_b^B \rho]$. We can then identify the right hand side of Eq. (8) as the quantum definition of conditional mutual information described, for example, in Ref. [11] [their Eq. (11)].

If we also measure subsystem A with a complete projective measurement $\{\Pi_a^A\}$, we find that

$$\rho'' = \sum_a \Pi_a^A \rho' \, \Pi_a^A = \sum_{a,b} p(a,b)\, \Pi_a^A\, \Pi_b^B, \tag{11}$$

where $p(a,b) = \mathrm{Tr}[\Pi_a^A \Pi_b^B \rho]$. It is also straightforward to verify that

$$I(\rho'') = J_C(\rho)_{\{a,b\}} := H(A) - H(A|B), \tag{12}$$

where the subscript $\{a,b\}$ indicates the measurement bases. We note that $I(\rho'')$ is equivalent to the classical mutual information I_C defined in Eq. (1).

For a bipartite, two-state system, $J(\rho)_{\{\Pi_b^B\}}$ is bounded by 1 bit. Since the choice of orthonormal projectors $\{\Pi_b^B\}$ can affect its value, we typically consider the maximum of this quantity, optimized over all possible orthonormal projectors:

$$\tilde{J}(\rho) = \max_{\{\Pi_b^B\}} \big[J(\rho)_{\{\Pi_b^B\}}\big]. \tag{13}$$

This form of mutual information can only account for the classical correlations of the state; this is apparent, for instance, in the definition of the quantum discord, which is a measure of nonclassical correlations in a quantum state: $\delta = I(\rho) - \tilde{J}(\rho)$. Nevertheless, we demonstrate how J and J_C for two qubits can lead to significantly different predictions between entangled and separable states when summed in different bases.

Let us consider a maximally entangled state ρ. For such a state, the conditional entropy is zero, which can be seen by noting that ρ_b is pure for all b [so $S(\rho_b) = 0$] when ρ is measured projectively in any basis $\{\Pi_b^B\}$. Additionally, the marginalized state ρ^A is fully mixed, giving $S(\rho^A) = 1$. Therefore, the measured mutual information in Eq. (8) is maximal in any basis. However, for separable states, $0 \leqslant J \leqslant 1$, depending on the measurement basis. To exploit this difference, we consider the sum

$$M_J = J(\rho)_{\{\Pi_b^B\}} + J(\rho)_{\{\Pi_{b'}^B\}} + J(\rho)_{\{\Pi_{b''}^B\}}, \tag{14}$$

where the set $\{b,b',b''\}$ denotes three *mutually unbiased bases*. For example, with the polarization states of light (e.g., $|\mathrm{H}\rangle$, $|\mathrm{V}\rangle$), one set of mutually unbiased bases includes analyzers at $b = \{h,v\}$, $b' = \{d,a\}$, and $b'' = \{r,l\}$ for linear polarizations horizontal (h), vertical (v), diagonal (d), and antidiagonal (a), and circular polarizations right (r) and left (l). This is the standard set of bases considered in this paper. In the following section, we will explain the motivation behind this choice and demonstrate why this quantity is useful from an experimental point of view.

We can also compute a similar sum using the classical definition [Eq. (4)]:

$$M_{J_C} = J_C(\rho)_{\{a,b\}} + J_C(\rho)_{\{a',b'\}} + J_C(\rho)_{\{a'',b''\}}. \tag{15}$$

In general, $M_J \neq M_{J_C}$. Furthermore, the choice of $\{a,a',a''\}$ and $\{b,b',b''\}$ as well as the ordering can drastically change the values of M_J and M_{J_C}. However, in practice, experimenters will typically agree ahead of time on their measurement bases; therefore, by calculating M_{J_C}, they can determine how much information they can extract from their qubits *with a predetermined basis*.

III. EXAMPLES AND SIMULATIONS

A few simple examples are as follows. First, consider a mixture of the singlet state ρ_s and the maximally correlated mixed state $\rho_m = (|\mathrm{HV}\rangle\langle\mathrm{HV}| + |\mathrm{VH}\rangle\langle\mathrm{VH}|)/2$, given by

$$\rho_M(p) = p\rho_s + (1-p)\rho_m, \tag{16}$$

where $0 \leqslant p \leqslant 1$. Using the three mutually unbiased bases listed above for both subsystems, we find that $M_J = M_{J_C}$. We also find that M_J has a value of 1 (in the case of a separable state, $p = 0$) and a value of 3 (in the case of a maximally entangled state, $p = 1$), such that $1 < M_J < 3$ for all other p. We note here that this range depends on the measurement basis. The cases of $p = 0$ and $p = 1$ have been studied experimentally and are discussed below.

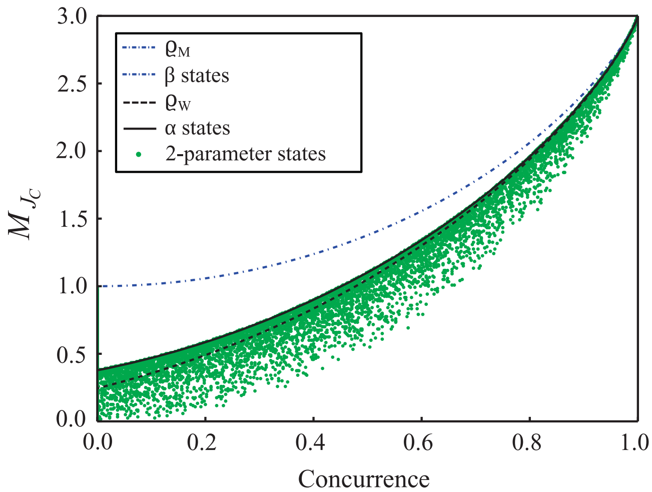

FIG. 2. (Color online) Parametric plot of the mutual information sum M_J and concurrence for the examples given in the text. Note that, for a given concurrence, M_J for ρ_M and $\rho(\beta)$ (they fall on the same curve) is uniformly higher than for the other three states. The points shown for the two-parameter state $\rho(a,b)$ are evaluated for a random, uniform sample of a and b.

The second example we consider is the Werner state [20], given by $\rho_W(p) = p\rho_s + (1-p)\mathbf{1}/4$, where $\mathbf{1}$ is the 4×4 identity and $0 \leqslant p \leqslant 1$ as before. We again find that $M_J = M_{J_C}$ and that, for a given concurrence, M_{J_C} for state $\rho_M(p)$ (using these measurement bases) is uniformly higher than for the Werner state. This can be seen in Fig. 2 where we plot M_{J_C} and concurrence parametrically for both $\rho_M(p)$ and $\rho_W(p)$. The reason ρ_M has a higher M_{J_C} than ρ_W is due to the maximum correlations that exist for the former in the $\{h,v\}$ basis. In the other two bases, the correlations are equal for these two states. That is, ρ_M is optimized for the $\{h,v\}$ basis without degradation in the other bases when compared to ρ_W. Furthermore, each term of M_{J_C} in Eq. (14) is equal for the Werner state; therefore, for some applications in quantum information, $\rho_M(p)$ may prove more useful than the Werner states, despite the high amount of entanglement possible in $\rho_W(p)$.

In Fig. 2 , we also include values for the α and β states $\rho(\alpha)$ and $\rho(\beta)$, which represent the upper and lower boundaries respectively in the discord-entanglement plane, as well as the two-parameter states $\rho(a,b)$, which contain $\rho(\alpha)$ and ρ_m [21]. We choose a and b uniformly from their specified ranges and find that M_{J_C} for $\rho(a,b)$ is less than or equal to M_{J_C} for $\rho(\alpha)$.

From Fig. 2, we can easily see a correlation between concurrence and M_{J_C} for many different states: the larger the entanglement, the larger the value of M_{J_C}. This is not surprising since M_{J_C} is measure of the mutual information (or correlations) across multiple unbiased bases. Additionally, given two states with equal concurrence, we believe that a larger value of M_{J_C} is, in general, more useful for two observers working in multiple, predetermined bases.

We contend that separable states have $M_J \leqslant 1$ and $M_{J_C} \leqslant 1$, noting that the measurement bases are *mutually unbiased*. However, due to the large state space created by the basis ambiguity, we rely on Monte Carlo simulations to justify this claim. We generate random physical density matrices using the method described in Ref. [22]. In particular, we first generate a random, 4×4 diagonal matrix ρ with diagonal elements given by

$$\rho_{11} = 1 - \xi_1^{1/3}, \tag{17}$$

$$\rho_{kk} = \left[1 - \xi_k^{1/(4-k)}\right]\left(1 - \sum_{i=1}^{k-1}\rho_{ii}\right), \tag{18}$$

for $k = \{2,3\}$; ρ_{44} is determined by $\mathrm{Tr}[\rho] = 1$. The three random numbers $\{\xi_k\}$ are uniformly distributed on the interval $(0,1)$. We then rotate this diagonal matrix to a new basis by generating a random unitary matrix U using Eqs. (3.1)–(3.3) in Ref. [23]. This gives $\tilde{\rho} = U\rho U^\dagger$; the set of matrices formed in this way sample the set of all density matrices uniformly [22].

We generated 10^6 such matrices and calculated M_J and M_{J_C} for each in 100 random, mutually unbiased bases. We separated the states into two groups: separable and entangled. For entangled states, we found that $M_J \in (0.05, 2.59)$ and $M_{J_C} \in (0.00, 2.22)$, with average values of $M_J = 0.43$ and $M_{J_C} = 0.35$ (maximized over bases and averaged over all matrices) and standard deviations of 0.22 and 0.20, respectively. Similarly, for separable states, we found that $M_J \in (0.00, 0.80)$ and $M_{J_C} \in (0.00, 0.73)$, with average values of $M_J = 0.14$ and $M_{J_C} = 0.11$ and standard deviations of 0.09 and 0.07, respectively. We found that 67.3% of all states were separable and that $M_J \geqslant M_{J_C}$. Based on the results of these simulations, we are confident that M_J and M_{J_C} are bounded by 1 for separable states. Therefore, $M_J(\rho) > 1$ and $M_{J_C}(\rho) > 1$ are sufficient conditions for the entanglement of a state.

It is interesting to note that it is trivial to construct a similar measure summed over only two mutually unbiased bases. Such a sum also results in an entanglement signature for the very same reasons listed above. Therefore, only eight measurements are required experimentally. Compare this to the standard Clauser, Horne, Shimony, and Holt (CHSH) inequality [24], for which 16 measurements are required. It is therefore experimentally faster to perform these mutual information sums, with the caveat that the experimenter may choose an inappropriate set of bases for detection, thereby failing to violate the bound.

IV. EXPERIMENT

Let us consider two photons created during degenerate, collinear, type-I SPDC using a two-crystal geometry [25], where the optic axis of each crystal is aligned in perpendicular planes. The photons are described by the joint density matrix $\rho = \rho^{AB}$, where photon A (B) is in port 1 (2). In our experimental setup, a 488 nm diode laser pumped two 3-mm BiBO down conversion crystals with a Soleil-Babinet compensator used for walkoff compensation. Use of a 3-nm bandpass filter restricted detection of entangled photons in a narrow band centered at 976 nm. The down-converted photons were separated with a 50:50 beam splitter, and the polarization of one photon was rotated with a half-wave plate to produce a singlet state. A maximally correlated mixed state was produced by removing the bandpass filter.

To determine the theoretical and experimental value of M_{J_C}, we modified the polarization state of the photons through local unitary operations (i.e., wave plates). Fixed polarizers and

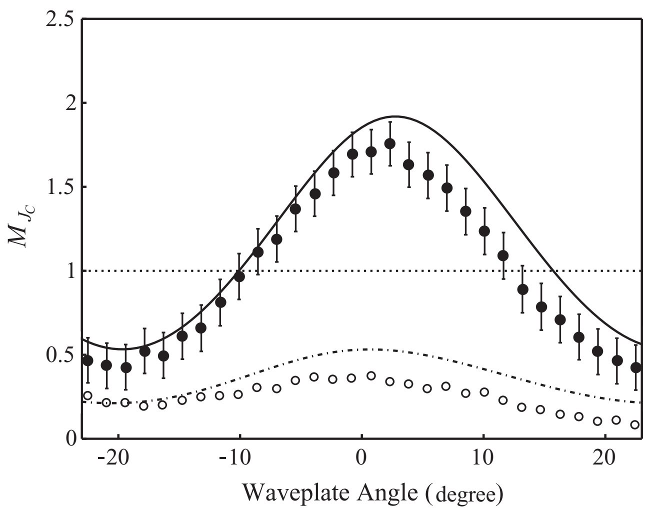

FIG. 3. Mutual information M_{J_C} recorded for the maximally correlated mixed state (hollow circles) and the singlet state (solid circles). Points are data composed of 36 min of integration (over 12 separate measurements) for the singlet state and 48 s of integration for the maximally correlated mixed state. The solid and dotted-dashed lines correspond to theoretical predictions of M_{J_C} based upon the tomographic reconstruction [26] of the singlet state and the maximally correlated mixed state, respectively. The error bars, which are smaller than the points for the maximally correlated mixed state, are calculated assuming shot noise limited detection. The dashed line indicates the classical bound of M_{J_C}.

variable wave plates mounted in computer-controlled rotation stages were used as analyzers in each port. Light was collected via multimode fibers coupled to single photon avalanche photodiodes. Coincidence counts in a 3-ns window were recorded with a PicoHarp 300. For each calculation of M_{J_C}, 12 measurements were made by recording the coincidence count rate while the angles of the analyzers were varied. The polarizers were fixed to pass vertical polarization. For experimental simplicity, we measured M_{J_C} in the aforementioned bases ($a = b = \{h,v\}$, $a' = b' = \{a,d\}$, $a'' = b'' = \{r,l\}$) and then rotated the angle of the half-wave plate in arm 2 through 45° to show a trend. For each angle, the measurement is performed in three mutually unbiased bases. We also perform quantum state tomography with maximum likelihood estimation [26] in order to reconstruct the density matrix for the theoretical calculation of M_{J_C}.

Data was taken for a maximally correlated mixed state (with a fidelity of 0.94) and a singlet state (with a fidelity of 0.92 and a concurrence of 0.84). From the coincidence count rates, M_{J_C} was calculated and is plotted in Fig. 3 along with the estimated values from the reconstructed state. We see a clear violation of the classical bound for the singlet state over a wide range of wave plate angles. However, as the measurement moves away from the ideal bases, we find that the value of M_{J_C} quickly drops, demonstrating the importance of this choice. We also note that the peak of M_{J_C} is shifted from 0° for both states; this is due to the asymmetry present in the reconstructed density matrices.

V. CONCLUSION

In conclusion, we find that the classical mutual information [Eq. (4)], as well as the classical part of the quantum discord [Eq. (13)], are responsible for an entanglement signature when summed over three mutually unbiased bases via Eqs. (14) and (15). Although such a sum depends heavily on the choice of bases, we believe this quantity serves a useful purpose from an information-theoretic perspective. It is experimentally faster and easier to extract an entanglement signature as compared to quantum state tomography and CHSH measurements. M_J also represents how much information two distant observers share with a particular set of mutually unbiased bases, therefore describing the communication channel and not just the quantum state of the qubits. We experimentally verified these predictions to demonstrate entanglement in our system and found good agreement with the theory.

ACKNOWLEDGMENTS

We acknowledge valuable discussions with J. H. Eberly, K. W. Chan, and M. V. Federov. This research was supported by the DARPA DSO InPho Grant No. W911NF-10-1-0404, the ARO Grant No. W911NF-09-1-0385, and the NSF Grant No. PHY-0855701.

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1949).
[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley, New York, 2006).
[3] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **40**, 2404 (1989).
[4] C. H. Bennett, Phys. Scr. **1998**, 210 (1998).
[5] W. Zurek, Ann. Phys. **9**, 855 (2000).
[6] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[7] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
[8] W. H. Zurek, Phys. Rev. A **67**, 012320 (2003).
[9] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[10] B. Dakić, V. Vedral, and C. Brukner, Phys. Rev. Lett. **105**, 190502 (2010).
[11] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[12] D. A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
[13] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acín, Phys. Rev. A **81**, 052318 (2010).
[14] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[15] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175-179.
[16] H. S. Eisenberg, G. Khoury, G. A. Durkin, C. Simon, and D. Bouwmeester, Phys. Rev. Lett. **93**, 193901 (2004).
[17] G. A. Durkin and C. Simon, Phys. Rev. Lett. **95**, 180402 (2005).

[18] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
[19] H. Araki and E. H. Lieb, Commun. Math. Phys. **18**, 160 (1970).
[20] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[21] A. Al Qasimi and D. F. V. James, Phys. Rev. A **83**, 032101 (2011).
[22] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
[23] K. Życzkowski and M. Kus, J. Phys. A: Mathematical and General **27**, 4235 (1994).
[24] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[25] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[26] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).