

Structure of dimension-bounded temporal correlations

Yuanyuan Mao¹, Cornelia Spee^{2,1}, Zhen-Peng Xu¹, and Otfried Gühne¹

¹Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany

²Institute for Theoretical Physics, University of Innsbruck, Technikerstraße 21A, 6020 Innsbruck, Austria

(Received 28 July 2020; revised 20 December 2020; accepted 5 January 2022; published 15 February 2022)

We analyze the structure of the space of temporal correlations generated by quantum systems. We show that the temporal correlation space under dimension constraints can be nonconvex. For the general case, we provide the necessary and sufficient dimension of a quantum system needed to generate a convex correlation space for a given scenario. We further prove that this dimension coincides with the dimension necessary to generate any point in the temporal correlation polytope. As an application of our results, we derive nonlinear inequalities to witness the nonconvexity for qubits and qutrits in the simplest scenario, and present an algorithm which can help to find the minimum for a certain type of nonlinear expressions under dimension constraints.

DOI: [10.1103/PhysRevA.105.L020201](https://doi.org/10.1103/PhysRevA.105.L020201)

Introduction. States of a quantum system are mathematically described by vectors in a Hilbert space. When no *a priori* information about the measurements or the states is known, one of the intrinsic properties we can possibly tell about an unknown quantum system is the dimension of its underlying Hilbert space. The dimension is considered as a valuable resource from an information-theoretical viewpoint [1–3]. Higher-dimensional quantum systems have been proven to be able to perform better in some tasks such as quantum key distribution [4,5] and so they can be used to implement more powerful protocols than lower-dimensional quantum systems [6].

But what can be concluded if the dimension is limited? For instance, in the semi-device-independent framework of quantum information processing, nothing else but the dimension of the quantum system is assumed [7,8]. The system is then measured in different experimental configurations and the statistics of the outcomes, usually referred to as quantum correlations, are recorded. The typical example of this scenario is the Bell test which proves that quantum mechanics is nonlocal. The resulting spatial correlations play a central role in many quantum information protocols, such as quantum key distribution and randomness certification [7,9]. Preceding works studied the space of quantum correlations arising from quantum systems of different dimensions in many scenarios [10–14], with various techniques using convex optimization designed to find the bound of some linear functionals of the correlations achievable with a given dimension [15,16]. In the Bell scenario, however, the sets of correlations arising from dimension-bounded Hilbert spaces are typically nonconvex [17–19]. Hence what linear functionals characterize are essentially the convex hulls of correlation sets, rather than correlation sets themselves. In addition, some of these Bell-type dimension tests have recently been critically investigated, as they may not characterize the experimentally relevant figures of merit [20,21].

In this Letter we consider a different model, where measurements are performed in a temporal sequence [22–26], instead of spatial correlations investigated in Bell tests. The temporal correlations obtained by sequential measurements can be used to violate Leggett-Garg inequalities [27,28], proving quantum mechanics is not a theory of macroscopic realism. We study the structure of temporal quantum correlations generated by dimension-bounded systems. First, we will prove that already for the simplest scenario, the correlation spaces obtained by qubit or qutrit systems are nonconvex, and we provide nonlinear witnesses detecting this nonconvexity. Namely, they can distinguish quantum systems with different dimensions even if the convex hulls of the correlation spaces are the same. For general scenarios, we give a formula for the necessary and sufficient dimension of quantum systems, from which a convex set of temporal correlations can be obtained. As an application, we show that our nonconvexity witnesses are also qualitatively better dimension witnesses than linear ones. In order to derive nonlinear inequalities able to test higher dimensions, we present an iterative algorithm which allows us to optimize a certain type of temporal correlation polynomials over dimension-bounded Hilbert spaces.

The space of temporal correlations. As illustrated in Fig. 1, a single system prepared in an initial state ρ_{in} is subjected to a sequence of measurements of a certain length L . At each time step, a measurement selected from a given set $\{\mathcal{M}_0, \mathcal{M}_1, \dots, \mathcal{M}_{S-1}\}$ is performed according to the input from an input alphabet $\mathcal{X} = \{0, 1, \dots, S-1\}$, and after each measurement an output from an alphabet $\mathcal{A} = \{0, 1, \dots, O-1\}$ is obtained. No assumption on the type of measurements will be imposed. In between two measurements we allow for an arbitrary quantum dynamics, which may depend on the former choice of measurements and the measurement outcomes. Given an initial state ρ_{in} , one obtains a probability distribution $p(ab \dots | xy \dots)$ for any input sequence $xy \dots$. We call the collection of the probability distributions generated by all possible inputs a temporal correlation. As a result of causality,

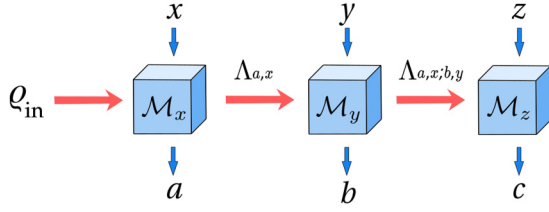


FIG. 1. A quantum system with initial state ρ_{in} is measured several times, and the measurements can be repeated. The output state after each measurement will be subjected to a quantum dynamics which may depend on the prior choice of measurements and the outcome of the measurements. In this figure we depict this scenario for $L = 3$.

the choice of latter measurements cannot affect the outcomes of former measurements. Hence, the temporal correlations have to fulfill the arrow of time (AoT) constraints [29]. For a two-step process, the constraints read

$$\sum_b p(ab|xy) = \sum_b p(ab|xy'), \quad (1)$$

for all $a, b \in \mathcal{A}$, $x, y, y' \in \mathcal{X}$. If there is no further assumption on the dimension of the quantum system, for any given L , S , and O , the temporal correlations form a polytope denoted by $P_{S,O}^L$ [29]. The extreme points of this polytope are the deterministic assignments, where each measurement has a fixed outcome and the AoT constraints are fulfilled [25,30]. A correlation $\{p(abc \cdots |xyz \cdots)\}$ is in the temporal correlation polytope if and only if it can be decomposed as

$$p(abc \cdots |xyz \cdots) = p(a|x)p(b|a, xy)p(c|ab, xyz) \cdots, \quad (2)$$

with $p(a|x)$, $p(b|a, xy)$, $p(c|ab, xyz)$, \dots denoting the local probability distribution where the measurement choice and their outcomes in the preceding time steps are fixed [25]. It has been shown that any correlation obeying the AoT condition can be reached in quantum mechanics [25,31], in contrast to the nonsignaling polytope in the Bell scenario [32], where not all the points can be realized.

Nonconvexity in the simplest case. The most basic experimental setup is to measure an uncharacterized quantum system twice, producing binary strings $ab \in \{0, 1\}^{\otimes 2}$. The performed measurements are chosen from a set of two-outcome measurements $\{\mathcal{M}_0, \mathcal{M}_1\}$, based on the input string $xy \in \{0, 1\}^{\otimes 2}$. Qubits can already be distinguished from higher-dimensional systems with this simple setup, since one can reach all the extreme points of the polytope by using qutrits, but not qubits [25]. Moreover, as we prove below, the set of quantum correlations generated by a qubit is not convex. For example, the two extreme points of the correlation polytope,

$$\begin{aligned} p_1 : p(10|00) = p(10|01) = p(01|10) = p(00|11) = 1, \\ p_2 : p(10|00) = p(10|01) = p(10|10) = p(10|11) = 1, \end{aligned} \quad (3)$$

can be attained by measuring a single qubit [25]. Nevertheless, the mixture of both, $p_m = \frac{p_1 + p_2}{2}$, cannot be achieved by a qubit. This can be seen as follows: In order to realize the correlation p_m , both measurements \mathcal{M}_0 and \mathcal{M}_1 have to be able to give each of the two results. Moreover, measuring \mathcal{M}_0 in the first step gives result “1” with certainty and in the second

step if \mathcal{M}_0 was measured in the first step, it produces result “0” with certainty. This means both of its effects have to be projective operators. Without loss of generality, we denote the initial state by $|1\rangle$. Then the measurement \mathcal{M}_0 is measuring the observable σ_z , and the intermediate state after choosing \mathcal{M}_0 as the first measurement is precisely $|0\rangle$. Based on the observation that measuring \mathcal{M}_1 on state $|0\rangle$ always gives outcome “0,” we can tell that the effect of \mathcal{M}_1 corresponding to outcome “0” is of the form $|0\rangle\langle 0| + \epsilon|1\rangle\langle 1|$, with $\epsilon \in [0, 1)$. If we measure \mathcal{M}_1 twice, the second step will give outcome “0” with certainty, which indicates that the intermediate state after measuring \mathcal{M}_1 is also the $|0\rangle$. However, in this case the probability $p(01|10)$ vanishes, which contradicts $p(01|10) = 1/2$.

Besides the case-to-case analysis, the nonconvexity can also be detected by nonlinear inequalities:

Observation 1. For correlations resulting from arbitrary measurements on a qubit, it holds that

$$\begin{aligned} S_1 = 2p(0|0) + p(0|0, 00) + 2p(0|1) \\ + p(0|0, 11) + p(1|0, 10)p(1|0, 01) \leq 6. \end{aligned} \quad (4)$$

Here, $p(b|a, xy) = p(ab|xy)/p(a|x)$ denotes the probability of obtaining the outcome “b” when measuring the measurement \mathcal{M}_y in the second time step, given that the measurement \mathcal{M}_x was measured in the first time step, and outcome “a” was obtained. The proof of Eq. (4) is presented in Appendix A of the Supplemental Material, wherein also an example of nonconvexity detected by Eq. (4) is given [33]. In this example, both extreme points we consider are achievable by a qubit, but the uniform mixture of them violates the inequality as demonstrated in Fig. 2. The maximal value $S_1 = 7$ can be achieved by an extreme point of the polytope, which corresponds to a qutrit system [25].

In the simplest scenario $L = S = O = 2$ all the extreme points are already achievable by qutrits, so linear dimension witnesses could not distinguish qutrits from higher-dimensional quantum systems. Still, nonlinear criteria can do that, as the following inequality shows:

Observation 2. For arbitrary measurements we have that

$$\begin{aligned} S_2 = p(0|0, 00) + p(0|0, 01) + p(0|0, 10) + p(1|1, 00) \\ + p(1|1, 10) + p(1|1, 11) \\ + p(1|0, 11) + p(0|1, 01) \leq 4 + 2\sqrt{2} \leq 5 + \sqrt{5}, \end{aligned} \quad (5)$$

where the first bound holds for a qubit, and the second bound for a qutrit. The algebraic maximum $S_2 = 8$ can be reached by a four-level system.

It should be noted that the above inequality can also be interpreted in the prepare-and-measure scenario where the pair (a, x) determines the prepared state and y the input defines the measurement setting. In this context, it corresponds to a quantum random access code [34], for which the qubit bound has already been shown analytically [35], and the qutrit bound has been obtained numerically [13]. This connection allows one to use inequalities and techniques known in the prepare-and-measure scenario for the study of temporal correlations and vice versa. In Appendix B of the Supplemental Material we provide a proof of the Observation, in particular we prove the

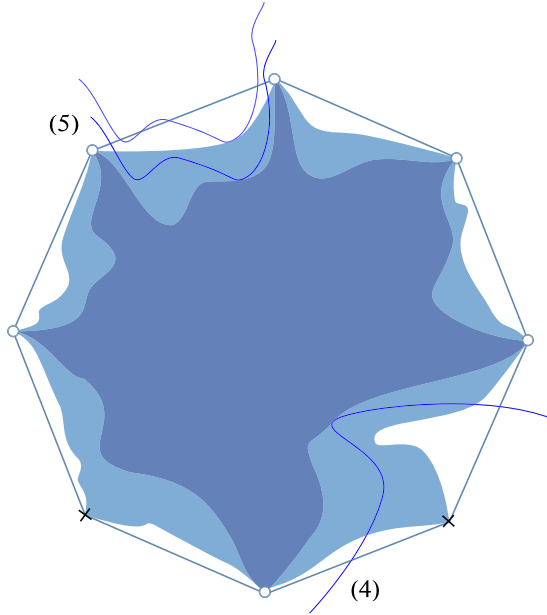


FIG. 2. Schematic illustration of the temporal correlation space in the simplest case. The octagon denotes the temporal correlation polytope, the darker area is the temporal correlation space generated by a qubit, and the lighter area denotes the temporal correlations that can be reached by a qutrit, but not a qubit. We label the extreme points achievable by a qubit with circles and other extreme points with crosses. The curve in the bottom describes (4), whose maximum is achieved by an extreme point which cannot be realized by qubit. The algebraic maximum of inequality (5), described by the double curves at the upper left, is achieved by the uniform mixture of two extreme points that are achievable by qubits.

qutrit bound analytically [33]. Alongside we show an example of two extreme points, who both can be reached by measuring a qubit, but the uniform mixture requires a four-level system and reaches $\mathcal{S}_2 = 8$.

Mixing with white noise. We will consider in the following that the experiment is affected by noise. We call the noise local white noise if the experiment is only disturbed at one time step, which causes the local-in-time distribution $\{p(a|hx)\}$ to be mixed with a local uniform distribution $\{p(a|hx) = \frac{1}{\mathcal{O}}\}$. Here, h stands for the history, i.e., the chosen measurements and their outcomes before the time step. If the correlation $\{p(abc \dots | xyz \dots)\}$ itself is mixed with a uniform distribution $\{p(abc \dots | xyz \dots) = \frac{1}{\mathcal{O}^L}\}$, we say that the noise is a global white noise. Counterintuitively, mixing a correlation $\{p(abc \dots | xyz \dots)\}$ with local or global white noise does not necessarily reduce the dimension required to realize it. This also exemplifies the nonconvexity of dimension-bounded temporal correlations. Here, we discuss the two kinds of white noise separately.

(i) *Local white noise:* For example, if the correlation is affected by local white noise to step two, the conditional probability distribution at the second step $\{p(b|a, xy)\}$ for chosen a, x, y is mixed with $\{p(b|a, xy) = \frac{1}{\mathcal{O}}\}$. Obviously for certain correlations, this process can have more outcomes for one time step, which may increase the necessary dimension of quantum system.

(ii) *Global white noise:* Consider a given correlation $\{p(abc \dots | xyz \dots)\}$ is mixed with the identity correlation $\{p(abc \dots | xyz \dots) = \frac{1}{\mathcal{O}^L}\}$. Here, we present two examples, where the necessary dimension increases.

Example 1. Consider a trivial extreme point in the (2-2-2) scenario, $p(00|00) = p(00|01) = p(00|10) = p(00|11) = 1$. Its uniform mixture with the identity is

$$p(ab|xy) = \begin{cases} \frac{5}{8}, & \text{for } a = 0, b = 0, \\ \frac{1}{8}, & \text{otherwise,} \end{cases} \quad (6)$$

which cannot be generated by a one-dimensional quantum system in contrast to the original correlations.

Example 2. Consider the extreme point defined by $p(00|00) = p(00|01) = p(00|10) = p(01|11) = 1$. It can be easily seen that this point can be realized with measurements on a qubit [25,36]. However, as we will show in Appendix C of the Supplemental Material, the convex combination of this point and sufficiently weak global white noise requires at least a qutrit for its realization [33].

From the discussion above, we see that the correlation space expands while the dimension d of the underlying quantum system increases, until the whole correlation polytope is obtained. For the simplest scenario, the nonconvexity of the qutrit correlation space shows that the whole correlation polytope cannot be reached with a qutrit, although all the extreme points can be achieved. A natural question then arises: Which dimension is needed in order to obtain the entire temporal correlation polytope? We give an explicit formula for this dimension in the following, and we show that any correlation space generated by a system with a smaller dimension is nonconvex.

General scenarios. For an arbitrary given scenario with L measurement steps, S possible measurements, and O possible outcomes per measurement, the temporal correlation polytope $P_{S,O}^L$ has $(O^S)^{\frac{S-1}{S}}$ extreme points [25]. The following theorem provides the smallest dimension of a quantum system, such that the generated set of temporal correlations will be convex. We call this the *critical dimension* $\mathcal{D}(L, S, O)$. We show moreover that the set of temporal correlations generated by a quantum system of critical dimension is already the temporal correlation polytope $P_{S,O}^L$. Hence, the set of temporal correlations of a quantum system cannot be extended by increasing its dimension beyond the critical dimension.

Theorem 1. The critical dimension is given by the following formula,

$$\mathcal{D}(L, S, O) = \min \left\{ O^S, \frac{(OS)^L - 1}{OS - 1} \right\}. \quad (7)$$

Quantum systems with a dimension larger than or equal to the critical dimension generate the correlation polytope $P_{S,O}^L$. Moreover, any correlation space generated by quantum systems with smaller dimension is nonconvex.

To give an example, with this formula we can calculate the critical dimension of the simplest case as $\mathcal{D}(2, 2, 2) = 4$. The detailed proof is presented in Appendix D of the Supplemental Material [33]. A sketch of the proof is as follows: In order to show that the critical dimension is necessary to achieve all the correlations in the polytope, we consider two density matrices which have to be able to each realize a certain

local-in-time correlation. Then we show an upper bound on the overlap of the eigenstates corresponding to the maximal eigenvalue of these two density matrices. One can then show that if the pairwise upper bound is low enough for a set of states, these states have to be linearly independent, which proves the necessity of the critical dimension. For the other direction, we construct protocols to realize an arbitrary point in the correlation space with a \mathcal{D} -dimensional system. Then we give examples contradicting the convexity of correlation space generated by systems whose dimension is smaller than critical dimension. Our results can be also straightforwardly used in the prepare-and-measure scenario where in addition to constraints on the dimension among others also the minimal overlap assumption has been considered [37].

Numerical algorithms. Finally, let us provide a seesaw algorithm that can find the maximum of the general polynomial, if the maximum is attained on pure states and projective measurements under dimension constraints. The polynomials discussed in this Letter all fulfill this assumption. Exploiting the correspondence between length-two temporal correlations and the prepare-and-measure setup, our method can be utilized in both scenarios.

Consider any given polynomial $p(X_1, X_2, \dots, X_n)$ where the X_i 's are the involved probabilities of the form $p(a|x)$ or $p(b|a, xy)$. Since every maximization problem can be converted into a minimization problem, we only present the method for finding the minimum of such a polynomial. To find the minimum of $p(X_1, X_2, \dots, X_n)$ for a d -dimensional quantum system, we can first choose a random number q , and check whether $p(X_1, X_2, \dots, X_n)$ can achieve a value smaller than q with correlations obtained from measuring a d -dimensional system. We illustrate this using the $d = 2$ case as an example. For a correlation that can be produced by a qubit, its corresponding (X_1, X_2, \dots, X_n) has a quantum representation $X_i = \text{tr}(\rho_i M_i)$, with ρ_i being the initial or intermediate states and M_i the measurement effects. By assumption, the polynomial is minimized by a correlation with pure states $\rho_i = |\psi_i\rangle\langle\psi_i|$ and projective measurement effects $M_i = |\phi_i\rangle\langle\phi_i|$. For this correlation we can construct a $2 \times 2n$ matrix

$$\Gamma = (|\psi_1\rangle, \dots, |\psi_n\rangle, |\phi_1\rangle, \dots, |\phi_n\rangle). \quad (8)$$

Then, the matrix $\Gamma^\dagger \Gamma$ is a $2n \times 2n$ positive semi-definite matrix with all diagonal entries equal to 1 and rank 2. Every $X_i = \text{tr}(\rho_i M_i) = |\langle\psi_i|\phi_i\rangle|^2$ is the absolute square of a certain entry. If the minimum of $p(X_1, X_2, \dots, X_n)$ is smaller than a number q , then there should exist a common object in the following two sets of $2n \times 2n$ matrices:

(M_1) Rank two positive semidefinite matrices.

(M_2) Hermitian matrices with the main diagonal $(1, 1, \dots, 1)$, whose entries corresponding to $\{X_i\}$ satisfy the inequality

$$p(X_1, X_2, \dots, X_n) \leq q. \quad (9)$$

To examine the existence of such a matrix, one can iterate between these two sets. Starting from a matrix in M_1 one can find analytically the closest matrix in M_2 . For this matrix, one can then find analytically the closest matrix in M_1 again, etc. We describe the algorithm in detail in Appendix E of the Supplemental Material [33]. A common object exists if the iteration converges, the converse is however not true. In Appendix F of the Supplemental Material we give an example of applying our method to treat the inequality (5) numerically [33].

Conclusions. We characterized the nonconvex structure of temporal correlation space generated by finite-dimensional quantum systems. For arbitrary scenarios, we derived the critical dimension of quantum systems to generate a convex set of temporal correlations. We established nonlinear inequalities for the simplest case with upper bounds satisfied by qubits or qutrits, respectively. These nonlinear inequalities can serve as implementable dimension witnesses. In this way, our results might trigger experimental investigations of the performance of systems with different finite dimensions.

Note that our setting allows for arbitrary dynamics to occur between adjacent time steps. The structure of the temporal correlation space can change if we limit the possible intermediate channels to certain classes, e.g., Markovian channels. It would be interesting to study the features of correlation space corresponding to restricted quantum channels. This might inspire a general method to experimentally reveal the properties of quantum channels by analyzing the obtained temporal correlations. We leave this problem for future research.

Acknowledgments. We would like to thank M. Túlio Quintino for discussions. We acknowledge financial support by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, Projects No. 447948357 and No. 440958198), the Sino-German Center for Research Promotion (Project M-0294), the ERC (Consolidator Grant No. 683107/TempoQ), and the DAAD (Projekt-ID: 57445566). Y.M. acknowledges funding from a CSC-DAAD scholarship. C.S. acknowledges support by the Austrian Science Fund (FWF): J 4258-N27. Z.-P.X. is thankful for the support of the Alexander von Humboldt Foundation.

-
- [1] A. S. Holevo, *Probl. Inf. Transm.* **9**, 177 (1973).
 [2] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, *Nat. Phys.* **5**, 134 (2009).
 [3] A. Acín, N. Gisin, and L. Masanes, *Phys. Rev. Lett.* **97**, 120405 (2006).
 [4] H. Bechmann-Pasquinucci and W. Tittel, *Phys. Rev. A* **61**, 062308 (2000).

- [5] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
 [6] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, *Light: Sci. Appl.* **7**, 17146 (2018).
 [7] M. Pawłowski and N. Brunner, *Phys. Rev. A* **84**, 010302(R) (2011).
 [8] Y.-C. Liang, T. Vértesi, and N. Brunner, *Phys. Rev. A* **83**, 022108 (2011).

- [9] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **85**, 052308 (2012).
- [10] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, *Phys. Rev. Lett.* **100**, 210503 (2008).
- [11] R. Gallego, N. Brunner, C. Hadley, and A. Acín, *Phys. Rev. Lett.* **105**, 230501 (2010).
- [12] N. Brunner, M. Navascués, and T. Vértesi, *Phys. Rev. Lett.* **110**, 150501 (2013).
- [13] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, *Phys. Rev. A* **92**, 042117 (2015).
- [14] J. Bowles, N. Brunner, and M. Pawłowski, *Phys. Rev. A* **92**, 022351 (2015).
- [15] M. Navascués and T. Vértesi, *Phys. Rev. Lett.* **115**, 020501 (2015).
- [16] A. Tavakoli, D. Rosset, and M. O. Renou, *Phys. Rev. Lett.* **122**, 070501 (2019).
- [17] J. M. Donohue and E. Wolfe, *Phys. Rev. A* **92**, 062120 (2015).
- [18] J. Sikora, A. Varvitsiotis, and Z. Wei, *Phys. Rev. Lett.* **117**, 060401 (2016).
- [19] J. Bowles, M. T. Quintino, and N. Brunner, *Phys. Rev. Lett.* **112**, 140407 (2014).
- [20] W. Cong, Y. Cai, J.-D. Bancal, and V. Scarani, *Phys. Rev. Lett.* **119**, 080401 (2017).
- [21] T. Kraft, C. Ritz, N. Brunner, M. Huber, and O. Gühne, *Phys. Rev. Lett.* **120**, 060502 (2018).
- [22] C. Budroni, T. Moroder, M. Kleinmann, and O. Gühne, *Phys. Rev. Lett.* **111**, 020403 (2013).
- [23] M. Żukowski, *Front. Phys.* **9**, 629 (2014).
- [24] S. Brierley, A. Kosowski, M. Markiewicz, T. Paterek, and A. Przysiężna, *Phys. Rev. Lett.* **115**, 120404 (2015).
- [25] J. Hoffmann, C. Spee, O. Gühne, and C. Budroni, *New J. Phys.* **20**, 102001 (2018).
- [26] C. Spee, H. Siebeneich, T. F. Gloger, P. Kaufmann, M. Johanning, C. Wunderlich, M. Kleinmann, and O. Gühne, *New J. Phys.* **22**, 023028 (2020).
- [27] A. J. Leggett and A. Garg, *Phys. Rev. Lett.* **54**, 857 (1985).
- [28] H. S. Karthik, H. A. Shenoy, and A. R. Usha Devi, *Phys. Rev. A* **103**, 032420 (2021).
- [29] L. Clemente and J. Kofler, *Phys. Rev. Lett.* **116**, 150401 (2016).
- [30] A. A. Abbott, C. Giarmatzi, F. Costa, and C. Branciard, *Phys. Rev. A* **94**, 032131 (2016).
- [31] T. Fritz, *New J. Phys.* **12**, 083055 (2010).
- [32] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
- [33] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevA.105.L020201> for discussions and proofs of the results and a detailed description of the algorithm in the main text.
- [34] S. Wehner, M. Christandl, and A. C. Doherty, *Phys. Rev. A* **78**, 062112 (2008).
- [35] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *J. ACM* **49**, 496 (2002).
- [36] C. Spee, C. Budroni, and O. Gühne, *New J. Phys.* **22**, 103037 (2020).
- [37] W. Shi, Y. Cai, J. B. Brask, H. Zbinden, and N. Brunner, *Phys. Rev. A* **100**, 042108 (2019).