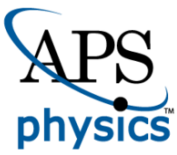

Device-Independent Tests of Entropy

Rafael Chaves, Jonatan Bohr Brask, and Nicolas Brunner

Phys. Rev. Lett. **115**, 110501 — Published 8 September 2015

DOI: 10.1103/PhysRevLett.115.110501

Device-Independent Tests of Entropy

Rafael Chaves,[1,2] Jonatan Bohr Brask,[3] and Nicolas Brunner[3]

[1]*Institute for Physics & FDM, University of Freiburg, 79104 Freiburg, Germany*
[2]*Institute for Theoretical Physics, University of Cologne, 50937 Cologne, Germany*
[3]*Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland*

(Dated: August 11, 2015)

We show that the entropy of a message can be tested in a device-independent way. Specifically, we consider a prepare-and-measure scenario with classical or quantum communication, and develop two different methods for placing lower bounds on the communication entropy, given observable data. The first method is based on the framework of causal inference networks. The second technique, based on convex optimization, shows that quantum communication provides an advantage over classical, in the sense of requiring a lower entropy to reproduce given data. These ideas may serve as a basis for novel applications in device-independent quantum information processing.

The development of device-independent (DI) quantum information processing has attracted growing attention recently. The main idea behind this new paradigm is to achieve quantum information tasks, and guarantee their secure implementation, based on observed data alone. Thus no assumption about the internal working of the devices used in the protocol is in principle required. Notably, realistic protocols for DI quantum cryptography [1] and randomness generation [2, 3] were presented, with proof-of-concept experiments for the second [3, 4].

The strong security of DI protocols finds its origin in a more fundamental aspect of physics, namely the fact that certain physical quantities admit a model-independent description and can thus be certified in a DI way. The most striking example is Bell nonlocality [5, 6], which can be certified (via Bell inequality violation) by observing strong correlations between the results of distant measurements. Notably, this is possible in quantum theory, by performing well-chosen local measurements on distant entangled particles. More recently, it was shown that the dimension of an uncharacterized physical system (loosely speaking, the number of relevant degrees of freedom) can also be tested in a DI way [7–10]. Conceptually, this allows us to study quantum theory inside a larger framework of physical theories, which already brought insight to quantum foundations [11–14]. From a more applied point of view, this allows for DI protocols and for black-box characterization of quantum systems [15–20].

In the present work, we show that another physical quantity of fundamental interest, namely the entropy of a message, can be tested in a DI way. Specifically, we present simple and efficient methods for placing lower bounds on the entropy of a classical (or quantum) communication based on observable data alone. We construct such "entropy witnesses" following two different approaches, first using the framework of causal inference networks [21], and second using convex optimization techniques. The first construction is very general,

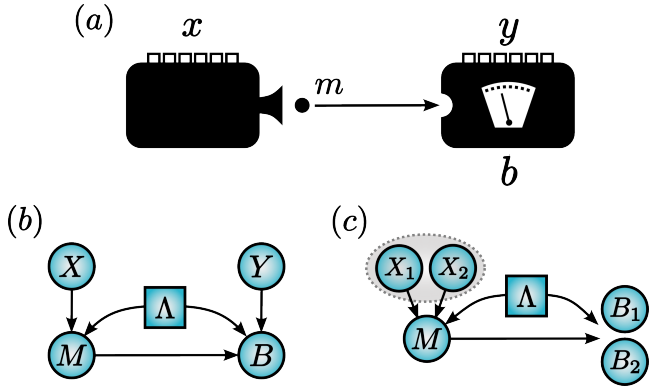

FIG. 1. Prepare-and-measure scenario. **(a)** Black-boxes representation. **(b)** Representation as a DAG. **(c)** Finer description of the prepare-and-measure scenario where the number of measurements is explicitly taken in to account.

but usually gives suboptimal bounds. The second construction allows us to place tight bounds on the entropy of classical messages for given data. Moreover, it shows that quantum systems provide an advantage over classical ones, in the sense that they typically require lower entropy to reproduce a given set of data.

The interest in placing DI bounds on entropy is twofold. First, from a conceptual point of view, this shows that a key concept in both classical and quantum information theory can be tested in a model independent manner. Moreover, the methods we develop here allow one to compare entropy in classical and quantum theory. Second, from the point of view of applications our work may open novel possibilities for partially DI quantum information processing, as we discuss at the end of the paper.

Scenario.—We consider the prepare-and-measure scenario depicted in Fig. 1(a). It features two uncharacterized devices, hence represented by black-boxes: a preparation and a measurement device. Upon receiving input x (chosen among n possible settings), the preparation device sends a physical system to the measuring

device. The state of the system may contain information about x. Upon receiving input y (chosen among l settings) and the physical system sent by the preparation device, the measuring device provides an outcome b (with k possible values). The experiment is thus fully characterized by the probability distribution $p(b|x,y)$. The inputs x, y are chosen by the observer, from a distribution $p(x,y)$, which will be taken here to be uniform and independent, i.e. $p(x) = 1/n$ and $p(y) = 1/l$ (unless stated otherwise). A set of data $p(b|x,y)$ will also be represented using the vector notation $\mathbf{p}$; the nlk components of $\mathbf{p}$ giving the probabilities $p(b|x,y)$.

Our main focus is the entropy of the mediating physical system, and our main goal will be to lower bound this entropy in a DI way, that is, based only on the observational data $\mathbf{p}$. We will consider both cases in which the mediating physical system is classical and quantum.

Let us first consider the quantum case. For each input x, the preparation device sends a quantum state ϱ_x (in a Hilbert space of finite dimension d). We are interested in the von Neumann entropy of the average emitted state

$$S(\varrho) = -tr(\varrho \log \varrho) \quad \text{where} \quad \varrho = \sum_x p(x)\varrho_x. \tag{1}$$

Specifically we want to find the minimal $S(\varrho)$ that is compatible with a given set of data, i.e. such that there exist states ϱ_x and measurement operators $M_{b|y}$ (acting on $\mathbb{C}^d$) such that $p(b|x,y) = \mathrm{tr}(\varrho_x M_{b|y})$. Note that in general we want to minimize $S(\varrho)$ without any restriction on the dimension d.

In the case of classical systems, for each input x, a message $m \in \{0, ..., d-1\}$ is sent with probability $p(m|x)$. The average message M is given by the distribution $p(m) = \sum_x p(m|x)p(x)$, with Shannon entropy

$$H(M) = -\sum_{m=0}^{d-1} p(m) \log p(m). \tag{2}$$

Again, for a given set of data, our goal is to find the minimal entropy compatible with the data, considering systems of arbitrary finite dimension d.

Entropy vs dimension.— Since our goal is to derive DI bounds on the entropy without restricting the dimension our work is complementary to that of Gallego et al. [10], where DI bounds on the dimension were derived. While the work of Ref. [10] derived DI lower bounds on worst case communication, our goal is to place DI lower bounds on the average communication.

More formally, Ref. [10] presented so-called (linear) dimension witnesses, of the form

$$V(\mathbf{p}) = \mathbf{v} \cdot \mathbf{p} = \sum_{x,y,b} v_{xyb} p(b|x,y) \leq L_d, \tag{3}$$

with (well-chosen) real coefficients v_{xyb} and bound L_d. The inequality holds for any possible data generated with systems of dimension (at most) d. Hence if a given set of data $\mathbf{p}$ is found to violate a dimension witness, i.e. $V(\mathbf{p}) > L_d$, then this certifies the use of systems of dimension at least $d+1$.

In this work, we look for entropy witnesses, that is, functions W which can be evaluated directly from the data $\mathbf{p}$ with the following properties. First, for any $\mathbf{p}$ requiring a limited entropy, say $H \leq H_0$, we have that

$$W(\mathbf{p}) \leq L(H_0). \tag{4}$$

Moreover, there should exist (at least) one set of data $\mathbf{p}_0$ such that $W(\mathbf{p}_0) > L(H_0)$, thus requiring entropy $H > H_0$. The problem is defined similarly for quantum systems, replacing the Shannon entropy with the von Neumann entropy.

Before discussing methods for constructing entropy witness, it is instructive to see that DI tests of entropy and dimension are in general completely different. Specifically, we show via a simple example, that certain sets of data may require the use of systems of arbitrarily large dimension d, but vanishing entropy.

Consider a prepare-and-measure scenario, and a strategy using classical systems of dimension $d+1$. We consider $n = d^2$ choices of preparations, and $l = n-1$ choices of measurements, each with binary outcome $b = \pm 1$. Upon receiving input $x \leq d$, send message $m = x$; otherwise, send $m = 0$. The entropy of the average message (with uniform choice of x) is found to be $H(M) = (2/d)\log(d) - (1-1/d)\log(1-1/d)$ which tends to zero when $n \to \infty$ (and hence $d \to \infty$). However, the corresponding set of data, $\mathbf{p}_0$, cannot be reproduced using classical systems of dimension d. This can be checked using a class of dimension witnesses [10]:

$$I_n(\mathbf{p}) = \sum_{y=1}^{n-1} E_{1y} + \sum_{x=2}^{n} \sum_{y=1}^{n+1-x} v_{xy} E_{xy} \leq L_d \tag{5}$$

where $E_{xy} = \sum_{b=\pm 1} b\, p(b|x,y)$ and $v_{xy} = 1$ if $x + y \leq n$ and -1 otherwise. For the above strategy, we obtain $I_n(\mathbf{p}_0) > L_d = n(n-3)/2 + 2d - 1$. Therefore, the data $\mathbf{p}_0$ requires dimension at least $d+1$ which diverges as $n \to \infty$, but has vanishingly small entropy in this limit.

Entropy Witnesses I.—The above example shows that testing entropy or dimension are distinct problems. Thus new methods are required for constructing DI entropy witnesses. We first discuss a construction based on the entropic approach to causal inference [21–24]. To the prepare-and-measure scenario of Fig. 1a, we associate a *directed acyclic graph* (DAG) depicted in Fig. 1b. Each node of the graph represents a variable of the problem (inputs X, Y, output B, and message M), and the arrows indicate causal influence. Moreover, we allow the devices to act according to a common strategy, represented with an additional variable Λ (taking val-

ues λ, with distribution $p(\lambda)$). We thus have that

$$p(b|x,y) = \sum_{\lambda,m} p(b|y,m,\lambda)p(m|x,\lambda)p(\lambda). \quad (6)$$

The key idea behind the entropic approach in the classical case is the fact that the causal relationships of a given DAG are faithfully captured by linear equations in terms of entropies [22]. These relations, together with the so-called Shannon-type inequalities (valid for a collection of variables, regardless of any underlying causal structure), define a convex set (the entropic cone) which characterizes all the entropies compatible with a given causal structure. Note that for the quantum case, a similar analysis can be pursued, with the only notable difference that causal relations of the form (6) must be replaced with data-processing inequalities; see [25] Sec. I and Ref. [23] for more details.

Using the methods of [23], we characterized the facets of the entropic cone for the DAG of Fig. 1(b). In the quantum case, the only non-trivial facet is given by

$$S(\varrho) \geq I(X:Y,B), \quad (7)$$

where $I(X:Y) = H(X) + H(Y) - H(X,Y)$ is the mutual information. Note that for the classical case, the Shannon entropy $H(M)$ replaces $S(\varrho)$. The above inequality, which in fact follows directly from Holevo's bound [26], provides a simple and general bound for the entropy for given data, valid for an arbitrary number of preparations, measurements, and outcomes. However, this comes at the price of a very coarse-grained description of the data, and therefore will typically provide a poor lower bound on the entropy.

It is possible to obtain a finer description by accounting explicitly for the fact that the number of measurements l is fixed. To do so, we replace the variables Y, B with l new variables B_y, and split the variable X into l separate variables $X = (X_1, \ldots, X_l)$; considering here $n = r^l$ for some integer r [27].

We first discuss the case of $l = 2$ measurements. The corresponding DAG is illustrated in Fig. 1(c). Applying again the methods of Ref. [23], we find a single non-trivial inequality (up to symmetries)

$$\begin{aligned} S(\varrho) \geq\ & I(X_1:B_1) + I(X_2:B_2) \\ & + I(X_1:X_2|B_1) - I(X_1:X_2). \end{aligned} \quad (8)$$

A general class of entropy witnesses can be obtained by extending the above inequality to the case of l measurements (details in [25] Sec. I.D):

$$\begin{aligned} S(\varrho) \geq\ & \sum_{i=1}^{l} I(X_i:B_i) + \sum_{i=2}^{l} I(X_1:X_i|B_i) \\ & - \sum_{i=1}^{l} H(X_i) + H(X_1,\ldots,X_l). \end{aligned} \quad (9)$$

These witnesses give relevant (although usually suboptimal) bounds on $S(\varrho)$. For instance, we show in [25] Sec. 2 that the maximal violation of the dimension witnesses $I_n(\mathbf{p})$ (given in (5)), which implies the use of systems of dimension $d = n$ [10], also implies maximal entropy, i.e. $S(\varrho) \geq \log n$.

Similar entropy witnesses can be derived for the case of classical communication, by simply replacing $S(\varrho)$ with $H(M)$ in (8) and (9). Note that (9) is reminiscent of the principle of information causality [13], but considering here a prepare-and-measure scenario [14, 28]. That is, we consider classical correlations and quantum communication rather than quantum correlations and classical communication. Thus, these witnesses cannot distinguish classical from quantum systems. More specifically, given a set of data, the classical and quantum bounds on the entropy will be the same, although this may not be the case in general, as we will see below.

To summarize, the entropic approach allows us to derive compact and versatile entropy witnesses, for scenarios involving any number of preparations, measurements and outcomes. Moreover, the bounds obtained on the entropy are valid for systems of arbitrary finite dimension. Nevertheless, this approach has an important drawback, namely that the obtained bounds typically underestimate the minimum entropy actually required to produce a given set of data. This is because there exist in general many different sets of data giving rise to the same value of the witness [29], e.g. the LHS of (9). The entropy bound will thus correspond to the lowest possible value $S(\varrho)$ among these sets of data. Below we investigate a different approach, which better exploits the structure of the data. Moreover, this technique will allow one to distinguish between classical and quantum systems, contrary to the above witnesses.

Entropy witnesses II.— We now discuss a method for placing bounds on the entropy using the entire set of data $\mathbf{p}$. This method can then be simplified to make use of only linear functions of the probabilities $p(b|x,y)$; in this case, we shall see that entropy witnesses can be directly constructed from dimension witnesses. This will allow us to show that, in the DI setting, quantum systems can outperform classical ones in terms of entropy.

Consider the case of classical communication. At first sight, one of the main difficulties is that we need to consider strategies involving messages of arbitrary dimension. However, notice that in the case of a finite number n of preparations, we can focus on messages of dimension $d \leq n$ without loss of generality (see [25] Sec. III). It then follows that we have a finite number D of deterministic strategies labeled by λ. For each strategy, the message m is given by a deterministic function, $g_\lambda(x)$, and the output b is given by a deterministic function $f_\lambda(y,m)$. Then, any set of data can be decomposed as convex combination over the determin-

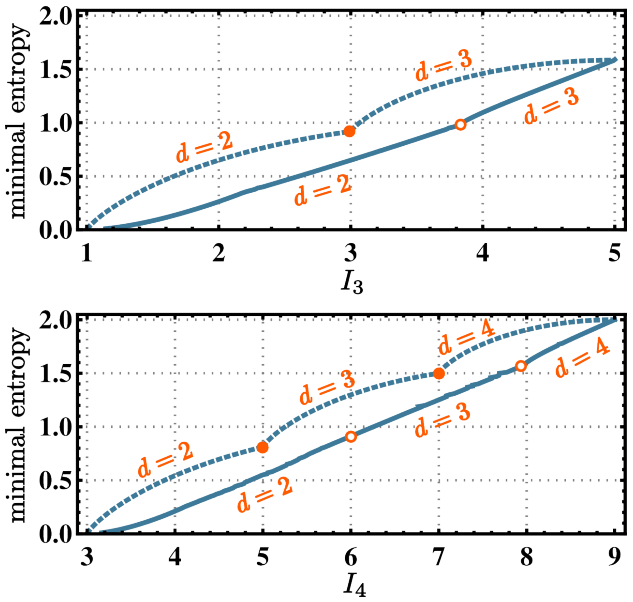

FIG. 2. Minimum values of $H(M)$ and $S(\varrho)$ compatible with a given value of witnesses I_3 or I_4. Curves for classical (dotted) and quantum (solid) strategies are shown. The use of quantum strategies allow for a significant reduction in the communication entropy.

istic strategies. More formally, we thus write $\mathbf{p} = \mathbf{A}\mathbf{q}$, where $\mathbf{q}$ is a D-dimensional vector with components $q_\lambda = p(\lambda)$ representing the probability to use strategy λ, and $\sum_\lambda q_\lambda = 1$. The matrix $\mathbf{A}$, of size $nlk \times D$, has elements $A_{(xyb),\lambda} = \delta_{b,f_\lambda(y,m)}\delta_{m,g_\lambda(x)}$.

The problem can thus be expressed as follows

$$\min H(M) \quad \text{s.t.} \quad \mathbf{A}\mathbf{q} = \mathbf{p}, q_\lambda \geq 0 \text{ and } \sum_\lambda q_\lambda = 1. \quad (10)$$

where the minimization is taken over all possible convex combinations of deterministic strategies that reproduce $\mathbf{p}$. Notice that this set of possible convex decompositions of $\mathbf{p}$ forms a polytope $\mathbb{Q}$ (in the space of $\mathbf{q}$). Thus, although the objective function $H(M)$ is not linear in $\mathbf{q}$, this problem can be addressed by noting that $H(M)$ is concave in $\mathbf{q}$. It follows that the minimum of $H(M)$ will be obtained for one of the vertices of $\mathbb{Q}$.

The above procedure is analytical, and can therefore be applied for any given $\mathbf{p}$, in principle. However, it is computationally too demanding, even in the simplest cases, mainly due to the characterization of the polytope $\mathbb{Q}$. We thus further simplify the problem. First, we consider specific linear functions of the data $V(\mathbf{p})$ (instead of the entire data $\mathbf{p}$). The first condition in (10) thus becomes $V(\mathbf{A}\mathbf{q}) = V(\mathbf{p})$. Moreover, we notice that this condition implies constraints on the distribution of the message $p(m)$, which can be characterized via a finite number of linear programs (see [25] Sec. IV for details).

We apply this method to the linear dimension witnesses $I_n(\mathbf{p})$ (see (5)) for $n \leq 5$ (in [25] Sec. IV we also discuss the $2 \to 1$ random access code). For each value of the witness I_n, we obtain the minimum on the entropy $H(M)$ compatible with it. Results for $n = 3, 4$ are shown on Fig. 2. Clearly $\min H(M)$ is a non-trivial function of I_n, for which we obtained (up to numerical precision) an explicit form for the entropy witness. Given a value of I_n in the range $L_{d-1} \leq I_n \leq L_d$ (i.e. requiring a d-dimensional message), the following witness holds:

$$H(M) \geq \frac{d-2}{n}\log n - \alpha \log \alpha - \beta \log \beta, \quad (11)$$

where $\alpha = (2 - (L_d - I_n))/2n$, $\beta = 1 - \alpha - (d-2)/n$. Moreover, this witness turns out to be tight, as the inequality can be saturated using a simple strategy. Upon receiving input $x \leq d-2$, send message $m = x$; if $x = d-1$, send $m = 0$ with probability $p = (L_d - I_n)/2$, and send $m = d-1$ with probability $(1-p)$; otherwise send $m = 0$. The entropy of the average message is then given by the right hand side of (11). Note that this strategy uses messages of dimension d. Hence, minimal entropy can be achieved using the lowest possible dimension. Another interesting feature is that no shared correlations between the preparation and measurement devices are needed. We also notice that, perhaps surprisingly, (11) turns out to provide optimal entropy for all dimension witnesses that we have tested (see [25] Sec. IV). Whether this strategy is optimal for any dimension witness is an interesting open question. In any case, (11) provides a non-trivial upper bound on $\min H(M)$. We refer to [25] Sec. VII for a comparison between (11) and the entropy inequality (9).

A relevant question is now to see if the use of quantum communication may help reducing the entropy. That is, for a given witness value, we ask what is the lowest possible entropy achievable using quantum systems. This is in general a difficult question, as we have no guarantee that using low-dimensional systems is optimal. Nevertheless, we can obtain upper bounds on $S(\varrho)$ by considering low dimensional systems. We performed numerical optimization for quantum strategies involving systems up to dimension $d = 4$ (see [25] Sec. VI). Results are presented in Fig. 2. Interestingly, the use of quantum systems allows for a clear reduction of the entropy (compared to classical messages) for basically any witness value. Whether the use of higher dimensional systems could help reduce $S(\varrho)$ further is an interesting open question.

Conclusion.—We have shown that the entropy, a fundamental quantity in classical and quantum information, can be tested in a DI way. Two complementary methods tailored for this task were presented. The first, based on inference networks, can be readily applied to very general scenarios, but gives usually suboptimal bounds. The second method gives tight bounds on the

entropy, allowing to show that quantum communication provides an advantage over classical, since it requires a lower entropy to reproduce given data. However, since is based on convex optimization, its direct application is restricted to simpler scenarios. Nonetheless, using this method we have shown how entropy witnesses can be directly constructed from dimension witnesses inequalities.

The simplest tests presented here are certainly amenable to experiments and would provide an interesting new perspective to the recent experimental DI characterization of the dimension of quantum systems [17]. Moreover, given the success of the DI approach for quantum information processing, it would be interesting to investigate potential applications based on the present work, in particular in the context of the semi-DI approach [30, 31]. The latter is intermediate between the fully DI approach and the standard (device-dependent) one, and thus combines partial DI security and ease of implementation [32, 33]. Semi-DI protocols are prepare-and-measure, and their security has been so far based on the assumption that the mediating system is of bounded dimension, e.g. qubits. It would be interesting to see if security could also be guaranteed based on the assumption that the system has limited entropy, which is indeed a strictly weaker assumption and perhaps more natural in a communication protocol.

Acknowledgements.—We thank Tamás Vértesi for useful discussions. We acknowledge financial support from the Excellence Initiative of the German Federal and State Governments (Grants ZUK 43 & 81), the US Army Research Office under contracts W911NF-14-1-0098 and W911NF-14-1-0133 (Quantum Characterization, Verification, and Validation), the DFG (GRO 4334 & SPP 1798), the Swiss National Science Foundation (grant PP00P2_138917 and Starting Grant DIAQ), SEFRI (COST action MP1006), and the EU SIQS.

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[2] R. Colbeck, *Ph.D. Thesis*, Ph.D. thesis, University of Cambridge (2007).
[3] S. Pironio *et al.*, Nature **464**, 1021 (2010).
[4] B. G. Christensen *et al.*, Phys. Rev. Lett. **111**, 130406 (2013).
[5] J. S. Bell, Physics **1**, 195 (1964).
[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[7] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).
[8] T. Vértesi and K. F. Pál, Phys. Rev. A **77**, 042106 (2008).
[9] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).
[10] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).
[11] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[12] W. van Dam, arXiv e-print, 0501159 (2015).
[13] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, Nature **461**, 1101 (2009).
[14] N. Brunner, M. Kaplan, A. Leverrier, and P. Skrzypczyk, New Journal of Physics **16**, 123050 (2014).
[15] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[16] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).
[17] M. Hendrych, R. Gallego, M. Micuda, N. Brunner, A. Acin, and J. P. Torres, Nat Phys **8**, 588 (2012); J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nat Phys **8**, 592 (2012); V. D'Ambrosio, F. Bisesto, F. Sciarrino, J. F. Barra, G. Lima, and A. Cabello, Phys. Rev. Lett. **112**, 140503 (2014).
[18] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, and V. Scarani, Phys. Rev. Lett. **107**, 050502 (2011).
[19] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).
[20] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).
[21] J. Pearl, *Causality* (Cambridge University Press, 2009).
[22] R. Chaves, L. Luft, T. O. Maciel, D. Gross, D. Janzing, and B. Schölkopf, Proceedings of the 30th Conference on Uncertainty in Artificial Intelligence , 112 (2014).
[23] R. Chaves, C. Majenz, and D. Gross, Nature communications **6** (2015).
[24] R. Chaves and T. Fritz, Phys. Rev. A **85**, 032113 (2012); T. Fritz and R. Chaves, IEEE Trans. Inform. Theory **59**, 803 (2013); R. Chaves, L. Luft, and D. Gross, New J. Phys. **16**, 043001 (2014).
[25] See Supplementary Material [URL], which includes Ref. [34–36], for details of the two methods for deriving entropy witnesses, as well as the optimisation for quantum strategies.
[26] A. Holevo, Problems of Information Transmission **9**, 177 (1973).
[27] Note that the method also applies for arbitrary number of preparations x. Simply assign zero probability to all but n of the possible inputs $(x_1, \ldots, x_l)$.
[28] L. Czekaj, M. Horodecki, P. Horodecki, and R. Horodecki, arXiv e-print, 1403.4643 (2014).
[29] R. Chaves, Phys. Rev. A **87**, 022102 (2013).
[30] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).
[31] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[32] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[33] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, arXiv preprint arXiv:1410.3443 (2014).
[34] R. W. Yeung, *Information theory and network coding*, Infor-

mation technology–transmission, processing, and storage (Springer, 2008).
[35] H. P. Williams, Amer. Math. Monthly **93**, 681 (1986).
[36] R. Chaves, R. Kueng, J. B. Brask, and D. Gross, Phys. Rev. Lett. **114**, 140403 (2015).