Semi-device-independent framework based on natural physical assumptions

Semi-device-independent framework based on natural physical assumptions

Thomas Van Himbeeck[1,2], Erik Woodhead[3], Nicolas J. Cerf[2], Raúl García-Patrón[2], and Stefano Pironio[1]

[1]Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium
[2]Centre for Quantum Information and Communication, Université libre de Bruxelles (ULB), Belgium
[3]ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

October 6, 2017

The semi-device-independent approach provides a framework for prepare-and-measure quantum protocols using devices whose behavior does not need to be characterized or trusted, except for a single assumption on the dimension of the Hilbert space characterizing the quantum carriers. Here, we propose instead to constrain the quantum carriers through a bound on the mean value of a well-chosen observable. This modified assumption is physically better motivated than a dimension bound and closer to the description of actual experiments. In particular, we consider quantum optical schemes where the source emits quantum states described in an infinite-dimensional Fock space and model our assumption as an upper bound on the average photon number in the emitted states. We characterize the set of correlations that may be exhibited in the simplest possible scenario compatible with our new framework, based on two energy-constrained state preparations and a two-outcome measurement. Interestingly, we uncover the existence of quantum correlations exceeding the set of classical correlations that can be produced by devices behaving in a purely pre-determined fashion (possibly including shared randomness). This feature suggests immediate applications to certified randomness generation. Along this line, we analyze the achievable correlations in several prepare-and-measure optical schemes with a mean photon-number constraint and demonstrate that they allow for the generation of certified randomness. Our simplest optical scheme works by the on-off keying of an attenuated laser source followed by photocounting. It opens the path to more sophisticated energy-constrained semi-device-independent quantum cryptography protocols, such as quantum key distribution.

1 Introduction

Understanding the nature and extent of correlations that distinct systems may display is a central problem in many applications of quantum physics. In particular, it is an essential stone for developing device-independent (DI) quantum information protocols [1–7], where the correlations that are observed between separate quantum devices provide a guarantee that the protocol performs as expected. This guarantee follows independently

Thomas Van Himbeeck: thomas.van.himbeeck@ulb.ac.be

of any assumptions on the local behavior of the quantum devices, hence its name, but it must necessarily rely on some specific constraints on the information that they exchange. Indeed, if arbitrary, unlimited communication is allowed between the devices, any kind of correlations can be generated, even in a scenario restricted to classical physics.

In the standard DI framework based on Bell non-locality [8], the constraint on communication is maximal: the separate devices are not allowed to communicate any type of information, neither classical nor quantum. This no-communication constraint has the conceptual advantage of having a clear physical and operational significance. In particular, it is in principle possible to enforce it without knowledge of the internal behavior of the devices, i.e., by adequate shielding or space-like separation of the devices. However, the generation of useful, non-classical correlations in the absence of quantum communication must then necessarily rely on (loophole-free) entanglement, which presently represents a serious obstacle to practical DI applications.

This difficulty has motivated the development of an alternative framework for DI applications, which is inspired by the traditional prepare-and-measure implementation of quantum key distribution and where communication is allowed between the quantum devices. As noted above, a constraint, though, must be put on this communication and it is usually formulated as a bound on the Hilbert space dimension of the exchanged quantum messages [9–11]. With such a constraint, useful non-classical correlations can already be generated by restricting the communication to qubits or qutrits in a purely prepare-and-measure scenario, without the need of entanglement, which provides a clear advantage from the implementation point of view. Several protocols for randomness generation (RNG) [12] and quantum key distribution (QKD) [13, 14] have been introduced within this framework, which is usually referred to as "semi-device-independent" (semi-DI). The downside, however, is that the dimension assumption, even if it represents a convenient abstraction for a theorist, is only an idealization. Carriers of quantum information, such as photons, live in an infinite Hilbert space, and assuming that information is encoded in only a few degrees of freedom is not justified without some intricate characterization of the devices (hence the terminology "semi device independent").

In this paper, we propose a physically better motivated approach for constraining the exchanged quantum messages in a semi-DI framework. We express the restriction on the exchanged states in terms of the mean values of some well-chosen observable, such as the energy. As a simple example, consider the case where the Hilbert space carrying the quantum messages is the Fock space of several quantum optical modes. This is the appropriate space to describe quantum optics experiments, including those demonstrating results based on dimension bounds, in which attenuated laser sources [15] or non-ideal heralded photon sources [12, 16] are used. In this context, the emitted states can in principle occupy an infinite-dimensional space so that, instead of putting a limit on the dimension, it is much more natural to constrain the average number of photons. The corresponding observable would then be the photon-number operator, which has a clear physical significance. Alternatively, we could constrain the energy contained in one or more frequency modes containing the quantum message, as the two are closely related. This is thus a natural substitute for the dimension of a finite Hilbert space. Moreover, designing devices in such a way that the average photon number does not exceed a given threshold or verifying experimentally that it does not exceed such a threshold will typically require a less detailed modeling of the devices than would be needed to verify, e.g., that the emitted states span a Hilbert space of a given dimension.

A prerequisite for the development of any DI or semi-DI protocol is to examine the set of correlations that are available under the assumptions considered. Much work has been done specifically on this question in the standard settings based on non-locality

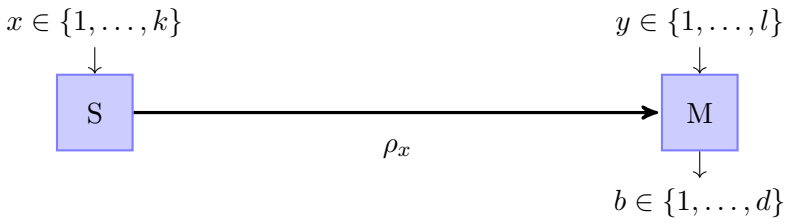


Figure 1: A general prepare-and-measure scenario. Source (S) emits one of k states ρ_x depending on an input $x \in \{1, \ldots, k\}$. A measurement device (M) performs one of l measurements on the state received, depending on an input $y \in \{1, \ldots, l\}$, and registers an outcome $b \in \{1, \ldots, d\}$. The behaviors of S and M are not characterized and could even depend on shared hidden parameters λ. But we trust that the prepared states satisfy constraints that are expressed in term of the expectations $\mathrm{tr}[H\rho_x]$ of some given Hermitian operator H.

and dimension bounds, see e.g. [8, 17–22] and [9–11, 23, 24]. Here, we fully characterize analytically the set of available correlations in the simplest scenario compatible with our general framework. This uncovers interesting features suggesting immediate applications to randomness generation, which will be fully developed in a forthcoming publication [25].

In Section 2, we introduce the general framework of semi-DI prepare-and-measure scenarios and modify it to account for a physical constraint (mean value of an observable) instead of a dimension bound. We define a simple setting with two state preparations and a single measurement with binary outcomes, which suffices to produce a separation between the quantum and classical correlations, and subsequently suggest a few simple potential implementations using currently accessible quantum optics technology. The quantum region (i.e., the set of available quantum correlations) is analyzed in Sections 3 and 4, while the classical region (i.e., the set of available correlations arising from a mixture of classical deterministic behaviors) is studied in Section 5. Then, in Section 6, with an eye toward the application to certified random number generation, we characterize an intermediate deterministic region; correlations outside of this region are those for which randomness can be certified for a specified input. We also show that correlations outside this intermediate region are achievable with simple optical implementations. Finally, we conclude in Section 7 and discuss other possible applications.

2 Semi-DI setting with a physical constraint

2.1 Definition of the general model

Let us first remind the general framework of semi-DI prepare-and-measure scenarios. As depicted in Fig. 1, a source S is linked through a quantum channel to a measurement device M. On the source S, an input $x \in \{1, \ldots, k\}$ can be selected, resulting in the emission of an unknown quantum state ρ_x. The state is then measured by M, according to a measurement selected through an input $y \in \{1, \ldots, l\}$, and yields an outcome $b \in \{1, \ldots, d\}$. This later process is characterized by a set of unknown measurement operators $\{M_{b|y}\}$.

To an external observer that has access only to the inputs and output of S and M, the joint behavior of the two devices is completely characterized by the probabilities

$$P(b|y, x) = \mathrm{tr}[M_{b|y}\, \rho_x]\,. \tag{1}$$

More generally, the behavior of the two devices could be correlated through dependence on an additional hidden random parameter λ shared between the devices, in which case

the probabilities take the more general form

$$P(b|y,x) = \sum_{\lambda} p_\lambda \operatorname{tr}\left[M^{\lambda}_{b|y}\, \rho^{\lambda}_{x}\right] . \tag{2}$$

In the semi-DI approach, no detailed assumptions are made on the states and measurements underlying the correlations $P(b|y,x)$, except for a specific constraint on the messages ρ_x. Here, we propose to express such a constraint in terms of an observable H, describing a physical property of the emitted states ρ_x that we trust or on which we have control (more generally, one could introduce several such observables). A restriction on the quantum messages ρ_x can then be formulated as a constraint on the corresponding mean values $H_x = \operatorname{tr}[H\rho_x]$ of this observable.

Note that contrarily to the states ρ_x and measurement operators $M_{b|y}$, which are a priori unspecified and unknown, the observable H must be well defined. It is also implicit that it should be defined on some given (possibly infinite) Hilbert space $\mathcal{H}$ describing the physics of the quantum systems emitted by S. Thus, one should also assume that ρ_x is defined on $\mathcal{H}$.

This general formulation encompasses the usual dimension assumption, for instance, by defining H as the projector onto a qudit subspace of $\mathcal{H}$ and requiring $H_x = 1$ for all x. Expressing the dimension assumption in this form has the merit of making explicit that the message qudits live in a subspace of a larger Hilbert space $\mathcal{H}$, which in practice must also be properly defined and characterized if one wants to make sure that information is propagating in the relevant subspace and not in possible additional degrees of freedom, which in a cryptographic protocol could be exploited by an eavesdropper (side channels).

As stated in the introduction, the main interest of our more general formulation, however, is that it can be used to model communication constraints that are more natural and better motivated physically than the usual dimension bounds. A particular example is the case where H is the photon-number operator of a quantum optical system.

With this application in mind, we will consider in this work two types of constraints on the mean values of H. The first, which we denote the *max-average assumption*, corresponds to assuming upper bounds

$$H_x = \operatorname{tr}[H\rho_x] = \sum_{\lambda} p_\lambda \operatorname{tr}[H\rho^{\lambda}_{x}] \leq \omega_x \,, \quad \forall x \tag{3}$$

on the mean values H_x for given thresholds ω_x. For instance, if H is the photon-number operator, we may trust that for all states ρ_x emitted by the source, the mean photon numbers H_x are below some threshold, though we may not know what the actual photon number is.

In the case where the states emitted by S vary from run to run according to some random parameter λ, the max-average assumption only bounds the mean value H_x averaged over all possible values of λ. But it does not constrain the maximum values of $H_{x|\lambda} = \operatorname{tr}[H\rho^{\lambda}_{x}]$, which could in principle be arbitrarily high. It is therefore natural to introduce another (stronger) assumption, which we call the *max-peak assumption*, according to which

$$\max_{\lambda} H_{x|\lambda} = \max_{\lambda} \operatorname{tr}[H\rho^{\lambda}_{x}] \leq \omega_x \,, \quad \forall x \,. \tag{4}$$

Note that if H is, e.g., the photon-number operator, this second condition still allows for fluctuations in the photon number within each state ρ^{λ}_{x} and does not correspond to a truncation of the Fock space, as the constraint only imposes a bound on the *mean* values $\operatorname{tr}[H\rho^{\lambda}_{x}]$ of H for every ρ^{λ}_{x}. In particular, the states ρ^{λ}_{x} could have a non-zero amplitude in any of the number-basis states.

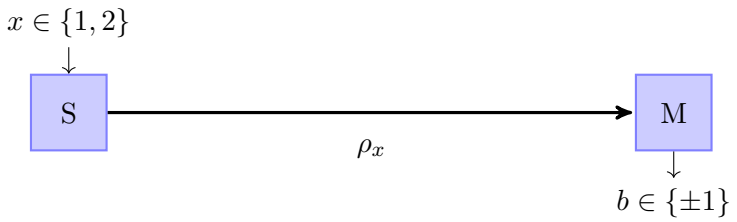


Figure 2: The prepare-and-measure scenario considered here, a special case of Fig. 1.

These two possible physically-motivated constraints on the communicated quantum messages will be analyzed on specific examples later on. The max-average assumption has the advantage that it could in principle be verified "from the outside" by performing tests on the average emitted states ρ_x without any knowledge of the internal behavior of the source. Verifying that the max-peak assumption is satisfied, on the other hand, would typically rely on some modeling of the source. Its main advantage is that it is more constraining and thus can certify useful properties that wouldn't be certified using the average-peak assumption (see examples in Sections 5 and 6).

2.2 The simplest setting: two inputs and two outputs

In the rest of this paper, we consider the simple situation where the source S has two possible inputs $x \in \{1,2\}$ and the measurement device M has no input (i.e., $y \in \{1\}$) and two possible outputs, which we denote $b \in \{\pm 1\}$ for convenience, see Fig. 2. Note that this corresponds to the simplest non-trivial prepare-and-measure scenario. Indeed, M must obviously output at least two different possible values, and S must have at least two different preparation choices, otherwise no quantum messages are needed and any observed behavior can be classically simulated by S and M.

This prepare-and-measure scenario is simpler than any possible scenario based on a dimension bound, for which one must have at least three choices on the source, i.e., $x \in \{1,2,3\}$, and any measurement device outputting a single bit $b \in \{\pm 1\}$ should have at least two inputs, i.e., $y \in \{1,2\}$. Indeed, since the smallest dimension bound corresponds to one qubit, the channel connecting S to M always has a capacity of at least 1 bit under a dimension assumption. This implies that the number of inputs on S should be larger than two, because otherwise the input x can be encoded perfectly in the channel and transmitted to M, who knowing x can now generate an output b compatible with any probability distribution $p(b|x,y)$. There should also be a number of binary measurements greater than one, because otherwise S could locally choose a value $b \in \{\pm 1\}$ compatible with any probability distribution $p(b|x)$ and simply send that value b to M through the channel. Strikingly, such strategies are not available under the assumptions that we consider here, since, as we will see, they constrain the classical channel capacity to be sub-unity by forcing the two emitted states ρ_1 and ρ_2 to have some non-zero overlap.

In our scenario, the joint behavior of S and M is thus characterized by the four probabilities $P(b|x) = \mathrm{tr}[M_b \rho_x]$ where $x = 1,2$ and $b = \pm 1$. It will be convenient to work with the equivalent representation

$$E_x = \mathrm{tr}[M \rho_x] \qquad (x = 1,2)\,, \tag{5}$$

where $E_x = P(+1|x) - P(-1|x)$ is the expectation value of the observable $M = M_{+1} - M_{-1}$, with $-\mathbb{1} \leq M \leq \mathbb{1}$. The value of E_x characterizes the bias of the output b toward $+1$ or -1 for a given input x. We refer in the following to the quantities E_x as "correlations" as they represent how the output of M is correlated to the input of S. For instance if $E_1 = 1$

and $E_2 = -1$, the output of M is completely correlated to the input of S. More precisely, the presence of correlations is actually reflected by the fact that $|E_-| = |E_1 - E_2| > 0$. In particular, a value $|E_-| > 0$ implies that the measurement device M can (at least partly) distinguish the two states ρ_1 and ρ_2. We will see further below that the quantity E_- plays a special role in our analysis, analogous to a Bell expression in the context of non-locality.

Having defined the general behavior of S and M, we now specify the properties of the observable H that we use to model our assumptions on the quantum messages. As noted above, in our scenario the two states ρ_1, ρ_2 should have a non-zero overlap, otherwise they could encode faithfully the two values $x = 1, 2$ and our entire problem would become trivial. One simple possibility for satisfying this condition in an optical system is simply to have both states ρ_1, ρ_2 sufficiently close to the vacuum state $|0\rangle$. In a multimode system with a discrete and finite number of possible mode frequencies ω, this amounts to upper bounding the expectation values of the photon-number operator $H = \sum_\omega a_\omega^\dagger a_\omega$ or the energy operator $H = \sum_\omega \hbar\omega\, a_\omega^\dagger a_\omega$. Alternatively, one could directly bound the weight of the non-vacuum component, i.e., the expected value of the non-vacuum projector $H = \mathbb{1} - |0\rangle\langle 0|$. More generally, the condition that ρ_1, ρ_2 have a non-zero overlap is satisfied if they are both close to some given reference state $|\phi\rangle\langle\phi|$, i.e., if the expectation values H_x of the observable $H = \mathbb{1} - |\phi\rangle\langle\phi|$ are below some sufficiently small thresholds.

Formally, all the above examples correspond to constraints on the expected values of an observable H satisfying the two following conditions:

1. H has a non-degenerate ground state,

2. H has a finite gap.

The results that we will derive below apply to any observable H satisfying these two conditions, independently of their physical meaning. Without loss of generality, we can assume (if necessary by rescaling H) that the ground state eigenvalue is 0 and the gap is 1. In the following, we let $|0\rangle$ denote the ground state of H.

Before characterizing, in Sections 3 and 4, the set of possible correlations E_x between S and M in terms of the constrained mean values H_x of such observables H, we briefly describe for concreteness some standard optical circuit implementations that can be analyzed in our framework.

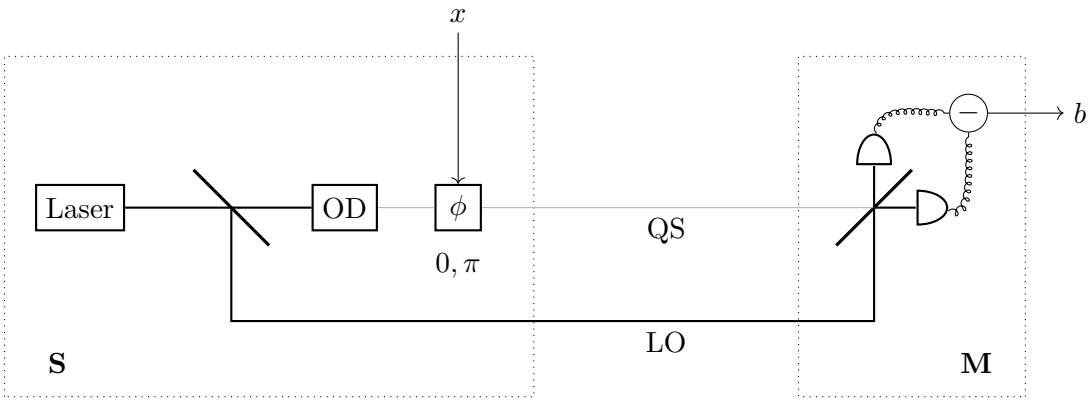
2.3 Examples of optical circuits

2.3.1 Binary Phase-Shift Keying (BPSK)

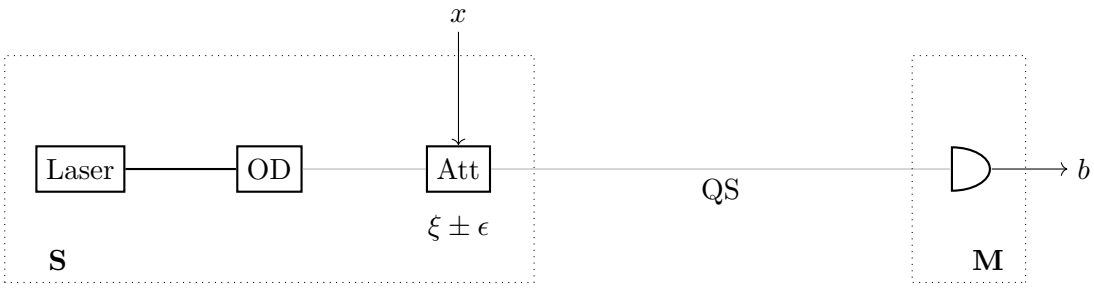
Our first optical implementation corresponds to the Binary Phase-Shift Keying (BPSK) scheme and is illustrated in Fig. 3(a). We consider a single optical mode described over the phase space (X, P) of the two quadratures of light ($[X, P] = \frac{i}{2}$). Depending on x, the source prepares one of two coherent states $|\phi_1\rangle = |\xi\rangle$ or $|\phi_2\rangle = |-\xi\rangle$, where ξ is a small positive real parameter, so that both states are close to the vacuum $|0\rangle$. Although these two states have a non-zero overlap $e^{-2|\xi|^2}$, it is possible to partly distinguish them by performing a homodyne measurement of the quadrature X. In particular if we define the output of the measurement device M as $b = \mathrm{sign}(X)$, then a straightforward calculation gives

$$E_1 = \mathrm{erf}(\sqrt{2}\xi)\,, \qquad\qquad E_2 = -\,\mathrm{erf}(\sqrt{2}\xi)\,, \tag{6}$$

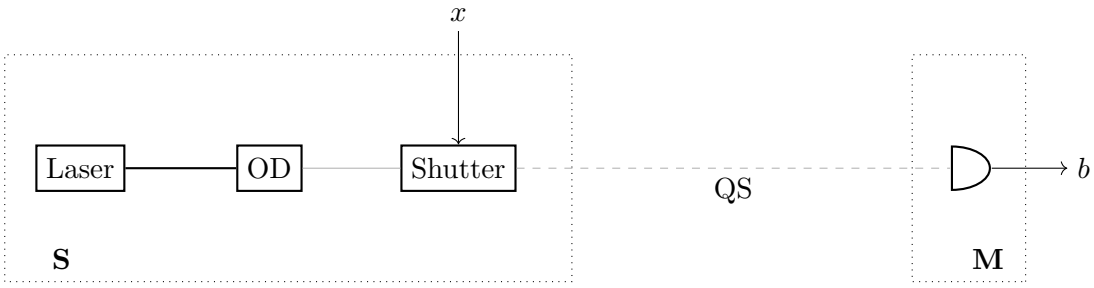
i.e., we observe a correlation between the sign of b and the input x whose strength depends on the value ξ.



(a) BPSK implementation. The source (S) consists of a laser that produces a coherent pulse which is sent through an unbalanced beam splitter. The intense reflected beam is sent to the measurement device (M) as a phase reference, i.e., local oscillator (LO); the transmitted beam is highly attenuated at an optical density (OD) and phase shifted by 0 or π depending on x at a phase shifter. This is the quantum signal (QS) sent to M. M then performs a homodyne measurement on QS: the two beams interfere on a balanced beam splitter and two photodiodes measure the intensities of the resulting beams. The difference of the two intensities is proportional to the quadrature X of the quantum signal. Finally, M outputs the sign of X. Note that the LO does not depend on the input x and can be modeled as shared randomness.



(b) 2ASK implementation. The source (S) consists of a laser that produces a coherent pulse, which is, at first, highly attenuated at an optical density (OD), and then sent through a variable attenuator (Att), so that, depending on x, the amplitude of the resulting coherent states is $\xi \pm \epsilon$. This is the quantum signal (QS) sent to the measurement device (M). M is a single-photon detector that outputs $b = +1$ if it clicks, and $b = -1$ otherwise.



(c) OOK implementation. The source (S) consists of a laser that produces a coherent pulse, which is, at first, highly attenuated at an optical density (OD). A controllable shutter then transmits or blocks the beam depending on the value of x. The measurement device is a single-photon detector that outputs $b = +1$ if it clicks, and $b = -1$ otherwise. Alternatively to the use of a shutter, the laser can simply be turned on and off depending on x.

Figure 3: Three experimental implementation propositions.

A semi-DI analysis for this setup (see Sections 5 and 6) is possible based only on the assumption that the source emits optical systems with low mean photon number (choosing $H = \sum_\omega a_\omega^\dagger a_\omega$) or small non-vacuum component (choosing $H = \mathbb{1} - |0\rangle\langle 0|$). The coherent states $|\pm\xi\rangle$ have a mean photon number $|\xi|^2$ and non-vacuum component $1 - e^{-|\xi|^2}$, where the mean photon number is larger than the non-vacuum component: $|\xi|^2 > 1 - e^{-|\xi|^2}$. Thus for given ξ, one can impose more constraining bounds if one defines H as the non-vacuum projector rather than the photon-number operator and we will thus make the former choice in the following. The difference between $1 - e^{-|\xi|^2}$ and $|\xi|^2$, though, is negligible when ξ is small and this choice does not fundamentally affect our results. When performing the semi-DI analysis of the above setup, we will thus take $H = \mathbb{1} - |0\rangle\langle 0|$ and upper bound the expectation values of this operator through the max-average assumption (3) or the max-peak assumption (4) using thresholds

$$\omega_1 = \omega_2 = 1 - e^{-|\xi|^2} . \tag{7}$$

Note that in the implementation illustrated in Fig. 3(a), in addition to the quantum states $|\phi_x\rangle$, the source also emits an intense reference laser beam that serves as a local oscillator to define the phase of these states. This local oscillator can, however, be modeled as shared randomness (for instance it could exit the source S before the input x is chosen). Alternatively, one could also consider more involved implementations where a phase synchronization between S and M can be achieved without the need for the transmission of a local oscillator signal between S and M [26].

2.3.2 2-level Amplitude-Shift Keying (2ASK)

Our second example corresponds to the 2-level Amplitude-Shift Keying (2ASK) scheme and is illustrated in Fig. 3(b). The source emits the two coherent states $|\phi_1\rangle = |\xi + \epsilon\rangle$ or $|\phi_2\rangle = |\xi - \epsilon\rangle$, where ξ and ϵ are two real, positive parameters. The measurement device is a photodetector that outputs $b = -1$ if no photon is detected and $b = +1$ if at least one photon has been detected. This setup generates the correlations

$$E_1 = 1 - 2e^{-(\xi+\epsilon)^2} , \qquad E_2 = 1 - 2e^{-(\xi-\epsilon)^2} . \tag{8}$$

Suitable choices for ξ and ϵ can easily be found so that $|E_1 - E_2| > 0$, i.e., such that the output of M and the input of S are correlated.

In this second example, the two states $|\phi_1\rangle = |\xi + \epsilon\rangle$ and $|\phi_2\rangle = |\xi - \epsilon\rangle$ are not necessarily close to the vacuum if ξ is large, but they are close to the intermediate state $|\xi\rangle$. We thus define for the purpose of the semi-DI analysis of this setup (see Sections 5 and 6) the observable H as $H = \mathbb{1} - |\xi\rangle\langle\xi|$, which measures the proximity of the states $|\phi_x\rangle$ to the reference state $|\xi\rangle$. Specifically, we have $\langle\phi_x|H|\phi_x\rangle = 1 - e^{-\epsilon^2} \simeq \epsilon^2$ for $x = 1, 2$. Thus we will constrain the expected values of H using thresholds

$$\omega_1 = \omega_2 = 1 - e^{-\epsilon^2} . \tag{9}$$

Note that, contrarily to the previous example, such an assumption on the expectation values of H may actually require a more detailed characterization of the source. First, the observable does not correspond to a natural property, like the energy, and, second, an experimental verification of the assumption would require a displacement operation with a beam that is coherent with the quantum message followed by a photon number measurement. It is thus probably not the most natural in a semi-DI setting. We nevertheless include this example to stress that our formulation can be adapted to different constraints on the source.

2.3.3 On-Off Keying (OOK)

Our final example corresponds to the On-Off Keying (OOK) scheme and is illustrated in Fig. 3(c). When $x = 1$, the source emits a coherent state $|\xi\rangle$ where $|\xi|^2$ is small, and when $x = 2$ it emits the vacuum state $|0\rangle$. The measurement performed at M corresponds, as in the previous example, to a photodetector that outputs $b = -1$ if no photon is detected and $b = +1$ if at least one photon has been detected. This yields

$$E_1 = 1 - 2e^{-|\xi|^2} \simeq -1 + 2|\xi|^2 , \qquad E_2 = -1 . \tag{10}$$

That is, when $x = 2$ one obviously observes the result $b = -1$ with certainty, while when $x = 1$, there is a non-zero probability $1 - e^{-|\xi|^2} \simeq |\xi|^2$ to obtain the outcome $b = +1$. The measurement performed at M can thus be interpreted as a partial unambiguous discrimination of the two states ρ_1, ρ_2 in the sense that when we find $b = +1$, we are sure that the state sent was ρ_1, but we cannot conclude anything definite when $b = -1$.

As in the first example, the semi-DI analysis for this setup (see Sections 5 and 6) will only rely on the assumption that the source emits optical systems with low non-vacuum component, i.e., we use $H = \mathbb{1} - |0\rangle\langle 0|$. The non-vacuum component is $1 - e^{-|\xi|^2}$ for $x = 1$ and 0 for $x = 2$ and we will thus use the thresholds

$$\omega_1 = 1 - e^{-|\xi|^2} , \qquad \omega_2 = 0 . \tag{11}$$

Note that contrarily to the two above examples, here we bound differently the expectation values of H in the case $x = 1$ and $x = 2$ since the implementation is not symmetric with respect to the two situations. Alternatively to bounding the non-vacuum component, we could use the mean photon number, but the difference would be negligible when ξ is small and making one choice or the other does not fundamentally affect our results.

3 Pure-state quantum correlations

As we have explained earlier, a prerequisite for the development of any DI or semi-DI protocol is to examine the set of correlations that are available under the assumptions considered. One of our objectives is thus to characterize the most general set of quantum correlations (E_1, E_2) compatible with arbitrary implementations of our prepare-and-measure scenario.

In general, the source S and the measurement device M could behave in a way depending on shared random parameters λ. As a first step, it is useful to consider the case where the devices do not exploit such shared randomness and where in addition the source S emits *pure* states ϕ_1, ϕ_2. In Section 4, we will relax these conditions and consider completely general implementations.

Let us therefore define the set of pure-state correlations as

$$\mathcal{Q}_{H_1,H_2} = \left\{ (E_1, E_2) \mid E_x = \mathrm{tr}[M\phi_x],\ H_x = \mathrm{tr}[H\phi_x] \text{ for } x = 1, 2 \right\} , \tag{12}$$

that is, the set of possible values (E_1, E_2) that are attainable with arbitrary pure states $\phi_x = |\phi_x\rangle\langle\phi_x|$ and an arbitrary measurement operator M satisfying $-\mathbb{1} \leq M \leq \mathbb{1}$, and which are compatible with given expectation values (H_1, H_2) for an observable H with non-degenerate ground state, lowest eigenvalue 0, and finite gap 1. To simplify the notation, we will often write $\mathcal{Q}$ for $\mathcal{Q}_{H_1,H_2}$ with the implicit understanding that the values (H_1, H_2) are fixed.

A first observation is that if $H_1 + H_2 = 1$ then any correlations (E_1, E_2) satisfying the trivial constraints $|E_x| \leq 1$ belong to $\mathcal{Q}$. Indeed, let $|0\rangle$ be the ground state of H

and $|1\rangle$ an eigenstate with eigenvalue 1. Clearly, $H_1 + H_2 = \mathrm{tr}[H(\phi_1 + \phi_2)] = 1$ can be obtained for any two orthogonal states $|\phi_1\rangle$ and $|\phi_2\rangle$ in the space spanned by $|0\rangle$ and $|1\rangle$. Therefore, one cannot exclude that S emits two *orthogonal* pure states ϕ_1 and ϕ_2. But in this case, they can encode faithfully the two values $x = 1, 2$ and any correlations (E_1, E_2) are possible, for instance by setting M to $M = E_1\phi_1 + E_2\phi_2$.

However, if $H_1 + H_2 < 1$, then intuitively H_1 and H_2 are both small and both close to the non-degenerate ground state $|0\rangle$ of H. Thus they should have a non-zero overlap which will restrict the set of possible correlations (E_1, E_2). This intuition is made precise by the following result.

For $H_1, H_2 \geq 0$ and $H_1 + H_2 \leq 1$, the set $\mathcal{Q}_{H_1,H_2}$ consists of the values (E_1, E_2) satisfying $|E_x| \leq 1$ and

$$g(E_1, E_2) \geq h(H_1, H_2)\,, \tag{13}$$

where

$$g(E_1, E_2) = \frac{1}{2}\Big(\sqrt{1+E_1}\sqrt{1+E_2} + \sqrt{1-E_1}\sqrt{1-E_2}\Big)\,, \tag{14}$$

$$h(H_1, H_2) = \sqrt{1-H_1}\sqrt{1-H_2} - \sqrt{H_1}\sqrt{H_2}\,. \tag{15}$$

The trivial constraints $|E_x| \leq 1$ follow immediately from the definition of these quantities, so we only need to establish (13). We do this in two steps. First of all, given two pure states ϕ_1, ϕ_2, the set of correlations $(E_1, E_2) = (\mathrm{tr}[M\phi_1], \mathrm{tr}[M\phi_2])$ that can be obtained using an arbitrary measurement M obviously only depends on the scalar product $|\langle\phi_1|\phi_2\rangle|$. We show in Subsection 3.1 that this set is completely characterized by the constraint

$$g(E_1, E_2) \geq |\langle\phi_1|\phi_2\rangle|\,. \tag{16}$$

We then show in Subsection 3.2 that the parameters H_1, H_2 imply a tight lower bound on the scalar product,

$$|\langle\phi_1|\phi_2\rangle| \geq h(H_1, H_2)\,. \tag{17}$$

Combining these two bounds we obtain the relation $g(E_1, E_2) \geq h(H_1, H_2)$ in (13).

Note that we characterize the set $\mathcal{Q}$ only for values of H_1, H_2 such that $H_1 + H_2 \leq 1$. Indeed, in the next sections we are going to use pure-state correlations in $\mathcal{Q}$ as building blocks for more general sets of correlations but under the assumption that the possible expectation values H_x of the observable H are *upper bounded* by some given thresholds ω_x, as in (3) and (4). But since any correlations (E_1, E_2) are already possible in the case $H_1 + H_2 = 1$, as we pointed out above, there is obviously no advantage in considering larger values $H_1 + H_2 > 1$ to comply with the assumed thresholds. From now on, we thus always consider that $H_1 + H_2 \leq 1$ (and similarly that $\omega_1 + \omega_2 \leq 1$ in bounds of the type (3) and (4)).

3.1 Characterization of the possible correlations (E_1, E_2) for pure states as a function of their scalar product $\big|\langle\phi_1|\phi_2\rangle\big|$

Since $|E_x| \leq 1$, the region of possible values (E_1, E_2) is obviously contained in the square $[-1, 1] \times [-1, 1]$. We now show how a promise on the scalar product $|\langle\phi_1|\phi_2\rangle| = \gamma$ further constrains the possible values of (E_1, E_2).

The parameter γ satisfies $0 \leq \gamma \leq 1$. The two extreme cases are readily solved. When $\gamma = |\langle\phi_1|\phi_2\rangle| = 1$, the two states are indistinguishable and the measurement statistics must necessarily yield $E_1 = E_2$. When $\gamma = 0$, the two states are orthogonal and thus can perfectly encode the value of the input x. In particular, we can attain any value $(E_1, E_2) \in [-1, 1] \times [-1, 1]$ by setting M to $M = E_1\phi_1 + E_2\phi_2$. These two situations can

be summarized by the relation $g(E_1, E_2) \geq \gamma$, which implies $E_1 = E_2$ when $\gamma = 1$ and which does not put any restriction on (E_1, E_2) when $\gamma = 0$ since $g(E_1, E_2) \geq 0$ is always satisfied for $|E_x| \leq 1$.

Let us now assume $0 < \gamma < 1$. Obviously, we can restrict our analysis to the two-dimensional subspace spanned by ϕ_1 and ϕ_2. In that subspace, we can rewrite the states as qubit operators $\phi_x = (\mathbb{1} + \boldsymbol{n}_x \cdot \boldsymbol{\sigma})/2$, where $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli matrices and $\|\boldsymbol{n}_x\| = 1$. Then, a general measurement M in that subspace can be written as a convex combination $(p_0 - p_1)\mathbb{1} + p_2\, \boldsymbol{m} \cdot \boldsymbol{\sigma}$, where $p_i \geq 0$, $\sum_i p_i = 1$, $\|\boldsymbol{m}\| = 1$, and $\boldsymbol{m}$ can be taken in the span of $\{\boldsymbol{n}_1, \boldsymbol{n}_2\}$ without loss of generality. The resulting correlations correspond to the mixture

$$(E_1, E_2) = p_0(1, 1) + p_1(-1, -1) + p_2(\boldsymbol{n_1} \cdot \boldsymbol{m}, \boldsymbol{n_2} \cdot \boldsymbol{m}). \tag{18}$$

In other words, the region of allowed (E_1, E_2) is the convex hull of the points

$$\{(1, 1), (-1, -1), (\boldsymbol{n_1} \cdot \boldsymbol{m}, \boldsymbol{n_2} \cdot \boldsymbol{m})\} \tag{19}$$

Let us characterize further the points $(E_1, E_2) = (\boldsymbol{n_1} \cdot \boldsymbol{m}, \boldsymbol{n_2} \cdot \boldsymbol{m})$. Since $\boldsymbol{m}$ lies in the span of $\boldsymbol{n}_1$, $\boldsymbol{n}_2$ and since $(\boldsymbol{n}_1 + \boldsymbol{n}_2) \cdot (\boldsymbol{n}_1 - \boldsymbol{n}_2) = 0$, we can write without loss of generality

$$\boldsymbol{m} = \cos(\theta) \frac{\boldsymbol{n}_1 + \boldsymbol{n}_2}{\|\boldsymbol{n}_1 + \boldsymbol{n}_2\|} + \sin(\theta) \frac{\boldsymbol{n}_1 - \boldsymbol{n}_2}{\|\boldsymbol{n}_1 - \boldsymbol{n}_2\|}\,. \tag{20}$$

Using this formulation together with $\|\boldsymbol{n}_1 + \boldsymbol{n}_2\| = 2\gamma$ and $\|\boldsymbol{n}_1 - \boldsymbol{n}_2\| = 2\sqrt{1 - \gamma^2}$, we find

$$\frac{E_1 + E_2}{2\gamma} = \frac{\boldsymbol{n_1} + \boldsymbol{n_2}}{\|\boldsymbol{n}_1 + \boldsymbol{n}_2\|} \cdot \boldsymbol{m} = \cos(\theta)\,, \tag{21}$$

$$\frac{E_1 - E_2}{2\sqrt{1 - \gamma^2}} = \frac{\boldsymbol{n_1} - \boldsymbol{n_2}}{\|\boldsymbol{n}_1 - \boldsymbol{n}_2\|} \cdot \boldsymbol{m} = \sin(\theta)\,. \tag{22}$$

We thus find that the set of points $(E_1, E_2) = (\boldsymbol{n_1} \cdot \boldsymbol{m}, \boldsymbol{n_2} \cdot \boldsymbol{m})$ for a given γ corresponds to the ellipse

$$\left(\frac{E_+}{2\gamma}\right)^2 + \left(\frac{E_-}{2\sqrt{1 - \gamma^2}}\right)^2 = 1\,, \tag{23}$$

where we have defined $E_\pm = E_1 \pm E_2$. The region of allowed (E_1, E_2) for an arbitrary measurement M is therefore the convex hull of $(1, 1)$, $(-1, -1)$, and any points on this ellipse, as represented in Fig. 4.

We can represent this region in a compact way as the condition $g(E_1, E_2) \geq \gamma$. Indeed, first note that the ellipse (23) intersects the borders of $[-1, 1] \times [-1, 1]$ at the two points $(E_1, E_2) \in \{(2\gamma^2 - 1, 1), (-1, 1 - 2\gamma^2)\}$ in the region above the E_+-axis and at the two points $\{(1 - 2\gamma^2, -1), (1, 2\gamma^2 - 1)\}$ in the region below the E_+-axis, as represented in Fig. 4. These two pairs of points define two arcs of ellipses, as illustrated in Fig. 4. After some basic algebra (corresponding to writing (23) explicitly in terms of E_1, E_2), one finds that these two arcs of ellipses correspond to the values of (E_1, E_2) which solve $g(E_1, E_2) = \gamma$. It is not difficult to observe that any point in the convex hull of $(1, 1)$, $(-1, -1)$, and the ellipse (23) also belongs to the arcs of a second ellipse satisfying $g(E_1, E_2) = \tilde{\gamma} \geq \gamma$. Indeed, by increasing $\tilde{\gamma}$, the four intersection points defined above move towards the corners $(-1, -1)$ and $(1, 1)$, which they reach when $\tilde{\gamma} = 1$ and the ellipse becomes the line segment between the points $(1, 1)$ and $(-1, -1)$. Therefore, as $\tilde{\gamma}$ increases, the two corresponding arcs of ellipses stretch and move over the entire convex region for (E_1, E_2) defined above. We deduce that this convex region is given by the values of (E_1, E_2) satisfying $g(E_1, E_2) \geq \gamma$.

In summary, we have established that the set of correlations (E_1, E_2) that can be obtained by measuring two pure states with given scalar product $\gamma = |\langle \phi_1 | \phi_2 \rangle|$ is given by

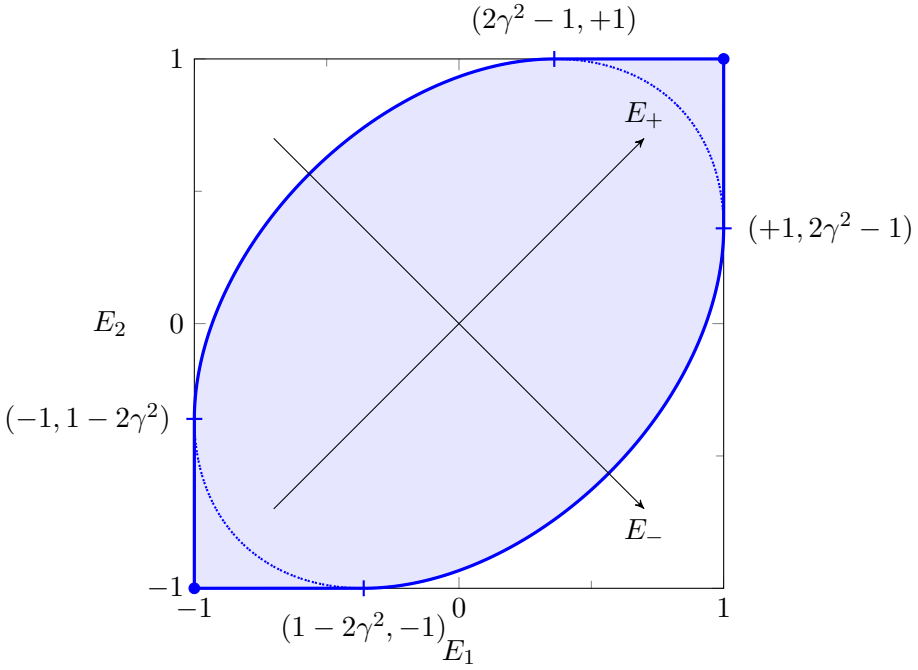


Figure 4: Representation of the ellipse (23) in the space (E_1, E_2), depicted here for $\gamma = 0.82$. The region of physically possible (E_1, E_2) corresponds to the convex hull of this ellipse with the two corner points $(1, 1)$ and $(-1, -1)$. The ellipse intersects the borders of the region $[-1, 1] \times [-1, 1]$ at the four depicted points. This defines two arcs of ellipses, corresponding to the portions of the ellipse represented in bold, and given by the solutions to $g(E_1, E_2) = \gamma$. The set of physically possible (E_1, E_2) then corresponds to the subset of $[-1, 1] \times [-1, 1]$ lying between these two arcs of ellipses. This corresponds to the region $g(E_1, E_2) \geq \gamma$.

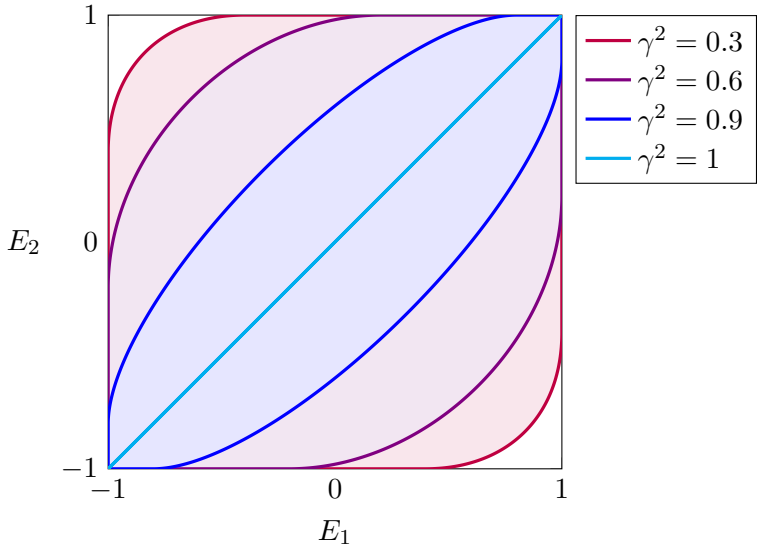


Figure 5: Region of possible values (E_1, E_2) satisfying $g(E_1, E_2) \geq \gamma$ for $\gamma = 0.55, 0.77, 0.95, 1$.

$g(E_1, E_2) \geq \gamma$, i.e., (16). The corresponding regions for different values of $|\langle\phi_1|\phi_2\rangle| = \gamma$ are represented in Fig. 5. Note that the regions strictly grow when the scalar product γ decreases, starting from the line segment $E_1 = E_2$ when $\gamma = 1$ (corresponding to two indistinguishable states), to the full square when $\gamma = 0$ (corresponding to two fully orthogonal states).

3.2 Lower bound on the scalar product $\left|\langle\phi_1|\phi_2\rangle\right|$ as a function of expectation values (H_1, H_2)

We have just seen that the region of possible correlations (E_1, E_2) attainable with pure states only depends on their scalar product through (16). We now show that the parameters (H_1, H_2) constrain the possible values of this scalar product through the lower bound $|\langle\phi_1|\phi_2\rangle| \geq h(H_1, H_2)$ where $h(H_1, H_2)$ is defined in (15). Intuitively if H_1 and H_2 are small, both states ϕ_1 and ϕ_2 are close to the non-degenerate ground state $|0\rangle$ of H and thus they should have a non-zero overlap. This is what (15) makes precise.

Let us first show that for any values of (H_1, H_2) it is indeed possible to find two states ϕ_1, ϕ_2 such that their scalar product satisfies $|\langle\phi_1|\phi_2\rangle| = h(H_1, H_2)$. This implies that any point (E_1, E_2) satisfying (13) can indeed be realized in our prepare-and-measure scenario.

For this, simply note that any H_1 and H_2 satisfying $H_1, H_2 \geq 0$ and $H_1 + H_2 \leq 1$ can be expressed as $H_x = \sin(\theta_x)^2$ for some suitable $\theta_x \in [0, \pi/2]$. Computing $h(H_1, H_2)$, we find $h(H_1, H_2) = \cos(\theta_1 + \theta_2)$. Define the two states

$$|\phi_1\rangle = \cos(\theta_1)|0\rangle + \sin(\theta_1)|1\rangle\,, \tag{24}$$

$$|\phi_2\rangle = \cos(\theta_2)|0\rangle - \sin(\theta_2)|1\rangle\,. \tag{25}$$

Then, their scalar product satisfies $|\langle\phi_1|\phi_2\rangle| = \cos(\theta_1 + \theta_2) = h(H_1, H_2)$, as required.

Let us now show that the scalar product between ϕ_1, ϕ_2 cannot be smaller than the value given by (15). This implies that no correlations outside the region defined by (13) can be obtained by measuring pure states in our scenario.

For this, let $\beta_x = 1 - \langle 0|\phi_x|0\rangle$ be the weight of the state ϕ_x in the subspace orthogonal to the groundstate $|0\rangle$ of H. We have that $\beta_x \leq H_x$ since $H_x = \mathrm{tr}[H\phi_x] = \sum_{i>0} \lambda_i \,\mathrm{tr}[P_i\phi_x] \geq \sum_{i>0} \mathrm{tr}[P_i\phi_x] = 1 - \mathrm{tr}[P_0\phi_x] = \beta_x$, where λ_i and P_i denote the eigenvalues of H and the corresponding projectors, with $\lambda_0 = 0$ and $\lambda_i \geq 1$ for $i > 0$. Writing

$$|\phi_x\rangle = \sqrt{1-\beta_x}|0\rangle + \sqrt{\beta_x}|\xi_x\rangle\,, \tag{26}$$

where $|\xi_x\rangle$ is in the subspace orthogonal to $|0\rangle$, we have that

$$\begin{aligned} |\langle\phi_1|\phi_2\rangle| &= |\sqrt{1-\beta_1}\sqrt{1-\beta_2} + \sqrt{\beta_1}\sqrt{\beta_2}\langle\xi_1|\xi_2\rangle| \\ &\geq |\sqrt{1-\beta_1}\sqrt{1-\beta_2} - \sqrt{\beta_1}\sqrt{\beta_2}| \\ &= \sqrt{1-\beta_1}\sqrt{1-\beta_2} - \sqrt{\beta_1}\sqrt{\beta_2} \\ &= h(\beta_1, \beta_2)\,, \end{aligned} \tag{27}$$

where in the second line we used that the right hand-side is minimized when $\langle\xi_1|\xi_2\rangle = -1$ and in the last line we used that $h(\beta_1, \beta_2)$ is positive when $\beta_1 + \beta_2 \leq 1$, which is the case since $H_1 + H_2 \leq 1$ and $\beta_x \leq H_x$. Now, given that the function $h(x, y)$ is non-decreasing in x and y in the region $x + y \leq 1$, we have that $h(\beta_1, \beta_2) \geq h(H_1, H_2)$, which gives (15).

4 General quantum correlations

4.1 Shared randomness

Let us now turn to the general case where S and M can exploit shared random parameters λ. This includes in particular the case where the source S can emit *mixed* states since any mixed state ρ_x can be viewed as a convex decomposition $\rho_x = \sum_\lambda p_\lambda \phi_x^\lambda$ of pure states. Let

$$\mathcal{Q}'_{H_1,H_2} = \left\{ \boldsymbol{E} = \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \mid \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda}, \sum_\lambda p_\lambda \boldsymbol{H}_\lambda = \boldsymbol{H} \right\}, \tag{28}$$

be the set of possible quantum correlations (E_1, E_2) compatible with given expectation values (H_1, H_2) in the presence of shared randomness, where we write $\boldsymbol{E} = (E_1, E_2)$ for the correlations averaged over the shared randomness λ, $\boldsymbol{E}_\lambda = (E_{1|\lambda}, E_{2|\lambda})$ for the correlations corresponding to a specific value of the shared randomness, and similarly for $\boldsymbol{H}$ and $\boldsymbol{H}_\lambda$. The set $\mathcal{Q}'$ (as in the previous section we drop the subindices H_1, H_2 to simplify the notation) thus corresponds to convex sums $\boldsymbol{E} = \sum_\lambda p_\lambda \boldsymbol{E}_\lambda$ of pure-state quantum realizations, each of which is characterized by expectation values $\boldsymbol{H}_\lambda$. The values $\boldsymbol{E}_\lambda$ must thus belong to $\mathcal{Q}_{\boldsymbol{H}_\lambda}$ and we require in addition that we recover on average the given expectations $\boldsymbol{H}$: $\sum_\lambda p_\lambda \boldsymbol{H}_\lambda = \boldsymbol{H}$.

We now show that

$$\mathcal{Q}'_{H_1,H_2} = \mathcal{Q}_{H_1,H_2}\,, \tag{29}$$

i.e., the set of pure-state correlations is closed under shared-randomness. Interestingly, the same property is also shared by pure-state quantum correlations in the context of Bell non-locality, but is not true in the context of semi-DI scenarios based on dimension bounds.

Since obviously $\mathcal{Q}' \supseteq \mathcal{Q}$, we need only prove that $\mathcal{Q}' \subseteq \mathcal{Q}$, i.e., that given any mixture $\boldsymbol{E} = \sum_\lambda p_\lambda \boldsymbol{E}_\lambda$ of pure-state correlations with average expectations $\boldsymbol{H} = \sum_\lambda p_\lambda \boldsymbol{H}_\lambda$, then the exact same correlations $\boldsymbol{E}$ can be obtained through a single pure-state quantum realization with expectation values $\boldsymbol{H}$. This simply amounts to showing that $g(\boldsymbol{E}) \geq h(\boldsymbol{H})$ since this condition fully characterizes the set of pure-state quantum correlations, or equivalently that $g(\boldsymbol{E})^2 - h(\boldsymbol{H})^2 \geq 0$ since the functions g and h are positive in the domain $H_1 + H_2 \leq 1$. We establish this by showing that g^2 and $-h^2$ are concave. Indeed, if this is the case we have

$$\begin{aligned} g(\boldsymbol{E})^2 - h(\boldsymbol{H})^2 &= g\big(\textstyle\sum_\lambda p_\lambda \boldsymbol{E}_\lambda\big)^2 - h\big(\sum_\lambda p_\lambda \boldsymbol{H}_\lambda\big)^2 \\ &\geq \sum_\lambda p_\lambda g(\boldsymbol{E}_\lambda)^2 - \sum_\lambda p_\lambda h(\boldsymbol{H}_\lambda)^2 \\ &= \sum_\lambda p_\lambda \big(g(\boldsymbol{E}_\lambda)^2 - h(\boldsymbol{H}_\lambda)^2\big) \\ &\geq 0 \end{aligned} \tag{30}$$

where we used the concavity of g^2 and $-h^2$ in the first inequality and the condition $g(\boldsymbol{E}_\lambda)^2 - h(\boldsymbol{H}_\lambda)^2 \geq 0$ for each λ in the second inequality, since by assumption $\boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda}$.

Note that both g^2 and $-h^2$ can be written in term of the function

$$f(x,y) = \left(\sqrt{xy} + \sqrt{(1-x)(1-y)}\right)^2 \tag{31}$$

as $g(E_1, E_2)^2 = f\big(\frac{1+E_1}{2}, \frac{1+E_2}{2}\big)$ and $-h(H_1, H_2)^2 = f(H_1, 1 - H_2) - 1$. Showing the concavity of g^2 and $-h^2$ thus reduces to showing that f is concave for $0 \leq x, y \leq 1$, i.e., that its Hessian matrix $\mathrm{Hess}(f)$ is negative semidefinite. A straightforward computation shows that $\mathrm{tr}\big[\mathrm{Hess}(f)\big] \leq 0$ and $\det\big[\mathrm{Hess}(f)\big] \geq 0$ for any $0 \leq x, y \leq 1$. Since $\mathrm{Hess}(f)$ is a 2×2 symmetric matrix, this implies, as desired, that both of its eigenvalues are nonpositive.

4.2 Upper bounds on the expectation values of H

The sets $\mathcal{Q}$ and $\mathcal{Q}'$ defined above assume that the source S emits states with given expectation values $\boldsymbol{H} = (H_1, H_2)$ for the observable H. However, as we pointed out in Section 2, rather than assuming that H takes some exact values, it is more natural to assume upper bounds on the possible values of H, and we introduced two possible ways to bound such values, either through the max-average assumption (3) or the max-peak assumption (4). This leads us to define the set of quantum correlations under the max-average assumption as

$$\overline{\mathcal{Q}}_{\omega_1,\omega_2} = \Big\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \mid \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda}, \sum_\lambda p_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \Big\} \tag{32}$$

and the set of quantum correlations under the max-peak assumption as

$$\widehat{\mathcal{Q}}_{\omega_1,\omega_2} = \Big\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \mid \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda}, \max_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \Big\}, \tag{33}$$

where we have written $\boldsymbol{\omega} = (\omega_1, \omega_2)$. Note that following the remark made at the end of Section 3, we always assume that $\omega_1 + \omega_2 \leq 1$, since any possible correlations (E_1, E_2) are already possible in the case $\omega_1 + \omega_2 = 1$.

From our previous results, the characterization of $\overline{\mathcal{Q}}_{\omega_1,\omega_2}$ and $\widehat{\mathcal{Q}}_{\omega_1,\omega_2}$ is immediate. First, it is easy to check that the sets $\mathcal{Q}_{H_1,H_2}$ of allowed values of (E_1, E_2) are strictly increasing with H_1, H_2. That is, $\mathcal{Q}_{H_1,H_2} \subseteq \mathcal{Q}_{H_1',H_2'}$ if $H_1 \leq H_1'$ and $H_2 \leq H_2'$. This follows from the fact that $h(H_1, H_2)$ is a non-increasing function of H_1 and H_2 in the range $H_1 + H_2 \leq 1$ and that the sets of values (E_1, E_2) defined by $g(E_1, E_2) \geq \gamma$ increase with decreasing γ, as illustrated in Fig. 5. It thus follows that in (32) one can always assume that $\sum_\lambda p_\lambda \boldsymbol{H}_\lambda = \boldsymbol{\omega}$ and in (33) that $\boldsymbol{H}_\lambda = \boldsymbol{\omega}$ for all values of λ. Using the results of the previous subsection on the behavior of $\mathcal{Q}$ under shared randomness, we deduce that

$$\overline{\mathcal{Q}}_{\omega_1,\omega_2} = \mathcal{Q}'_{\omega_1,\omega_2} = \mathcal{Q}_{\omega_1,\omega_2} = \widehat{\mathcal{Q}}_{\omega_1,\omega_2}\,. \tag{34}$$

We thus conclude that any correlations that can be generated by an arbitrary quantum realization constrained only by upper bounds ω_1 and ω_2 on H_1 and H_2, whether through the max-average or the max-peak assumption, always admit an equivalent pure-state quantum representation saturating these upper bounds. In this sense the max-average and max-peak assumptions are equivalent. As we will see in Sections 5 and 6, however, different quantum realizations of the same correlations may exhibit different underlying quantum properties, and the max-average and max-peak assumptions are different from this perspective.

5 Classical correlations

A basic property of fully- or semi-DI setups based on non-locality or dimension bounds is the existence of quantum correlations that have no classical analogue. This is clearly a prerequisite for any application of such correlations, e.g., for randomness certification. This property is also present in our semi-DI scenario as we now show.

5.1 Definition

We need first to define some notion of "classicality" in our context and a corresponding set of correlations. The no-communication assumption in standard Bell tests and the dimension bound in usual semi-DI protocols have a well-defined meaning in a classical context, without any reference to quantum theory. This is no longer the case for the

assumptions that we consider here, as they are expressed as constraints on the mean value of a quantum observable H and hence explicitly assume some underlying quantum model. It is nevertheless still possible to identify sets of correlations that are "classical" in the sense that they do not exhibit genuinely quantum features and thus are useless for semi-DI applications. The most straightforward way to do so is to proceed by analogy with standard Bell tests or usual semi-DI protocols, where classical correlations correspond mathematically to those that can be expressed, with the help of shared randomness, as convex combinations of *deterministic* correlations.

We thus define the set of classical correlations under the max-average assumption (3) as

$$\overline{\mathcal{C}}_{\omega_1,\omega_2} = \left\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \;\middle|\; \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda},\, \boldsymbol{E}_\lambda \in \{\pm 1\}\times\{\pm 1\},\, \sum_\lambda p_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \right\} \tag{35}$$

and under the max-peak assumption as

$$\widehat{\mathcal{C}}_{\omega_1,\omega_2} = \left\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \;\middle|\; \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda},\, \boldsymbol{E}_\lambda \in \{\pm 1\}\times\{\pm 1\},\, \max_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \right\}. \tag{36}$$

The constraint $\boldsymbol{E}_\lambda \in \{\pm 1\}\times\{\pm 1\}$ in these definitions implies that for any given value of the shared randomness λ, an output ± 1 for the measurement performed at M is completely pre-determined for each of the two states emitted by the source S. Thus no genuinely quantum behavior is exhibited by the two devices. Conversely, if some correlations $\boldsymbol{E}$ lie outside the set $\overline{\mathcal{C}}_{\omega_1,\omega_2}$, then necessarily the output of M cannot be predetermined for at least one of the states sent by S, a typically quantum feature.

We show that $\overline{\mathcal{C}}_{\omega_1,\omega_2}$ is a polytope, which apart from the trivial facets $|E_x| \leq 1$ is defined by

$$|E_-| = |E_1 - E_2| \leq 2(\omega_1 + \omega_2)\,. \tag{37}$$

Similarly, $\widehat{\mathcal{C}}_{\omega_1,\omega_2}$ is a polytope characterized by the stronger inequality

$$|E_-| = |E_1 - E_2| \leq 2\,\Theta(\omega_1 + \omega_2)\,, \tag{38}$$

where $\Theta(z) = 0$ if $z < 1$ and $\Theta(z) = 1$ if $z = 1$.

Let us first establish the characterization (37) of $\overline{\mathcal{C}}$. Remark that for any $(\boldsymbol{E}_\lambda, \boldsymbol{H}_\lambda) \in \mathcal{Q}$ for which $\boldsymbol{E}_\lambda \in \{\pm 1\}\times\{\pm 1\}$ there are two possibilities. Either $E_{1|\lambda} = E_{2|\lambda}$, in which case $|E_{1|\lambda} - E_{2|\lambda}| = 0$. Or $E_{1|\lambda} = -E_{2|\lambda}$, in which case the states emitted for $x = 1$ and $x = 2$ must be orthogonal pure states and thus $H_{1|\lambda} + H_{2|\lambda} \geq 1 = |E_{1|\lambda} - E_{2|\lambda}|/2$. By taking convex combination of these possibilities, we find

$$|E_1 - E_2| \leq \sum_\lambda p_\lambda |E_{1|\lambda} - E_{2|\lambda}| \leq \sum_\lambda p_\lambda 2(H_{1|\lambda} + H_{2|\lambda}) \leq 2(\omega_1 + \omega_2)\,. \tag{39}$$

Conversely, any correlations $\boldsymbol{E}$ satisfying the constraint (37) belong to $\overline{\mathcal{C}}$. To prove this, note that the polytope defined by (37) has the following six extreme points

$$(E_1, E_2) = \Big\{ (\pm 1, \pm 1),\, (\pm 1, \pm[1 - 2(\omega_1 + \omega_2)]),\, (\pm[1 - 2(\omega_1 + \omega_2)], \pm 1) \Big\}\,. \tag{40}$$

Proving that any $\boldsymbol{E}$ in this polytope belongs to $\overline{\mathcal{C}}$ amounts to showing, by convexity, that any of these six extreme points belongs to $\overline{\mathcal{C}}$. This is evident for the two points $(\pm 1, \pm 1)$. The point $(1, 1 - 2(\omega_1 + \omega_2))$ can be decomposed as $p_1\boldsymbol{E}_1 + p_2\boldsymbol{E}_2 + p_3\boldsymbol{E}_3$, where

$$p_1 = 1 - \omega_1 - \omega_2\,, \qquad \boldsymbol{E}_1 = (1, 1) \in \mathcal{Q}_{0,0}\,, \tag{41}$$

$$p_2 = \omega_1\,, \qquad \boldsymbol{E}_2 = (1, -1) \in \mathcal{Q}_{1,0}\,, \tag{42}$$

$$p_3 = \omega_2\,, \qquad \boldsymbol{E}_3 = (1, -1) \in \mathcal{Q}_{0,1}\,, \tag{43}$$

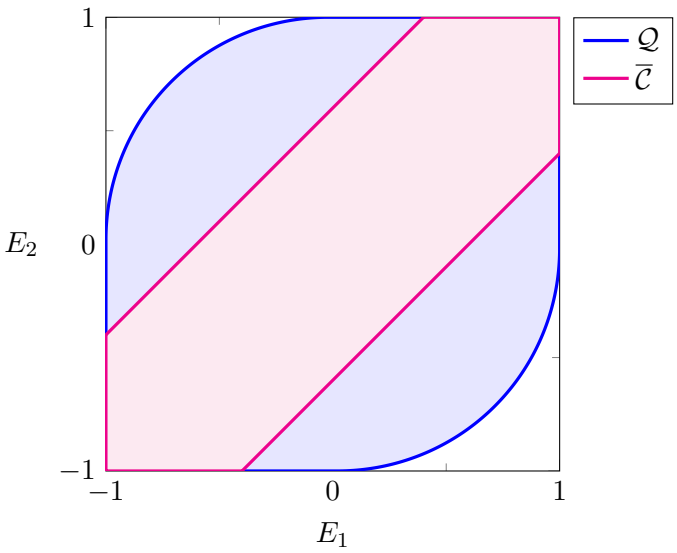


Figure 6: Comparison of the quantum set $\mathcal{Q}$ and the classical set $\overline{\mathcal{C}}$ for $\omega_1 = \omega_2 = 0.15$, showing that it is possible to violate the classical bound (37) with quantum systems. The E_--axis ($E_- = E_1 - E_2$) measures how quantum the behavior of the boxes is, in a way similar to the CHSH witness in the study of non-locality. For the particular case $\omega_1 = \omega_2 = 0.15$, classical systems are limited to $|E_-| \leq 0.6$ but the maximal value for quantum systems is $|E_-| \simeq 1.43$.

and thus also belongs to $\overline{\mathcal{C}}$. Similar decompositions are readily obtained for the three other points.

The characterization (38) of $\widehat{\mathcal{C}}$ follows from two simple observations. If $\omega_1 + \omega_2 < 1$, the only points $\boldsymbol{E}_\lambda \in \mathcal{Q}$ such that $\boldsymbol{E}_\lambda \in \{\pm 1\} \times \{\pm 1\}$ are $(1, 1)$ and $(-1, -1)$. Their convex combination defines the line segment $E_1 - E_2 = 0$. If $\omega_1 + \omega_2 = 1$, the four corner points $\{\pm 1\} \times \{\pm 1\}$ are available, and as usual we have no constraints on $\boldsymbol{E}$, so that $|E_1 - E_2|$ can reach the maximal value 2.

5.2 Bell inequality analogues

The inequalities (37) and (38) play the same role as the inequality $|\mathrm{CHSH}| \leq 2$ in the context of Bell non-locality, in that they separate the quantum region from the region of convex combinations of deterministic correlations, see illustration of the sets $\overline{\mathcal{C}}$ and $\mathcal{Q}$ in Fig. 6. The analogue of the Tsirelson inequality $|\mathrm{CHSH}| \leq 2\sqrt{2}$ is the inequality $|E_-| = |E_1 - E_2| \leq 2(\sqrt{H_1}\sqrt{1 - H_2} + \sqrt{1 - H_1}\sqrt{H_2})$. This quantum bound is readily obtained from the results of the previous sections (the points maximizing $|E_1 - E_2|$ in $\mathcal{Q}$ correspond to the points on the E_--axis of the ellipse (23)).

The axis E_- thus corresponds to the axis along which "quantumness" increases. Note that we can interpret $|E_-|$ as a measure of how well it is possible to guess which input $x = 1$ or $x = 2$ was used given the measurement outcome b. Indeed, since

$$\tfrac{1}{2}|E_-| = \tfrac{1}{2}|E_1 - E_2| = \tfrac{1}{2} \sum_{b=\pm 1} \left| P(b|x=1) - P(b|x=2) \right|, \tag{44}$$

the quantity $\frac{1}{2}|E_-|$ is equal to the statistical distance

$$d(P_{B|x=1}, P_{B|x=2}) \equiv \tfrac{1}{2} \sum_{b=\pm 1} \left| P(b|x=1) - P(b|x=2) \right| \tag{45}$$

between the output probability distributions $P_{B|x=1}$ and $P_{B|x=2}$ for the two possible inputs. In particular, the optimal probability to guess the input is $p_{\mathrm{g}} = \frac{1}{2}(1 + \frac{1}{2}|E_-|)$. For given H_1,

H_2, this probability is maximal when $|E_-|$ achieves its maximal value $2(\sqrt{H_1}\sqrt{1-H_2} + \sqrt{1-H_1}\sqrt{H_2})$, in which case we know for sure that the two states sent by S are as distinguishable as possible given the constraints on H_1 and H_2, and that M implements the measurement that best distinguishes them. When $\sqrt{H_1}\sqrt{1-H_2} + \sqrt{1-H_1}\sqrt{H_2} < 1$ (which necessarily happens when $H_1 + H_2 < 1$), it follows that it is not possible to deterministically guess which of the two choices $x = 1$ or $x = 2$ were made on S, which proves that the quantum channel relating S to M has sub-unit capacity, as previously anticipated.

5.3 Implementations discussion

The three experimental implementations that we have presented in Subsection 2.3 generate non-classical correlations as illustrated in Fig. 9. Note that the BPSK and 2ASK schemes do not admit a fully deterministic explanation under the max-average assumption, i.e., even if the source S is allowed to send states with arbitrary values for H, provided that the average values do not exceed the assumed thresholds. This is not true for the OOK implementation, which admits a deterministic explanation in this case. However, such a deterministic explanation is no longer possible if the peak values for H are constrained.

Note that for $\omega_1 + \omega_2 < 1$, the set $\widehat{\mathcal{C}}$ is of measure 0. We can get some intuition for the meaning of this set as follows. If $\omega_1 + \omega_2 < 1$, then for given λ every pair of states ϕ_1^λ, ϕ_2^λ emitted by the source must be non-orthogonal, as follows from the results of Subsection 3.2 and the max-peak assumption. Since there is no non-trivial measurement that will yield with certainty definite outcomes for two non-orthogonal states, the measurement device M, if it behaves deterministically, must actually ignore the quantum messages sent by M and simply output a pre-registered outcome $b = -1$ or $b = 1$, independently of whether $x = 1$ or $x = 2$. We thus necessarily have $E_1 = E_2$ in this case. Conversely, if we observe correlations for which $|E_1 - E_2| > 0$, we can conclude that the measurement device M did not simply output pre-registered values, but actually performed a non-trivial measurement on the states emitted by S, which are non-orthogonal. That is, the observation of $|E_1 - E_2| > 0$ witnesses a typical quantum feature, which in particular necessarily results in a non-deterministic outcome for at least one of $x = 1, 2$. A similar conclusion can be reached under the max-average assumption, but this now requires $|E_1 - E_2|$ to be above a finite value $2(\omega_1 + \omega_2)$, as follows from (37).

6 Correlations exhibiting certified randomness

If S and M generate correlations in the classical sets $\overline{\mathcal{C}}$ or $\widehat{\mathcal{C}}$, then the output b is predetermined simultaneously for *both* choices of inputs $x = 1, 2$, and the apparent randomness of b only arises from the pre-established classical randomness λ. Observing a point outside the sets $\overline{\mathcal{C}}$ or $\widehat{\mathcal{C}}$ thus guarantees that at least one of the inputs, $x = 1$ or $x = 2$ leads to genuinely random outcomes, but does not guarantee that a specific one, say $x = 1$ does, or that both $x = 1$ and $x = 2$ do. For instance, as can be seen in Fig. 6, the point $(E_1, E_2) = (1, 2h^2(\omega_1, \omega_2) - 1)$ does not belong to $\overline{\mathcal{C}}$ but nevertheless corresponds to a situation where M returns $b = 1$ with certainty when $x = 1$ is used. A similar situation arises in the context of Bell non-locality, in which correlations can be non-local and yet have definite values for a subset of the measurement inputs [27].

In cryptographic applications, and for instance in DI or semi-DI RNG protocols, it is usually the case that the certified randomness comes from a fixed subset of the inputs. For instance, in our context, a semi-DI RNG protocol along the lines of [28–30] would most of the time use the input $x = 1$ to generate the random string and from time to

time both $x = 1$ and $x = 2$ to estimate the correlations $\boldsymbol{E}$ produced by the devices. Given the estimated $\boldsymbol{E}$, it is then possible to lower bound the amount of randomness extractable from the $x = 1$ measurement data.

This leads us to consider sets based on a weaker constraint than those introduced in the previous section, those for which the output of M is deterministic when a specified input x is chosen, while potentially random for the remaining inputs:

$$\overline{\mathcal{D}}_{x,\omega_1,\omega_2} = \left\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \;\middle|\; \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda},\, E_{x|\lambda} \in \{\pm 1\},\, \sum_\lambda p_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \right\}, \tag{46}$$

$$\widehat{\mathcal{D}}_{x,\omega_1,\omega_2} = \left\{ \sum_\lambda p_\lambda \boldsymbol{E}_\lambda \;\middle|\; \boldsymbol{E}_\lambda \in \mathcal{Q}_{\boldsymbol{H}_\lambda},\, E_{x|\lambda} \in \{\pm 1\},\, \max_\lambda \boldsymbol{H}_\lambda \leq \boldsymbol{\omega} \right\}. \tag{47}$$

The sets $\overline{\mathcal{D}}_1$, $\overline{\mathcal{D}}_2$ clearly contain $\overline{\mathcal{C}}$ but can be larger, and similarly for $\widehat{\mathcal{D}}_1$, $\widehat{\mathcal{D}}_2$ with respect to $\widehat{\mathcal{C}}$, see Fig. 7. Observing a point outside $\overline{\mathcal{D}}_x$ or $\widehat{\mathcal{D}}_x$ now certifies that the output of M is (at least to some extent) random when the input x is chosen. Furthermore, observing a point outside the convex hull of $\overline{\mathcal{D}}_1 \cup \overline{\mathcal{D}}_2$ or $\widehat{\mathcal{D}}_1 \cup \widehat{\mathcal{D}}_2$ guarantees that the output of M is random, independently of which input $x = 1$ or $x = 2$ was used.

The sets $\overline{\mathcal{D}}_x$ and $\widehat{\mathcal{D}}_x$ have a direct significance in the context of semi-DI random number generation (RNG) protocols. The existence of quantum correlations outside, say, $\overline{\mathcal{D}}_1$ or $\widehat{\mathcal{D}}_1$ is sufficient to guarantee the existence of a semi-DI RNG protocol along the lines of [28–30], in which the input $x = 1$ is used to generate the random string and both $x = 1$ and $x = 2$ are used on a smaller subsets of the runs to estimate the correlations $\boldsymbol{E}$. As long as the estimated $\boldsymbol{E}$ is outside $\overline{\mathcal{D}}_1$ or $\widehat{\mathcal{D}}_1$ (modulo statistical corrections), one will be able to certify that a certain amount of randomness has been produced (how to quantify precisely this randomness will be presented in [25]).

6.1 Characterization of the set $\overline{\mathcal{D}}_x$

We show here that $\overline{\mathcal{D}}_x$ consists of the values $\boldsymbol{E}$ satisfying $|E_x| \leq 1$ and

$$E_x\, h^2\!\left(\frac{2\omega_1}{1+E_x}, \frac{2\omega_2}{1+E_x}\right) - E_{\bar{x}} \leq 1 - h^2\!\left(\frac{2\omega_1}{E_x+1}, \frac{2\omega_2}{E_x+1}\right), \tag{48a}$$

$$E_x\, h^2\!\left(\frac{2\omega_1}{1-E_x}, \frac{2\omega_2}{1-E_x}\right) - E_{\bar{x}} \geq -1 + h^2\!\left(\frac{2\omega_1}{1-E_x}, \frac{2\omega_2}{1-E_x}\right), \tag{48b}$$

where $\bar{x}$ denotes the input complementary to x ($\bar{x} = 2$ if $x = 1$ and $\bar{x} = 1$ if $x = 2$).

Let us consider the case $x = 1$ to simplify the notation (the derivation is the same for $x = 2$). Let $\boldsymbol{E} = \sum_\lambda p_\lambda \boldsymbol{E}_\lambda$ be an arbitrary point in $\overline{\mathcal{D}}_1$. Define $\Lambda_\pm$ as the set of λ's for which $E_{1|\lambda} = \pm 1$ and write

$$\boldsymbol{E} = p\boldsymbol{E}_+ + (1-p)\boldsymbol{E}_-\,, \tag{49}$$

$$\boldsymbol{\omega} \geq p\boldsymbol{H}_+ + (1-p)\boldsymbol{H}_-\,, \tag{50}$$

where

$$p = p_+ = \sum_{\lambda\in\Lambda_+} p_\lambda\,, \qquad 1-p = p_- = \sum_{\lambda\in\Lambda_-} p_\lambda \tag{51}$$

and

$$\boldsymbol{E}_\pm = \frac{1}{p_\pm} \sum_{\lambda\in\Lambda_\pm} p_\lambda \boldsymbol{E}_\lambda\,, \qquad \boldsymbol{H}_\pm = \frac{1}{p_\pm} \sum_{\lambda\in\Lambda_\pm} p_\lambda \boldsymbol{H}_\lambda\,. \tag{52}$$

We have thus regrouped the components $(\boldsymbol{E}_\lambda, \boldsymbol{H}_\lambda)$ in two subsets $(\boldsymbol{E}_\pm, \boldsymbol{H}_\pm)$, for which $E_{1|+} = +1$ and $E_{1|-} = -1$, respectively. Since $\mathcal{Q}$ is convex, the two points $(\boldsymbol{E}_\pm, \boldsymbol{H}_\pm)$ belong to $\mathcal{Q}$ and satisfy the constraints obtained in Section 3.

In particular, since $E_{1|+} = 1$, it follows that $E_{2|+} \geq 2h^2(H_{1|+}, H_{2|+}) - 1$ and thus that

$$E_2 \geq p(2h^2(H_{1|+}, H_{2|+}) - 1) - (1-p) = p\, 2h^2(H_{1|+}, H_{2|+}) - 1\,. \tag{53}$$

On the other hand,

$$H_{1|+} \leq \frac{\omega_1 - (1-p)H_{1|-}}{p} \leq \frac{\omega_1}{p}\,, \tag{54}$$

and similarly $H_{2|+} \leq \omega_2/p$. It is easily established that the function $h(x,y)$ is non increasing in its two arguments and thus that

$$E_2 \geq p\, 2h^2\left(\frac{\omega_1}{p}, \frac{\omega_2}{p}\right) - 1\,. \tag{55}$$

We can now use that $p = (1+E_1)/2$ and substitute in the inequality above, which gives (48a). Following the same lines to lower bound E_2, one obtains (48b). Finally, it is not difficult to verify that all the intermediate inequalities in our derivation are tight and thus that any $\boldsymbol{E}$ in the region defined by (48) can be attained by points in $\mathcal{D}_1$.

The sets $\overline{\mathcal{D}}_x$ are compared in Fig. 7 to $\overline{\mathcal{C}}$ and $\mathcal{Q}$.

6.2 Characterization of the set $\widehat{\mathcal{D}}_x$

The set $\widehat{\mathcal{D}}_x$ consists of the values $\boldsymbol{E}$ satisfying $|E_x| \leq 1$ and

$$\left|E_x\, h^2(\omega_1, \omega_2) - E_{\bar{x}}\right| \leq 1 - h^2(\omega_1, \omega_2)\,. \tag{56}$$

In order to establish the formula (56), note that, if $E_{x|\lambda} = 1$ and $H_{x|\lambda} \leq \omega_x$, then necessarily $1 \geq E_{\bar{x},\lambda} \geq 2h^2(\omega_1,\omega_2) - 1$, while if $E_{x,\lambda} = -1$, it holds that $-1 \leq E_{\bar{x},\lambda} \leq 1 - 2h^2(\omega_1,\omega_2)$. The convex hull of these points is readily seen to be completely characterized by (56) (together with the trivial inequalities $|E_x| \leq 1$).

The sets $\overline{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_1$ are compared in Fig. 8. Note that when $\omega_1 = 0$ or $\omega_2 = 0$, $\overline{\mathcal{D}}_1 = \overline{\mathcal{D}}_2 = \overline{\mathcal{C}}$.

6.3 Implementation examples

The three experimental implementations that we presented in Subsection 2.3 can be used to certify the production of genuine randomness, as illustrated in Fig. 9. The BPSK and 2ASK implementations can generate certified randomness under the max-average assumption, while the OOK implementation requires the max-peak assumption.

Note that the BPSK correlations (6) satisfy $E_+ = E_1 + E_2 = 0$ and thus only the values of $|E_-|$ are important to determine whether they are outside of $\overline{\mathcal{D}}_1$ or $\widehat{\mathcal{D}}_1$. Fig. 10 compares the BPSK value of $|E_-|$ to the intersections of the sets $\overline{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_1$ with the E_--axis as a function of the parameter ξ.

Finally, it is clear from Fig. 9 that the certification of randomness is robust to noise in the three implementations, i.e., to correlations that deviate from the ideal ones. Let us consider as an example the OOK implementation in the case where the source emits a coherent state $|\xi\rangle$ and the photodetector has a limited efficiency $\eta < 1$. The correlations (10) then change to

$$E_1 = 1 - 2e^{-|\xi|^2\eta} \simeq -1 + 2|\xi|^2\eta\,, \qquad\qquad E_2 = -1\,. \tag{57}$$

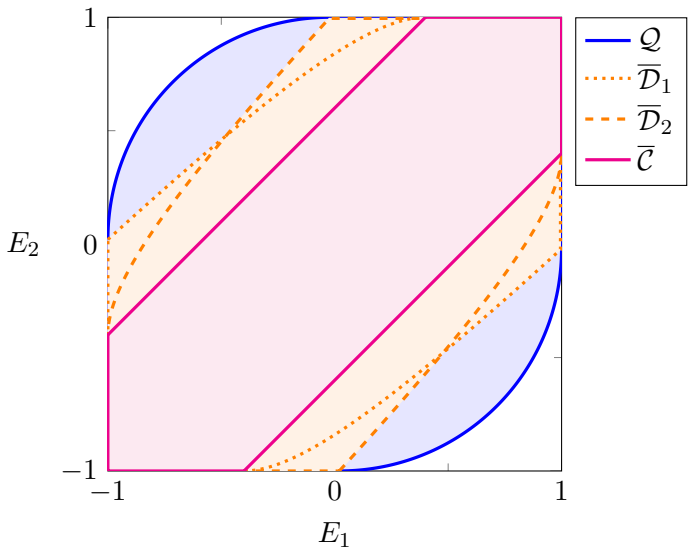


Figure 7: Representations of the sets $\overline{\mathcal{C}}$, $\overline{\mathcal{D}}_1$, $\overline{\mathcal{D}}_2$, and $\mathcal{Q}$ for $\omega_1 = \omega_2 = 0.15$. Since the quantum region is strictly larger than the individual sets $\overline{\mathcal{D}}_x$ (or even than their convex combination), it is possible to certify the production of genuine randomness.

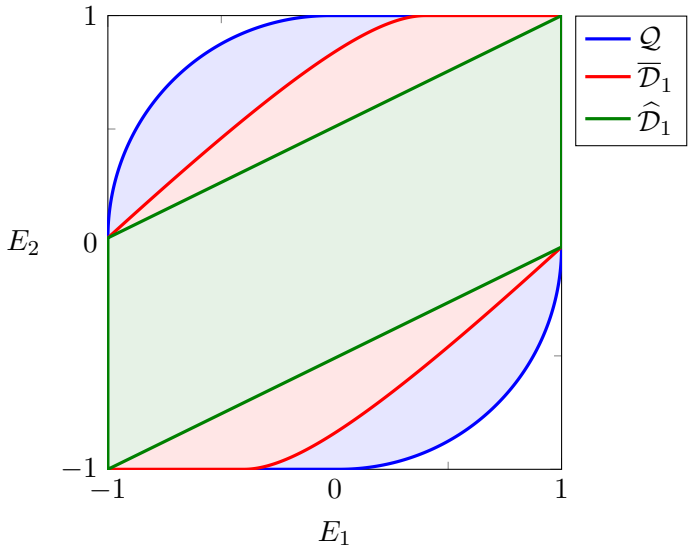


Figure 8: Comparison of the sets $\overline{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_1$, corresponding respectively to the *max-average* and *max-peak* assumptions, for $\omega_1 = \omega_2 = 0.15$, illustrating that the latter of the two assumptions puts a stronger constraint on the behavior of the devices. The quantum set $\mathcal{Q}$ is also represented for comparison.

The inequality (56) characterizing the region $\widehat{\mathcal{D}}_1$ is violated if $h^2(\omega_1,\omega_2)E_1 - E_2 > 1 - h^2(\omega_1,\omega_2)$. Inserting the above values for E_1 and E_2 and the threshold values (11) characterizing the source (which give $h(\omega_1,\omega_2) = e^{-|\xi|^2/2}$), we find the condition

$$(1 - 2e^{-|\xi|^2\eta})e^{-|\xi|^2} + 1 > 1 - e^{-|\xi|^2}\,, \tag{58}$$

which is satisfied provided that $e^{-|\xi|^2\eta} < 1$, i.e., that $\eta > 0$. In other words, the OOK implementation can generate certified randomness with arbitrarily low detection efficiency in the absence of other imperfections. The situation corresponding to $\eta = 25\%$ is represented in Fig. 9(c) and Fig. 9(d). Since in addition to this tolerance to detector inefficiency the OOK implementation is also very simple to implement experimentally, we will present in a forthcoming publication [25] a full theoretical analysis of a semi-DI RNG protocol based on this scheme.

7 Conclusion

In this paper, we introduced a new setting for semi-device-independent (semi-DI) quantum information. Contrarily to the usual approach, we do not assume bounds on the Hilbert space dimension of the carriers of quantum information, but instead on the mean values of one (or several) physical observable(s). Ideally, the choice of such an observable should be dictated by the physics of the source of quantum information carriers and rely as much as possible on a high-level characterization of its internal behavior. In quantum optics implementations, a natural choice is to upper bound the expected number of photons of the states emitted by the source or, alternatively, the energy contained in a range of frequency modes describing the system. We have completely characterized analytically the set of possible correlations in the simplest possible prepare-and-measure scenario compatible with such an assumption. We have in particular identified analogues of Bell inequalities, which are able to distinguish genuinely quantum devices from those behaving in a purely classically pre-determined fashion.

We note that semi-DI prepare-and-measure scenarios that do not rely on a Hilbert space dimension bound have also been introduced in [31]. However, they rely on a bound on the average von Neumann entropy of the emitted states, a quantity which as defined in [31] requires a greater level of characterization of the source and also depends on the probability distribution $p(x)$ used to select the preparation x.

Our approach has several interests. First of all, as with semi-DI approaches based on dimension bounds, it is of the prepare-and-measure type, and thus does not require the manipulation of entanglement. But, as with full DI approaches based on non-locality, it relies on assumptions that are physically motivated. It thus combines the practical advantages of these two different approaches.

Quite nicely, such an advantage from the implementation point of view does not come at the expense of theoretical simplicity. On the contrary, the minimal requirements on the number of inputs and outputs in our setting ($x \in \{1,2\}$, $y \in \{1\}$, $b \in \{\pm 1\}$) are smaller than those required for non-locality or dimension-bound protocols. Furthermore, in this minimal scenario, our assumptions are not only more natural than dimension bounds, but also more restrictive since they force the emitted states to have a sub-unit communication capacity.

A further point to notice is that the no-communication assumption in the non-locality scenario and the dimension-bound assumption are "yes or no" criteria (though it is also possible to introduce more refined assumptions in such contexts [14, 32]). Our assumptions are instead formulated in term of parameters that can take a continuous range of possible values, e.g., as thresholds on the average photon number. As such, they naturally allow

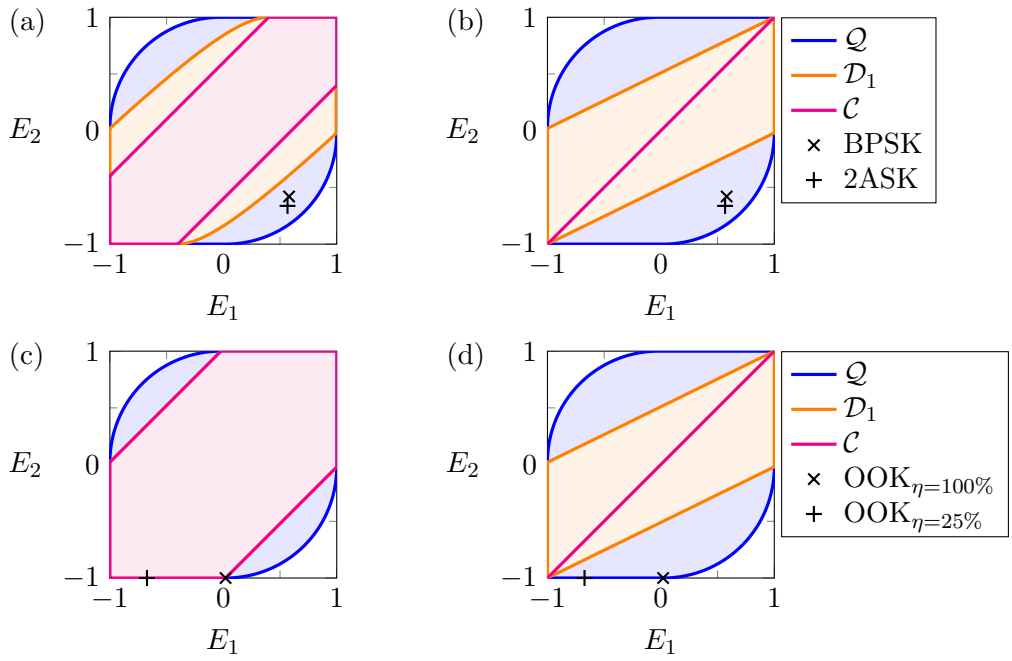


Figure 9: The sets $\mathcal{Q}$, $\mathcal{C}$, and $\mathcal{D}_1$ are displayed and compared to the correlations produced with the three implementations. The BPSK and the 2ASK protocols are analyzed with the constraints $\omega_1 = \omega_2 = 0.15$ under (a) the average-peak assumption and (b) the max-peak assumption. The OOK protocol is analyzed for two different detector efficiencies ($\eta = 100\%$ and $\eta = 25\%$) with the constraints $\omega_1 = 0.51$ and $\omega_2 = 0$ under (c) the average-peak assumption and (d) the max-peak assumption. Note that when $\omega_2 = 0$, the sets $\overline{\mathcal{C}}$ and $\overline{\mathcal{D}}_1$ coincide under the max-average assumption.

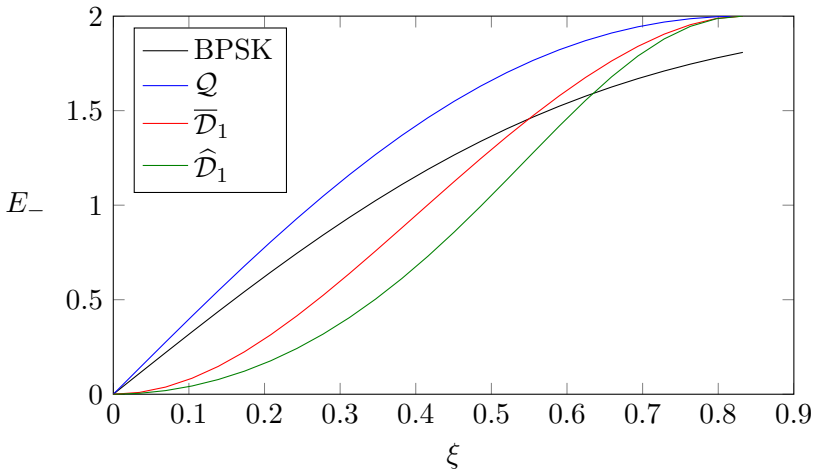


Figure 10: The correlations produced with the BPSK implementation are compared to the sets $\overline{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_1$. As these correlations lie on the E_--axis (they satisfy $E_1 + E_2 = 0$), it is only necessary to compare the value of E_- for the BPSK implementation to the intersections of the boundaries of the sets $\overline{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_1$ with the E_1-axis. This is done for different values of the parameter ξ, which determines corresponding values for ω_1 and ω_2 through (7). The range $0 \leq \xi \leq \sqrt{\ln 2} \approx 0.83$ was chosen such that $0 \leq \omega_1, \omega_2 \leq 0.5$. This figure shows that, with the BPSK implementation, it is possible to generate correlations that produce certifiable randomness for $\xi \lesssim 0.55$ under the max-average assumption and for $\xi \lesssim 0.63$ under the max-peak assumption.

for the introduction of additional "margins of security" making protocols based on them more robust to device imperfections. For instance, in an implementation using a source designed to prepare states with certain average photon numbers, one could performing the analysis assuming thresholds $\boldsymbol{\omega}$ corresponding to higher average photon numbers in order to allow for an additional margin for safety.

There are many potential applications of our results. First of all, note that one could reverse their interpretation. We have characterized the possible correlations $\boldsymbol{E}$ generated in a prepare-and-measure setting given upper bounds on the expectation values $\boldsymbol{H}$ of a physical observable H. But one can equally well understand these results as providing lower bounds for $\boldsymbol{H}$ given that some correlations $\boldsymbol{E}$ are observed. That is, in analogy to the concept of DI "dimension witnesses" [9, 10], our results imply the existence, e.g., of DI "photon-number witnesses". It is also reasonable to expect that our results could be exploited to perform self-testing of quantum properties, namely one could probably infer that the states and measurements have a specific form if certain correlations $\boldsymbol{E}$ are observed under our assumptions.

Our main motivation at the origin of the present paper, however, is the possibility to introduce new, physically motivated semi-DI random number generation and quantum key distribution protocols. We have seen in Section 2.3 that very simple implementations of our prepare-and-measure scenario can lead to correlations that do not admit any deterministic explanation. It is in fact possible to use the characterization of the quantum set that we have obtained here to compute precise lower bounds on the randomness that is produced by such implementations as a function of the correlations $\boldsymbol{E}$ they generate. Such lower bounds can directly be combined with the analysis of [28–30] and then lead to explicit protocols for semi-DI random number generation protocols. We will present in detail how to compute such lower bounds on the randomness and analyze the resulting semi-DI RNG protocols under realistic experimental condition in a forthcoming publication [25], with a special focus on the OOK implementation.

Note added The use of the On-Off Keying protocol of Fig. 3(c) in the context of semi-DI randomness generation has also been discussed by the authors of [33], although it was analyzed under different technical and security assumptions.

Acknowledgments

This work is supported by the Fondation Wiener-Anspach, the Interuniversity Attraction Poles program of the Belgian Science Policy Office under the grant IAP P7-35 photonics@be, the Spanish MINECO (Severo Ochoa grant SEV-2015-0522 and QIBEQI FIS2016-80773-P), the Generalitat de Catalunya (SGR 875 and CERCA Program), the Fundació Privada Cellex, the AXA Chair in Quantum Information Science, and the EU project QIT-BOX, S.P. and R.G.-P. are Research Associates of the Fonds de la Recherche Scientifique (F.R.S.-FNRS). N.J.C. acknowledges financial support from the Fonds de la Recherche Scientifique (F.R.S.-FNRS) under grant T.0199.13.

References

[1] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, 1998) pp. 503–509, arXiv:quant-ph/9809039.

[2] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005), arXiv:quant-ph/0405101.

[3] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis, University of Cambridge (2006), arXiv:0911.3814 [quant-ph]; R. Colbeck and A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011), arXiv:1011.4474 [quant-ph].
[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007), arXiv:quant-ph/0702152.
[5] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013), arXiv:1209.0448 [quant-ph].
[6] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, NY, USA, 2014) pp. 417–426, arXiv:1402.0489 [quant-ph].
[7] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs", (2016), arXiv:1607.01797 [quant-ph].
[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014), arXiv:1303.2849 [quant-ph].
[9] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008), arXiv:0802.0760 [quant-ph].
[10] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010), arXiv:1010.5064 [quant-ph].
[11] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 140407 (2014), arXiv:1311.1525 [quant-ph].
[12] 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), arXiv:1410.2790 [quant-ph].
[13] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011), arXiv:1103.4105 [quant-ph].
[14] E. Woodhead and S. Pironio, Phys. Rev. Lett. **115**, 150501 (2015), arXiv:1507.02889 [quant-ph].
[15] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nature Phys. **8**, 592 (2012), arXiv:1111.1277 [quant-ph].
[16] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Nature Phys. **8**, 588 (2012), arXiv:1111.1208 [quant-ph].
[17] B. S. Tsirel'son, J. Sov. Math. **36**, 557 (1987).
[18] R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001), arXiv:quant-ph/0102024.
[19] L. Masanes, "Necessary and sufficient condition for quantum-generated correlations", (2003), arXiv:quant-ph/0309137.
[20] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, in *Proc. Annu. IEEE Conf. Comput. Complex.* (IEEE, 2004) pp. 236–249, arXiv:quant-ph/0404076.
[21] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007), arXiv:quant-ph/0607119; M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008), arXiv:0803.4290 [quant-ph].
[22] A. C. Doherty, B. Toner, Y. C. Liang, and S. Wehner, in *Proc. Annu. IEEE Conf. Comput. Complex.* (IEEE, 2008) pp. 199–210, arXiv:0803.4373 [quant-ph].
[23] N. Brunner, M. Navascués, and T. Vértesi, Phys. Rev. Lett. **110**, 150501 (2013), arXiv:1209.5643 [quant-ph].
[24] M. Navascues and T. Vertési, Phys. Rev. Lett. **115**, 020501 (2015), arXiv:1412.0924 [quant-ph].
[25] T. Van Himbeeck *et al.*, in preparation.
[26] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015), arXiv:1503.00662 [quant-ph].

[27] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006), arXiv:quant-ph/0605182.
[28] S. Pironio, A. Acín, S. Massar, A. Boyer de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010), arXiv:0911.3427 [quant-ph].
[29] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013), arXiv:1111.6056 [quant-ph].
[30] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio, "Device-independent randomness generation from several Bell estimators", (2016), arXiv:1611.00352 [quant-ph].
[31] R. Chaves, J. B. Brask, and N. Brunner, Phys. Rev. Lett. **115**, 110501 (2015), arXiv:1505.07802 [quant-ph].
[32] J. Silman, S. Pironio, and S. Massar, Phys. Rev. Lett. **110**, 100504 (2013), arXiv:1211.5921 [quant-ph].
[33] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. A **7**, 054018 (2017), arXiv:1612.06566 [quant-ph].