Genuine Randomness \textit{vis-a-vis} Nonlocality: Hardy and Hardy type Relations

Souradeep Sasmal, Sayan Gangopadhyay, Ashutosh Rai, Dipankar Home, and Urbasi Sinha

1 Centre for Astroparticle Physics and Space Science (CAPSS), Bose Institute, Block EN, Sector V, Salt Lake, Kolkata 700 091, India
2 Raman Research Institute, Sadashivanagar, Bangalore, India
3 Department of Physics, Indian Institute of Science, C.V. Raman Avenue, Bangalore 560012, India
4 Institute for Quantum Computing, Department of Physics and Astronomy, University of Waterloo, Canada N2L3G1
5 Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia

Here we focus on comprehensively analysing the quantitative relationship between randomness and nonlocality based on the Hardy and Cabello-Liang relations. It is demonstrated that in the 2-2-2 (2 parties - 2 measurements per party - 2 outcomes per measurement) scenario, using the Cabello-Liang relations, one can achieve close to the theoretical maximum value of 2 bits of Genuine Randomness. Importantly, this maximum value is obtained using a range of pure non-maximally entangled states entailing small amounts of nonlocality. Thus, the quantitative incommensurability between the maximum achievable certified randomness, nonlocality and entanglement is revealed in the same testable context characterised by a given state and the measurement settings. This goes beyond the earlier Bell-CHSH inequality based findings about the relationship between randomness, nonlocality and entanglement in the same 2-2-2 scenario. On the other hand, we find that the device-independent guaranteed amount of Genuine Randomness is monotonically related to the Hardy/Cabello-Liang nonlocality, similar to that in the Bell-CHSH case. Therefore, the results of this combined study of the maximum achievable as well as the guaranteed amounts of Genuine Randomness, bring out that the nature of the quantitative relationship between randomness and nonlocality is crucially dependent on which aspect (the guaranteed/maximum amount) of Genuine Randomness is considered.

I. Introduction

Randomness is a fundamental feature of nature, and a key resource for myriad applications in diverse areas of sciences ranging from communication, cryptography to statistical sampling and varied types of algorithmic studies. For such applications, certifying and quantifying reliable randomness is a crucial issue, which requires true unpredictability to be guaranteed even in the presence of uncontrollable imperfections and/or adversarial tampering of the random number generator (RNG). This means that the reliability of the generated randomness has to be guaranteed solely in terms of the input-output statistics of the given RNG without verifying its inner workings. This is the requirement of device-independence which is not satisfied even by the RNG based on the inherent unpredictability of Quantum Mechanics (QM). Moreover, Quantum-RNG cannot rule out the possibility that the generated sequence could have been copied several times - the given device may just be producing one of these records. Thus, it is necessary to go beyond Quantum-RNG to generate and certify randomness in a device-independent (DI) way, which we call Genuine Randomness.

An important realisation [1–3] has been that the violation of Bell-CHSH inequality for the entangled states not only implies nonlocality but also provides a necessary requirement for certifying Genuine Randomness. This realisation immediately calls for analysing the relationship between randomness and nonlocality, which then gives rise to the following specific questions: (i) Whether randomness, nonlocality and entanglement are quantitatively commensurate in the sense that the greater amount of nonlocality or entanglement necessarily implies larger amount of randomness. (ii) What would be the optimal resource (in terms of the amount of nonlocality or entanglement) for obtaining the maximum amount of Genuine Randomness.

Considering the question (i), it is important to note that by analysing the implications of the suitably defined bounds of the amount of certified Genuine Randomness, a couple of instructive results had earlier been obtained [3, 4] which suggest that the quantitative relationship between Genuine Randomness and the Bell-CHSH based nonlocality is quite nuanced. This is because the way the amount of Genuine Randomness is related to nonlocality seems to depend on which bound of randomness is considered, i.e., whether it is the guaranteed bound or the maximum achievable bound. Thus, a more comprehensive probing of this issue requires analysis from various perspectives based on different formulations of nonlocality. To this end, the present paper fills this requirement by invoking the Hardy [5] and the Cabello-Liang (CL) relations [6, 7] which are known to provide demonstrations of nonlocality without requiring the Bell-type inequalities.

Regarding the question (ii), an earlier study [4] had shown that in the 2-2-2 scenario, the theoretical maximum amount of 2 bits of certified Genuine Randomness can be realised only for \textit{either} a maximally entangled state corresponding to a small violation of the Bell-CHSH inequality (implying small amount of nonlocality) \textit{or} for the non-maximally pure entangled states corresponding to essentially the maximal violation of the ‘many-settings tilted’ Bell inequality (going beyond the 2-2-2 scenario). On the other hand, in the present paper, we show that in the 2-2-2 scenario, close to the maximum 2 bits of Cabello-Liang certified randomness is obtained even for the

\*

usinha@ri.res.in

\footnote{2 parties - 2 measurements per party - 2 outcomes per measurement}
pure non-maximally entangled two-qubit states. This, therefore, displays quantitative nonequivalence between not only randomness and nonlocality but also with entanglement, significantly, in a single setup\(^2\).

The paper is organised as follows. We begin by reanalysing the issue of certification of randomness. First, note that the violation of Bell inequality as a consequence of local realism does not necessarily rule out the possibility of nonlocal deterministic ontological models consistent with the observed violation of Bell inequality (e.g., the Bohm Model of QM). Thus, such a violation cannot be argued to unequivocally certify Genuine Randomness. This gap can be filled by invoking the treatment given by Cavalcanti et al [1, 8] which shows that the Bell inequality can be derived from the statistical condition of ‘predictability’ used in conjunction with the fundamental principle of ‘no-signalling’ applied at the statistical level. This implies that the statistics of measurement outcomes violating the Bell-CHSH inequality [9, 10] would not only require any underlying realist event-by-event description to be necessarily nonlocal [9], such outcomes would have to also embody the violation of the predictability, thereby implying Genuine Randomness irrespective of any theoretical model. In this paper, we show (Sec II) that the Hardy and CL relations can also be derived from the statistical condition of predictability and the no-signalling principle. Thus, the Hardy and CL relations can also be legitimately used for certifying Genuine Randomness.

Next, by suitably quantifying the guaranteed and the maximum achievable bounds of Genuine Randomness in Sec. III, we evaluate (Sec. IV) the maximum amount of Genuine Randomness for both the cases of the Hardy and CL relations. This is first done by optimising over all pure two-qubit entangled states as well as over all measurement settings for both the Hardy and CL relations. We also evaluate this bound by numerically characterising the quantum extremal behaviours (such behaviour cannot be expressed as a convex combination of other quantum behaviours) in the 2-2-2 scenario using the Hardy and CL relations (Appx. F). Note that while evaluating the maximum bound, we have assumed two-qubit pure states and the measurements to be projective. This bound is called the device-dependent (DD) maximum achievable bound of Genuine Randomness.

Then, in Sec. V, we analyse the way the guaranteed bound of Genuine Randomness can be quantified in the DI scenario. Here, we evaluate such bound in two different ways. Since QM is a special case of the set all possible no-signalling theories violating Bell inequality, in Sec. VA, we first consider the analytical evaluation of this bound in the context of the most general framework of the no-signalling theory which does not involve any assumption other than the no-signalling condition. As illustrated by several recent works [11–18], the role of such general no-signalling theories in providing powerful information-theoretic resource is of considerable interest. In particular, from the point of view of ensuring future-secure secret communication or key distribution protocols, it is desirable to formulate such protocols without requiring the power of the adversaries to be constrained by the QM principles. For example, the secret key distribution protocols have recently been proposed [19–21] whose provable security is based solely on the no-signalling principle. Thus, in the context of such cryptographic protocols, the evaluation of the DI guaranteed bound of Genuine Randomness within the no-signalling theory acquires special relevance.

Subsequently, by restricting this study within the QM framework, in Sec. VB, we proceed to evaluate this bound by optimising over all quantum states as well as over all measurement settings. For this purpose, we take recourse to the numerical computation by employing the technique of Semi Definite Programming (SDP) [22, 23], as discussed by Pironio et al [3]. Then one needs to take the minimum of all the SDP computed bounds pertaining to all the four combinations of the pairs of measurement settings. This is because, it is this minimum quantity which provides a measure of provable security in the DI scenario. In contrast, the only other study [24] based on the Hardy or CL relations for the quantification of randomness in QM uses a quantifier that corresponds to the maximum of all the SDP computed bounds (as elaborately explained in Sec. VB, see also fig. 2) pertaining to all the four possible combinations of the pairs of measurement settings.

The key results obtained on the basis of our study are as follows:

(a) The QM maximum amount of randomness that can be certified by the Hardy relations is numerically found to be 1.6774 bits, and 1.9998 bits for the CL case. Both these maximum values occur corresponding to the small amounts of nonlocality. This feature of incommensurability between the maximum amount of randomness and nonlocality has been shown earlier [4], but restricted to using only the Bell-CHSH inequality. Further, an important result is that, unlike in the Bell-CHSH case, our present study shows that in the 2-2-2 scenario, close to the maximum 2 bits CL certified randomness is obtained even for the pure non-maximally entangled two-qubit states.

(b) The DI guaranteed bounds of Genuine Randomness by using the Hardy/CL relations for both QM and the no-signalling theory are found to be monotonically related to the amount of nonlocality. This is illustrated in Fig. 1 by plotting both the SDP computed QM bounds and the analytically obtained no-signalling bounds of randomness with respect to nonlocality. Then, in Sec. VC, we compare the obtained results in the Hardy/CL case with the earlier obtained results for the Bell-CHSH case, and explain in what sense the Hardy and CL relations are advantageous over the Bell-CHSH inequality for quantifying Genuine Randomness.

The implications of these results and future directions of studies are discussed in the final Sec. VI.

\( ^2 \) By ‘a single setup’, we mean a single experimental arrangement defined by a given state and a specific choice of the measurement settings.
II. Certification of Genuine Randomness using Hardy and Cabello-Liang relations

Let us consider a system of two spatially separated and correlated subsystems shared between two parties Alice and Bob. Their joint state is prepared by a reproducible experimental procedure, $κ_μ$, $μ \in \mathbb{Z}^+$. Alice and Bob measure dynamical variables on each of their sub-systems. Alice can perform one of the possible local measurements $X_i \in \{X_1, X_2, \ldots, X_n\}$ on her subsystem, and the corresponding measurement outcomes are $a \in \{1, 2, \ldots, d_a\}$. Similarly, measurements $Y_j \in \{Y_1, Y_2, \ldots, Y_m\}$ are performed by Bob with the outcomes denoted by $b \in \{1, 2, \ldots, d_b\}$. The statistics arising from a given preparation procedure $κ_μ$ and a particular choice of pairs of measurement settings $X_i$ and $Y_j$ is characterised by a vector in a real number space, $\mathbb{P}_{\text{obs}} = \{P_{\text{obs}}(a, b|X_i, Y_j, κ_μ)\} \in \mathbb{R}^{nm \times d_μ}$, where $P_{\text{obs}}(a, b|X_i, Y_j, κ_μ)$ denotes the observed probability of joint-outcomes $(a,b)$ when $(X_i, Y_j)$ measurement is performed on the shared bipartite system. It is this vector $\mathbb{P}_{\text{obs}}$ which will henceforth be used to denote an observed behaviour corresponding to a fixed preparation procedure.

In such a scenario, it has been shown that the following two assumptions at the operational/statistical level, viz. (a) Predictability and (b) No-signalling, lead to certain bounds on the observable statistical behaviours [1, 8]. Interestingly, the algebraic condition obtained based on this set of assumptions at the operational level turns out to be the Bell-CHSH inequality derived from the assumption of local realism at the ontological level.

The assumptions of predictability and no-signalling, stated precisely, are as follows:

(a) Predictability: Given any state preparation procedure specified by the parameter $κ_μ$, measurement $X_i$ of Alice, and measurement $Y_j$ of Bob, if the respective outcomes $a$ and $b$ of the measurements by Alice and Bob are predictable with certainty, this means that the predicted probability of joint measurement outcomes is given by

$$P(a, b|X_i, Y_j, κ_μ) \in \{0, 1\} \; \forall \; a, b, X_i, Y_j, κ_μ$$

(b) No-signalling condition: This means impossibility of transmitting information from one particle to its spacelike separated partner, implying that the probability of any measurement outcome in one wing is independent of the choice of measurement setting in the other wing, i.e.

$$P(a|X_i, Y_j, κ_μ) = P(a|X_i, κ_μ) \; \forall \; a, X_i, Y_j, κ_μ$$

$$P(b|X_i, Y_j, κ_μ) = P(b|Y_j, κ_μ) \; \forall \; b, X_i, Y_j, κ_μ$$

It was shown in [8] that the above stated assumptions, (a) and (b), lead to the factorisability of the joint probabilities of measurement outcomes at the operational level, i.e.

$$P(a, b|X_i, Y_j, κ_μ) = P(a|X_i, κ_μ) \cdot P(b|Y_j, κ_μ) \; \forall \; a, b, X_i, Y_j, κ_μ$$

Now, this factorisability condition of joint probabilities can be used to derive various conditions for certifying Genuine Randomness. In particular, it has been shown [8] in the 2-2-2 scenario ($n = m = 2$, $d_a = d_b = 2$) that the factorisability condition given by Eq. (4) leads to the Bell-CHSH inequality, whose violation certifies Genuine Randomness:

$$B = \langle X_1 Y_1 \rangle + \langle X_2 Y_2 \rangle + \langle X_2 Y_1 \rangle - \langle X_2 Y_2 \rangle \leq 2$$

where $\langle X_i Y_j \rangle = P(a = b|X_i, Y_j, κ_μ) - P(a ≠ b|X_i, Y_j, κ_μ)$ with $(i, j) \in \{1, 2\}$ and $(a, b) \in \{+1, -1\}$.

In this paper we show (see Appx.A and Appx.B) that from the above mentioned factorisability condition of joint probabilities, one can derive other conditions for certifying Genuine Randomness in the bipartite scenario, the conditions which are also independently derivable from the assumption of local realism, namely, the Hardy [5] and CL relations [6, 7], given by the following respective equations

$$P(+, +|X_1, Y_1, κ_μ) = P_{\text{Hardy}} > 0$$

$$P(−, +|X_2, Y_1, κ_μ) = 0$$

$$P(+, −|X_1, Y_2, κ_μ) = 0$$

$$P(−, +|X_2, Y_2, κ_μ) = 0$$

Note that the simultaneous validity of the Hardy relations given by Eqs. (6 - 9) contradicts the factorisability condition given by Eq. (4) (see Appx.A). Similarly, this also holds good for the Cabello-Liang relations given by Eqs. (10 - 12) (see Appx.B). Hence, the simultaneous validity of all the conditions imposed on the four joint probabilities given either by Eqs. (6 - 9) or by Eqs. (10 - 12) is inconsistent with the factorisability condition derived from the assumptions of predictability and no-signalling. Thus, like the violation of the Bell-CHSH inequality, the measurement outcome statistics satisfying the Hardy or CL relations can also be used to certify Genuine Randomness.

Here if we compare both the above mentioned relations with the Bell-CHSH function, we observe that in the case of the Bell-CHSH function, the constraint provided in Eq. (5) pertains to all the joint probabilities involving different pairs of measurement settings. On the other hand, the respective constraints on the four joint probabilities appearing in both the Hardy and CL relations depend upon choice of the pairs of measurement settings. For instance, in the Hardy relations, while the constraint used for the pairs of measurement settings $(X_2, Y_1)$, $(X_1, Y_2)$ and $(X_2, Y_2)$ is the same, it differs from what is used for the pair of measurement settings $(X_1, Y_1)$. For the CL relations, the constraint used for $(X_2, Y_1)$ and $(X_1, Y_2)$ is different from what is used for $(X_1, Y_1)$ and $(X_2, Y_2)$. Further, another fundamental difference between the Bell-CHSH test of nonlocality and that using the Hardy and CL relations is that it is not possible to exhibit nonlocality of maximally entangled state(s) by using the Hardy/CL relations.
predicted joint probabilities satisfy all the conditions given by Eqs. (6 - 9) [5] or the conditions given by Eqs. (10-12)[6, 7]. This, therefore, implies violation of the condition of predictability, and then the corresponding measurement outcomes can be regarded as genuinely random.

We now proceed to first discuss some basics of the way Genuine Randomness is quantified, followed by the analysis of its DI-quantification relevant in the cryptographic context. Subsequently, considering the DD scenario, we will discuss the maximum amount of certified Genuine Randomness - this is of particular relevance to applications in algorithmic simulations, statistical sampling etc.

### III. Quantification of certified Genuine Randomness in terms of min.-Entropy

In Information Theory, Entropy characterises the unpredictability involved in the statistics of the outcomes of events [27]. Renyi Entropy [28] generalises the different types of entropic function. The Renyi Entropy associated with a random variable X with outcomes 1, 2, ..., n is given by

\[ H_\alpha(X) = \frac{1}{1 - \alpha} \log_2 \left[ \sum_{i=1}^{n} p_i^\alpha \right], \quad 0 \leq \alpha \leq \infty \] (13)

It is to be noted that for different values of \( \alpha \), this quantity \( H_\alpha(X) \) characterises different features of a probability distribution [29]. Interestingly, for \( \alpha \rightarrow \infty \), Renyi Entropy is determined only by the event with highest probability, independent of the probabilities of the other events. This is known as min.-Entropy \( H_\infty \) which characterises the minimum ignorance or unpredictability involved in the probability distribution [29]. It is this quantity which we will use as a measure of Genuine Randomness in our present treatment.

Here it is worth pointing out that an operationally significant justification for regarding the quantity min-Entropy as a quantifier of guaranteed Genuine Randomness stems from the area of cryptographic applications. In such contexts, the reliability of certified randomness must be analysed from the adversarial perspective [31]. Since, for a given set of events, the best strategy for guessing any one of them would be to guess the most probable event [32, 33], it is necessary to consider the maximum probability of guessing the generated random outputs. Further, note that the string of outcome-pairs \( \{(a_i, b_i)\} \), of the two spatially separated measurements on a bipartite system is, in general, non-uniform. In order to make such a string to be useful in the cryptographic applications, it is necessary to make the string to be uniform by applying an extractor. Thus, it is the maximum entropy of such an extracted uniform string which is crucial for determining the optimality of this extraction process, and this quantity is bounded by min-Entropy of the non-uniform original string [31]. In other words, min-Entropy can be regarded as a parameter specifying the optimal length of the extracted uniform string which plays a key role in using Genuine Randomness for different cryptographic applications.

Of course, there are also other measures of randomness that have been invoked in different contexts. In the context of our present work, we should mention that all the studies to date concerning various aspects of the quantification of randomness, based on either QM or no-signalling theory, have essentially used min-Entropy as the measure. Hence, the use of min-Entropy as the quantifier of randomness in our treatment facilitates meaningful comparison of our results with those of the earlier relevant works.

Next, we proceed by writing the amount of randomness associated with a probability distribution \( \bar{P} \equiv \{p_i\} \in \mathbb{R}^n \) with randomness being measured in bits, as given by

\[ R(\bar{P}) = H_\infty(\bar{P}) = -\log_2 p_{\max} \] (14)

The above measure of randomness given by Eq. (14) is then applied for the purpose of quantifying the certified Genuine Randomness embodied in the measurement outcomes violating the Bell-CHSH inequality or satisfying the Hardy / CL relations. For this, we consider the scenario introduced in Section II. The amount of randomness corresponding to the Bell-CHSH violating or the Hardy/CL satisfying observed behaviour \( \bar{P}_{\text{obs}} \) is then given by

\[ R(\bar{P}_{\text{obs}}; X_i, Y_j) = H_\infty(\bar{P}_{\text{obs}}; X_i, Y_j) = -\log_2 \left[ \max_{(a,b)} P_{\text{obs}}(a,b|X_i, Y_j, \kappa_\mu) \right] \] (15)

Now, for a given amount of unpredictability quantified by the Bell-CHSH values or the non-zero values of Hardy/CL parameters, in general, there can be more than one behaviours, \( \bar{P}_{\text{obs}} \). Therefore, in order to evaluate the amount of randomness \( R_{ij} \) corresponding to \( q^\text{th} \) choice of Alice’s measurement and \( p^\text{th} \) choice of Bob’s measurement, \( P_{\text{obs}}(a,b|X_i, Y_j, \kappa_\mu) \) need to be maximised over all \( \bar{P}_{\text{obs}} \). Then the amount of randomness corresponding to a given amount of unpredictability is given by

\[ R_{ij} = -\log_2 \left[ \max_{(a,b)} P_{\text{obs}}(a,b|X_i, Y_j, \kappa_\mu) \right] \] (16)

In order to consider all possible observed behaviours, \( \bar{P}_{\text{obs}} \), we first need to make an assumption of the theory which governs the realisation of such observed behaviours. Here, we consider three types of theory which governs these observed behaviours -(i) Classical theory in which the set of behaviours obey both the no-signalling and predictability condition (compatible with local determinism), we denote this set as \( \mathbb{L} \). (ii) No-signalling theory [1] in which the set of behaviours necessarily obey the no-signalling conditions (as given by the Eqs. (2) and (3)), we denote this set as \( \mathbb{NS} \). (iii) Quantum theory in which the set of behaviours are described by QM, we denote this set as \( \mathbb{Q} \). The sets \( \mathbb{L}, \mathbb{Q} \) and \( \mathbb{NS} \) are closed, bounded and convex [34, 35]. It is also well known that these sets follow the relation, \( \mathbb{L} \subseteq \mathbb{Q} \subseteq \mathbb{NS} \).

\[ \text{Convexity means that if } \bar{P}^1 \text{ and } \bar{P}^2 \text{ belong to one of these sets, then the mixture } q\bar{P}^1 + (1-q)\bar{P}^2 \text{ with } 0 \leq q \leq 1 \text{ also belongs to this set.} \]
Now, in order to solve the optimisation problem given by Eq. (16) by characterising all the observed behaviours, we first take note of the following basic features. Every convex set can be expressed in terms of the extremal behaviours\(^4\). We denote the extremal behaviours as \(\mathcal{F}_{\text{ext}}\) and the set of extremal behaviours by \(\mathbb{S}_{\text{ext}}\). The Krein-Milman theorem [34] states that any convex compact set (in a finite-dimensional vector space) is equal to the convex hull\(^5\) of the extremal behaviours of that set, i.e., \(\mathbb{S} = \text{Conv} (\mathbb{S}_{\text{ext}})\). Therefore, the observed behaviour can be expressed as

\[
\vec{p}_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} \vec{p}_{\text{ext}}
\]

where \(q_{\text{ext}}\) is a probability distribution over extremal behaviours satisfying, \(q_{\text{ext}} \geq 0\) and \(\sum_{\text{ext}} q_{\text{ext}} = 1\).

Thus, in view of Eq. (17), it is sufficient to perform the optimisation given by Eq. (16) restricted to only the extremal behaviours of the \(\mathbb{S}\). Based on this understanding, we can simplify the optimisation problem as follows

\[
R_{ij} = -\log_{2} \left[ \max_{(q, \vec{p}_{\text{ext}})} \sum_{\text{ext}} q_{\text{ext}} G(\vec{p}_{\text{ext}}, X_i, Y_j) \right]
\]

where \(G(\vec{p}_{\text{ext}}, X_i, Y_j) = \max_{(a,b)} P_{\text{ext}}(a, b|X_i, Y_j)\) and \(P_{\text{ext}}(a, b|X_i, Y_j) \in \mathcal{F}_{\text{ext}}\) is the joint probability.

Here, we note that the quantity \(R_{ij}\) defined in Eq. (18) has explicit dependence on the measurement choices \(i\) and \(j\). Thus, there are two possible ways for evaluating the amount of Genuine Randomness (independent of \(i\) and \(j\)) corresponding to a given amount of nonlocality - (i) one can maximise \(R_{ij}\) over all \(i, j\) and obtain the maximum amount of Genuine Randomness \((R_{\text{max}})\) and (ii) one can minimise \(R_{ij}\) over all \(i, j\) and obtain the minimum amount of Genuine Randomness \((R_{\text{min}})\). Next, we first focus on evaluating \(R_{\text{max}}\) corresponding to Hardy and CL relations.

IV. Results: Maximum amount of Genuine Randomness based on the Hardy/Cabell-Liang relations

In order to evaluate the maximum amount of certified Genuine Randomness for a given amount of unpredictability, we have to maximise the Eq. (18) over the Alice’s and Bob’s possible choices of measurement settings

\[
R_{\text{max}} = \max_{X_i, Y_j} \left( R_{ij} \right) = -\log_{2} \left[ \min_{X_i, Y_j} \max_{(q, \vec{p}_{\text{ext}})} \sum_{\text{ext}} q_{\text{ext}} G(\vec{p}_{\text{ext}}, X_i, Y_j) \right]
\]

Now, in the following we first evaluate the maximum amount of Genuine Randomness in the no-signalling theory.

\footnote{The extremal behaviour of any convex set cannot be expressed as any convex combination of other behaviours in that set.}

\footnote{The set of all convex combinations of behaviours belonging to a convex compact set.}

A. \(R_{\text{max}}\) in no-signalling theory

Given that the procedure for certifying Genuine Randomness that we have discussed in Sec. II hinges only on the no-signalling condition, it is thus natural to first discuss the way its maximum bound can be computed within the most general framework assuming only the no-signalling condition. In particular, this is done by relating such bound to the observable values of, say, the Bell-CHSH function, Hardy and CL parameters.

Let us begin by considering the observable behaviour, \(\vec{p}_{\text{obs}} \in \mathbb{NS}\). An important point to be noted is that the no-signalling sets are polytopes (geometric objects with flat sides) and any polytope has finite numbers of extremal behaviours. In particular, the no-signalling polytope in the 2-2-2 scenario can be expressed as the convex hull of 24 extremal distributions, of which 16 distributions are local deterministic (LD) (no-signalling and predictable) and other 8 are Popescu-Rohrlich (PR) box nonlocal distributions (no-signalling and unpredictable distributions) [36, 37].

Note that, out of 8 PR box distributions, only one PR box (see PR box-1 of Appendix A of [38]) exhibits nonlocality by the particular Bell-CHSH inequality (having Bell-CHSH value be 4) given by Eq. (5) or Hardy/CL relations (having \(P_{\text{Hardy}} = P_{\text{CL}} = \frac{1}{2}\)) given by Eqs. (6-9) or Eqs. (10-12).

Therefore, in order to obtain the desired bound, it is sufficient to consider only one PR box distribution. This would correspond to the maximum values of the Bell-CHSH function or Hardy/CL parameters. For such distributions, the evaluated amount of genuine randomness is 1 bit.

B. \(R_{\text{max}}\) in QM

Here we present the results computed on the basis of Eq. (19) for the maximum bounds of certified Genuine Randomness in QM, using the 2-outcome Hardy and CL relations respectively. We consider the observable behaviours, \(\vec{p}_{\text{obs}} \in Q\) where the set \(Q\) is realised by performing local measurements on the quantum systems. The elements of the set \(\vec{p}_{\text{obs}}, P_{\text{obs}}(a, b|X_i, Y_j, k) = \text{tr}[(M_{aX_i} \otimes M_{bY_j}) \rho]\).

Note that in this study, in order to estimate the numerical accuracy of the calculations, we have used as the testbed the analytical result [39] that the maximally entangled states do not exhibit nonlocality through the CL relations, i.e., the maximum value of the CL parameter \((P_{\text{CL}})\) is zero. We then evaluate the maximum value of \(P_{\text{CL}}\) for the maximally entangled state (singlet state) by optimising over all measurement settings. The repeated runs of such numerical calculations show that the first non-zero number appears at the 5\textsuperscript{th} decimal place. Hence, while presenting the results of this study, all the numerical values have been approximated up to 4\textsuperscript{th} decimal place.

An important point to be noted here is that the key property of the set \(\mathbb{NS}\) being a polytope has enabled us to analytically obtain the maximum bound of Genuine Randomness. However, the set \(\mathbb{Q}\) is a convex compact set but not a poly-
tope. Hence, characterising the set of all extremal points of the set $Q$ is, in general, an open problem. Here, for computing the maximum bound of Genuine Randomness, two different procedures are adopted: (i) Using the observed behaviours, $\overline{E}_{\text{obs}}$ arising from the statistics of the projective measurements performed on a pure non-maximally entangled state, and (ii) based on a set of quantum extremal behaviours, by invoking the criterion for quantum extremality given in refs. [40, 41].

For the first procedure, the measurements of Alice and Bob are described by the dichotomic observables $X_i = \pi_{+Y}^X - \pi_{-Y}^X$ and $Y_j = \pi_{+Y}^Y - \pi_{-Y}^Y$ respectively. Here, the projectors $\pi_{\pm Y}^X = \frac{\pm Y_{\pm Y}^X}{2}$ and $\pi_{\pm Y}^Y = \frac{\pm Y_{\pm Y}^Y}{2}$, $a \in \{+1, -1\}$ and the unit vectors $x_i$, $y_j$ in $\mathbb{R}^3$ are given by, $u \in \{x_i, y_j\}$ where $u = \sin \theta_u \cos \phi_u \hat{x} + \sin \theta_u \sin \phi_u \hat{y} + \cos \theta_u \hat{z}$ with $0 \leq \theta_u \leq \pi$ and $0 \leq \phi_u \leq 2\pi$.

Then, maximising over all two-qubit pure states as well as over all possible projective measurements specified by the directions $x_i$, $y_j$, we obtain the maximum amount of certified Genuine Randomness

$$R_{\text{max}}^{\text{DD}} = \max_{X_i, Y_j} R(\overline{E}_{\text{obs}}, X_i, Y_j)$$

$$= -\log_2 \left[ \min_{(a,b)} \max_{(a,b)} \frac{P(a, b|X_i, Y_j, \rho)}{P_{\text{Hardy}} > 0 \text{ or } P_{\text{CL}} > 0} \right]$$

such that

$$P_{\text{Hardy}} > 0 \text{ or } P_{\text{CL}} > 0$$

where $\rho = |\psi\rangle\langle \psi|$ is the density matrix of the pure two-qubit entangled state and $|\psi\rangle = a|01\rangle - \sqrt{1 - a^2}|10\rangle$. We call this quantity computed in this way as device-dependent (DD) maximum bound of genuine randomness ($R_{\text{max}}^{\text{DD}}$) using the numerical method explained in Appx. E. Some representative results are given in Tables I and II.

These results show that in the simplest 2-2-2 scenario, there is a range of non-maximally entangled states using the CL relations and appropriate measurement settings for which it is possible to achieve greater than or equal to 1.99 bits amount of Genuine Randomness. In particular, we have obtained the maximum of 1.9995 bits of CL certified Genuine Randomness for a specific choice of non-maximally entangled state (given in Table II). Note that here the measurement settings yielding close to 2 bits of Genuine Randomness entail arbitrarily small amount of nonlocality implied by the small value of $P_{\text{CL}}$. This finding, therefore, enables demonstrating quantitative incomensurability of the maximum achievable bound of Genuine Randomness with nonlocality and entanglement using a single setup.

Next, for carrying out the second procedure, the maximum amount of Hardy/CL certified Genuine Randomness is estimated by characterising a set of quantum extremal behaviours. In particular, we numerically obtain such extremal behaviours satisfying the Hardy or CL relations by invoking the criterion for quantum extremality [40, 41]. We then find that the maximum amount of Genuine Randomness that can be achieved by extremal Hardy behaviours is 1.6774 bits corresponding to $P_{\text{Hardy}}^{\text{ext}} = 0.0642$ (Appx. F1). For the case of the CL relations, the maximum amount of Genuine Randomness is found to be 1.9997 bits corresponding to $P_{\text{CL}}^{\text{ext}} = 0.0701$ (Appx. F2). Note that results obtained here are the same as that obtained by using the first procedure.

V. Results: Guaranteed amount of Genuine Randomness based on the Hardy/Cabello-Liang relations

This bound has particular importance in the context of cryptographic applications for ensuring the security of a random string under any adversarial guessing. Here it is important to stress that a DI lower bound of Genuine Randomness needs to be computed in order to estimate the guaranteed amount of certified Genuine Randomness which is provably secure, irrespective of whether an adversary has access to information regarding the settings of the measurements performed by the user [42, 43] and/or has control over the preparation procedure. It is using such a measure that one can guarantee a RNG to satisfy Shannon’s version of Kerckhoffs’s principle [30] which is a central tenet of modern cryptography viz. the requirement that a cryptographic system should be designed assuming that “the enemy knows the system”. Therefore, in order to compute DI-guaranteed bound of Genuine Randomness, one has to minimise the quantity $R_{ij}$ defined in the Eq. (18) over Alice’s and Bob’s possible choices of combinations of the pair of measurement settings. Then the DI-guaranteed bound of Genuine Randomness is given by

$$R_{\text{guaranteed}}^{\text{DI}} = \min_{X_i, Y_j} \left( R_{ij} \right)$$

$$= -\log_2 \left[ \max_{X_i, Y_j} \max_{q_{ext}, \bar{R}_{\text{ext}}} \sum_{c_{ext}} q_{ext} G(\overline{E}_{\text{ext}}, X_i, Y_j) \right]$$

such that

$$P_{\text{Hardy}} > 0 \text{ or } P_{\text{CL}} > 0$$

A significance of the above expression given by Eq. (21) lies in determining the DI upper bound on the probability of guessing the most probable pair of outcomes, which is given by $R_{\text{guaranteed}}^{\text{DI}}$, a quantity of key importance from the point of view of adversarial guessing [29, 31–33].

In a nutshell, the quantity $R_{\text{guaranteed}}^{\text{DI}}$ has the following precise operational meaning: For an arbitrarily prepared system and any combination of the pairs of measurement settings, if the statistics of joint measurement outcomes violate the Bell-CHSH inequality or satisfy the 2-outcome Hardy/CL relations, at least $R_{\text{guaranteed}}^{\text{DI}}$ bits amount of Genuine Randomness is ensured.

A. $R_{\text{guaranteed}}^{\text{DI}}$ in NS theory

For the evaluation of the DI guaranteed bound, we use the following theorem [38]. This theorem states that any no-signalling behaviour can be expressed as a convex combination of exactly one PR box and 8 local deterministic (LD) distributions that saturate the Bell-CHSH inequality violated by
that PR box. Therefore, it is sufficient to consider any
signalling distribution, $\tilde{P}^{\text{obs}} \in \mathbb{NS}$ as a convex mixture of these
9 distributions, given by

$$\tilde{P}^{\text{obs}} = q_0 (\tilde{P}^{\text{PR}}) + \sum_{i=1}^{8} q_i (\tilde{P}^{\text{LD}})$$  \hspace{1cm} (22)$$

Here $q_i \geq 0 \ \forall \ j = \{0, 1, \ldots, 8\}$ and $q_0 + \sum_{i=1}^{8} q_i = 1$.

Next, using Eqs. (21) and (22), we analytically obtain (see
Appx. C) the DI guaranteed bounds of Genuine Randomness
in any no-signalling theory as a function of the observable
values of the Hardy and CL parameters, which are given by

$$(R_{\text{guaranteed}}}^{\text{Hardy}})_{\mathbb{NS}} = -\log_2 \left(1 - P^{\text{obs}}_{\text{Hardy}}\right) \hspace{1cm} (23)$$

$$(R_{\text{guaranteed}}}^{\text{CL}})_{\mathbb{NS}} = -\log_2 \left(1 - P^{\text{obs}}_{\text{CL}}\right) \hspace{1cm} (24)$$

**B. $R_{\text{guaranteed}}^{\text{Hardy}}$ in QM**

Note that the set $\mathbb{Q}$ is a convex compact set but not a polytope. Hence, characterising the set of all extremal points of the set $\mathbb{Q}$ is, in general, an open problem. Thus, the optimisation problem defined in Eq. (21) is recast in the following form

$$R_{\text{guaranteed}}^{\text{DI}} = -\log_2 \left[ \max_{\tilde{P}^{\text{obs}} \in \mathbb{Q}} \max_{\{X_j, Y_j, \kappa_j\}} P(a,b|X_j, Y_j, \kappa_j) \right]$$

such that

$$B > 2 \ \text{or} \ P_{\text{Hardy}} > 0 \ \text{or} \ P_{\text{CL}} > 0$$

$$\tilde{P}^{\text{obs}} \in \mathbb{Q}$$ \hspace{1cm} (25)

The above optimisation needs to be performed over all observable behaviours, $\tilde{P}^{\text{obs}} \in \mathbb{Q}$. Given the analytical complexity in characterising all $\tilde{P}^{\text{obs}}$ in QM, we take recourse to the numerical computation (see Appx. D) by employing the SDP technique [3, 22, 23].

The DI bound of Hardy/CL certified randomness for the different non-vanishing values of $P_{\text{Hardy}}/P_{\text{CL}}$ is then computed. The quantitative relationships of this bound with the respective non-vanishing values of $P_{\text{Hardy}}$ and $P_{\text{CL}}$ are shown in Fig. 1. We observe that for the varying values of $P_{\text{Hardy}}$ and $P_{\text{CL}}$, these respective DI guaranteed bounds of Genuine Randomness grow from zero (corresponding to $P_{\text{Hardy}} = P_{\text{CL}} = 0$) with the increasing amount of nonlocality quantified by the respective increasing values of $P_{\text{Hardy}}$ and $P_{\text{CL}}$. Thus, such DI guaranteed bound is a monotonically increasing function of Hardy/CL nonlocality. In particular, when the value of $P_{\text{Hardy}}$

| $R_{\text{max}}^{DD}$ | $P_{\text{Hardy}}$ | State | Settings in radian |
|-------------------|-----------------|-------|------------------|
| 1. 1.6787         | 0.0640          | 0.5380 | $|01\rangle - 0.8429 \ |10\rangle$ | 0.9432, 1.3482, 2.1984, 1.7934, 4.6405, 1.4989, 4.6405, 1.4989 |
| 2. 1.3937         | 0.0902          | 0.4192 | $|01\rangle - 0.9079 \ |10\rangle$ | 0.6081, 1.1937, 2.533, 1.9479, 4.6928, 1.5512, 4.6928, 1.5512 |

**TABLE I.** Two different values of the QM computed device-dependent maximum achievable bound of certified Genuine Randomness ($R_{\text{max}}^{DD}$) corresponding to the respective values of $P_{\text{Hardy}}$ are shown in the respective columns. One of them is the maximum value of $R_{\text{max}}^{DD}$ given by 1.6787 bits, obtained for $P_{\text{Hardy}} = 0.0640 \ (\leq (P_{\text{Hardy}})_{\text{max}} = 0.0902)$ corresponding to a pure non-maximally entangled state. Similarly, the other value of $R_{\text{max}}^{DD}$ given by 1.3937 bits (less than its maximum value) corresponds to $(P_{\text{Hardy}})_{\text{max}} = 0.0902$. Thus, these two examples show that the maximum achievable bound of randomness, nonlocality and entanglement are quantitatively non-equivalent. For both these cases, the respective measurement directions that are required for achieving the values of $R_{\text{max}}^{DD}$ for the corresponding pure non-maximally entangled states are mentioned above.

| $R_{\text{max}}^{DD}$ | $P_{\text{CL}}$ | State | Settings in radian |
|-------------------|-----------------|-------|------------------|
| 1. 1.9995         | 0.0002          | 0.7067 | $|01\rangle - 0.7075 \ |10\rangle$ | 1.2607, 1.3036, 1.8391, 1.8798, 3.9213, 2.2619, 5.4035, 0.7797 |
| 2. 1.5814         | 0.1078          | 0.4804 | $|01\rangle - 0.8771 \ |10\rangle$ | 0.5940, 1.0192, 2.5476, 2.1224, 4.6890, 1.5474, 4.6890, 1.5474 |

**TABLE II.** Two different values of the QM computed device-dependent maximum achievable bound of certified Genuine Randomness ($R_{\text{max}}^{DD}$) corresponding to the respective values of $P_{\text{CL}}$ are shown in the respective columns. One of them is the maximum value of $R_{\text{max}}^{DD}$ given by 1.9995 bits, obtained for $P_{\text{CL}} = 0.0002 \ (\leq (P_{\text{CL}})_{\text{max}} = 0.1078)$ corresponding to a pure non-maximally entangled state. A range of states is given in $E$ for which the amount of CL certified Genuine Randomness is greater than or equal to 1.99 bits. The other value of $R_{\text{max}}^{DD}$ given by 1.5814 bits (less than its maximum value) corresponds to $(P_{\text{CL}})_{\text{max}} = 0.1078$. Thus, these two examples show that the maximum achievable bound of randomness is quantitatively non-equivalent with nonlocality and entanglement. For both these cases, the respective measurement directions that are required for achieving the values of $R_{\text{max}}^{DD}$ for the corresponding pure non-maximally entangled states are mentioned above.
reaches its maximum value 0.0902, then the maximum value of the QM DI guaranteed Genuine Randomness is 0.6674 bits. Similarly, for the maximum $P_{CL} = 0.1078$, the maximum value of the QM DI guaranteed Genuine Randomness is 0.6207 bits. On the other hand, for the Bell-CHSH case, along with the monotonicity of the amount of Genuine Randomness with respect to nonlocality, the QM DI guaranteed maximum value has been computed to be 1.23 bits [3], which is higher than the values we have obtained by using the Hardy or CL relations.

It is to be noted that in the bipartite two measurement settings scenario, there are four possible combinations of the pairs of measurement settings $(X_1, Y_1), (X_1, Y_2), (X_2, Y_1), (X_2, Y_2)$ where the values of $X, Y$ span over all possible measurement directions. If we consider two-outcomes per setting, there will be four joint probabilities of outcomes corresponding to each such combination. Then, there exists a corresponding amount of certified randomness for each such combination. Our computation reveals an important feature that the amount of Hardy/CL certified randomness differs according to the choice of the combination of the pairs of measurement settings (see Fig. (2)). This is because, each of the four joint probabilities in the Hardy/CL relations occurs separately in each such combination. These joint probabilities are, crucially, subjected to different constraints given by the respective Eqs. (6-9), or Eqs. (10-12). Hence, for obtaining the DI guaranteed randomness, it is necessary to first optimise over all possible quantum states as well as over all possible measurement directions using SDP and then take the minimum of the SDP computed bounds for the four different combinations of the pairs of measurement settings. On the other hand, the quantity evaluated in the treatment by Li et al [24] corresponds to the maximum of the SDP computed bounds for these four different combinations. Thus, this quantity does not correspond to the DI guaranteed bound of Genuine Randomness (as explicitly shown in Fig. (2)).

C. The DI guaranteed bounds of Genuine Randomness vis-a-vis nonlocality in terms of the Bell-CHSH value

For any specified value of the Bell-CHSH expression signifying a measure of nonlocality [44, 45], subject to the no-signalling condition, it is possible to express the Bell-CHSH value in terms of the four joint probabilities which occur in the Hardy and CL relations. Then, taking cue from the earlier studies [46–48], for any set of joint probabilities satisfying the Hardy and CL relations, one can show that the Bell-CHSH value reduces to $4P_{Hardy} + 2$ and $4P_{CL} + 2$ respectively (see Appx. G). Thus, for any amount of nonlocality as quantified by the Bell-CHSH value, one can compare the SDP-computed DI guaranteed bounds of Genuine Randomness certified using the Bell-CHSH inequality, Hardy and CL relations respectively. In Fig. 3, this comparison is exhibited for the different Bell-CHSH values, which shows that

$$R_{\text{DI,guaranteed}}(\text{Hardy}) \geq R_{\text{DI,guaranteed}}(\text{CL}) \geq R_{\text{DI,guaranteed}}(\text{Bell-CHSH})$$

Hence, we conclude that the use of the Hardy relations is advantageous than using the CL relations or the Bell-CHSH inequality for obtaining a higher amount of DI guaranteed randomness corresponding to any given amount of nonlocality which is less than or equal to the Bell-CHSH value $10\sqrt{5} - 2 \approx 2.3607$. This threshold Bell-CHSH value corresponds to the QM maximum value of the Hardy parameter, $P_{Hardy} = \frac{5 \sqrt{5} - 11}{2}$.

VI. Salient Features and Outlook

We summarise the key findings of the present work as follows:

(a) As the basis for this work, we have provided justification of the way the Hardy and Cabello-Liang relations can enable the certification of Genuine Randomness, by invoking only the no-signalling condition at the statistical level.

(b) A key result is that in the simplest 2-2-2 scenario, by using the CL relations, it is possible to realise close to the maximum amount of 2 bits of Genuine Randomness for a range of pure non-maximally entangled states, even for small amounts of nonlocality. Therefore, this result shows the incommensurability between the maximum achievable amount of randomness, nonlocality and entanglement in a single setup.

(c) Further, using the Hardy and CL relations, we have analytically obtained the DI guaranteed amount of Genuine Randomness as a function of nonlocality for any no-signalling theory. Then, this Hardy/CL certified bound is evaluated within the QM framework by performing the computation using SDP technique.

The above evaluations show that the DI guaranteed bounds of Genuine Randomness in the no-signalling framework for both the Hardy and CL relations are lower than that obtained for the corresponding QM cases (see Fig. 1), similar to that obtained [3] for the Bell-CHSH inequality. Hence, it is seen that against any omnipotent adversary who is constrained only by the no-signalling principle, the guaranteed amount of secure randomness is, in general, less than that estimated quantum mechanically.

Further, the monotonicity between the bound $R_{\text{DI,guaranteed}}$ and the amount of Hardy/CL nonlocality is shown to be similar to that for the Bell-CHSH case. This reinforces the point that greater the amount of nonlocality, higher is the assured amount of Genuine Randomness.

---

6 The DI guaranteed bound of the Bell-CHSH certified Genuine Randomness is the same for any combination of the pairs of measurement settings. This is because, the single Bell-CHSH constraint involves all the four combinations of the pairs of measurement settings entailing sixteen joint probabilities of outcomes.
(a) The curves 'a' and 'b' showing the variation of the DI guaranteed bound of Genuine Randomness ($R_{\text{DI}}^{\text{min}}$) with Hardy nonlocality ($P_{\text{Hardy}}$).

(b) The curves 'a' and 'b' showing the variation of the DI guaranteed bound of Genuine Randomness ($R_{\text{DI}}^{\text{min}}$) with Cabello-Liang nonlocality ($P_{\text{CL}}$).

FIG. 1. The curves represent the monotonic relationship between the DI guaranteed bound of Genuine Randomness ($R_{\text{DI}}^{\text{guaranteed}}$) and nonlocality for both the cases of Hardy and Cabello-Liang relations. In both the Figs. (a) and (b), the results given by the curves a have been obtained by using no-signalling (NS) principle alone. The curves b represent the QM computed results obtained by the SDP technique, as explained in Appx. D. The QM computed maximum values of $R_{\text{DI}}^{\text{guaranteed}}$ in the Hardy and Cabello-Liang cases are 0.6674 and 0.6207 bit respectively. On the other hand, the NS computed maximum values of $R_{\text{DI}}^{\text{guaranteed}}$ in the Hardy and Cabello-Liang cases are found to be 0.1564 and 0.1646 bit respectively which are the same as that analytically evaluated using Eqs. (23) and (24).

(a) The curves 'a' and 'b' correspond to the different bounds of randomness pertaining to all the combinations of the pairs of measurement settings for the Hardy relations.

(b) The curves 'a', 'b' and 'c' correspond to the different bounds of randomness pertaining to all the combinations of the pairs of measurement settings for the Cabello-Liang relations.

FIG. 2. These curves represent the QM computed results obtained by the SDP technique. Note that the curve 'a' corresponds to the minimum of the bounds obtained in this way ($R_{11}$ or $R_{21}$ or $R_{12}$ for Hardy case and $R_{11}$ or $R_{21}$ for Cabello-Liang case) which represents the DI guaranteed bound of Genuine Randomness.

Thus, our work stands out in analysing the question of quantitative commensurability between randomness and nonlocality in a unified way, both by considering the DI guaranteed bound and the device-dependent (DD) maximum bound of randomness using the Hardy and Cabello-Liang relations.

The upshot of the results of this work, combined with those obtained by S. Pironio et al [3] and A. Acin et al [4], is the reinforcement of the realisation of a fundamental feature of the quantum world which is linked with randomness. While the certification of Genuine Randomness necessarily requires nonlocality, the nature of the quantitative relationship between them critically differs according to the bound of certified Genuine Randomness in question. For the DI guaranteed bound, the quantitative commensurability between randomness and nonlocality holds good. However, in the case of the DD maximum amount, a striking quantitative incommensurability between them is manifested. Importantly, both these findings are valid irrespective of the type of arguments used for show-
ing nonlocality, either in terms of the Bell inequalities or by invoking the Hardy and Hardy-type (CL) relations. It will, therefore, be interesting to extend this line of study by using other arguments of nonlocality, such as different forms of the higher settings Bell inequality [49–59], or the generalised variants of the Hardy relations [60, 61]. Another possible direction of study could be to go beyond the 2-2-2 scenario using the recently suggested measure of nonlocality which has been invoked to argue for ensuring the commensurability between entanglement and nonlocality for arbitrary dimensional system [62, 63].

Acknowledgements

Helpful discussions related to this work with Antonio Acín during the Int. Conf. QFF2020 at RRI, Bangalore are gratefully acknowledged. SS acknowledges the financial support from INSPIRE programme, Department of Science and Technology, Govt. of India. SG acknowledges the KVPY scholarship funded by the Department of Science and Technology, Govt. of India. AR acknowledges the funding and support from VEGA Project No. 2/0136/19 and the Slovak Academy of Sciences. DH thanks NASI for the support provided by Senior Scientist Platinum Jubilee Fellowship and acknowledges support of the QuEST-DST Project Q-98 of the Govt. of India. US acknowledges the support provided by Ministry of Electronics & Information Technology (MeitY), Government of India under grant for “Centre for Excellence in Quantum Technologies” with Ref. No. 4(7)/2020-ITEA.

A. Certification of Genuine Randomness using the 2-outcome Hardy relations

Let us consider the two-outcome Hardy relations characterised by the simultaneous validity of the following four conditions on joint probabilities

\[ P(+1, +1|X_1, Y_1, \kappa_\mu) = P_{Hardy} > 0 \quad (A1) \]
\[ P(-1, +1|X_2, Y_1, \kappa_\mu) = 0 \quad (A2) \]
\[ P(+1, -1|X_1, Y_2, \kappa_\mu) = 0 \quad (A3) \]
\[ P(+1, +1|X_2, Y_2, \kappa_\mu) = 0 \quad (A4) \]

Now, applying the factorisability condition given in the text by Eq. (4) to the above mentioned Hardy relations, we obtain

\[ P(+1|X_1, \kappa_\mu) P(+1|Y_1, \kappa_\mu) = P_{Hardy} > 0 \quad (A5) \]
\[ P(-1|X_2, \kappa_\mu) P(+1|Y_1, \kappa_\mu) = 0 \quad (A6) \]
\[ P(+1|X_1, \kappa_\mu) P(-1|Y_2, \kappa_\mu) = 0 \quad (A7) \]
\[ P(+1|X_2, \kappa_\mu) P(+1|Y_2, \kappa_\mu) = 0 \quad (A8) \]

Next, we show that the simultaneous validity of the above four Eqs. (A5)-(A8) is inconsistent with the factorisability condition. Specifically, we show the inconsistency of Eq. (A5) with Eqs. (A6-A8). For this purpose, we rewrite Eqs. (A6) and (A7) respectively as follows

\[ P(+1|Y_1, \kappa_\mu) = P(+1|X_1, \kappa_\mu) P(+1|X_2, \kappa_\mu) \quad (A9) \]
\[ P(+1|X_1, \kappa_\mu) = P(+1|X_1, \kappa_\mu) P(+1|Y_2, \kappa_\mu) \quad (A10) \]

Multiplying the above two equations leads to the following

\[ P(+1|X_1, \kappa_\mu) P(+1|Y_1, \kappa_\mu) = P(+1|X_1, \kappa_\mu) P(+1|Y_1, \kappa_\mu) P(+1|X_2, \kappa_\mu) P(+1|Y_2, \kappa_\mu) \quad (A11) \]

Finally, using Eq.(A8) in Eq.(A11), we obtain

\[ P(+1|X_1, \kappa_\mu) P(+1|Y_1, \kappa_\mu) = 0 \quad (A12) \]

which contradicts Eq. (A5), i.e., the condition that \( P_{Hardy} > 0 \). Hence, the simultaneous validity of all the conditions imposed on the four joint probabilities given by Eqs. (A1 - A4) is inconsistent with the factorisability condition given by Eq. (4) in the text. This implies violation of the condition of predictability. Thus, the Hardy relations can be employed for certifying Genuine Randomness.

B. Certification of Genuine Randomness using the Cabello-Liang relations

Here we consider a variant of the Hardy relations, namely, the CL relations which have also been used for showing [6, 7] quantum nonlocality independent of the Bell type inequalities. In the following, we will show that the simultaneous validity of all the CL relations contradicts the factorisability condition given by Eq. (4).
The CL relations can be written as follows

\[ P_{CL} = P(+1, +1|X_1, Y_1, \kappa) - P(+1, +1|X_2, Y_2, \kappa) > 0 \] (B1)

\[ P(-1, +1|X_2, Y_1, \kappa) = 0 \] (B2)

\[ P(+1, -1|X_1, Y_2, \kappa) = 0 \] (B3)

Now, applying the factorisability condition given by Eq. (4), Eqs. (B2) and (B3) can be rewritten respectively as

\[ P(+1|Y_1, \kappa) = P(+1|Y_1, \kappa) P(+1|X_2, \kappa) \] (B4)

\[ P(+1|X_1, \kappa) = P(+1|X_1, \kappa) P(+1|Y_2, \kappa) \] (B5)

It then follows from the above two Eqs. (B4) and (B5)

\[ P(+1|X_1, \kappa) P(+1|Y_1, \kappa) - P(+1|X_2, \kappa) P(+1|Y_2, \kappa) = P(+1|X_2, \kappa) P(+1|Y_2, \kappa) \{ -1 + P(+1|X_1, \kappa) P(+1|Y_1, \kappa) \} \leq 0 \]

\[ \Rightarrow P_{CL} \leq 0. \] (B6)

thereby contradicting Eq. (B1). Hence, any joint probability distribution of the measurement outcomes satisfying all the CL relations given by Eqs. (B1-B3) would be inconsistent with the factorisability condition (Eq. (4) in the text). This implies violation of the condition of predictability. Thus, the CL relations can be employed for certifying Genuine Randomness, similar to the use of the Hardy relations.

### C. Analytically obtained DI guaranteed bounds of Genuine Randomness in any NS theory

For the convenience of this demonstration, we introduce a quantity defined as \( G(\mathbb{E}^{obs}, X, Y) = \max_{a,b} P(ab|x, y, \kappa) \). This quantity has a precise physical meaning that it denotes the probability with which an adversary can guess the joint outcomes of the measurements \((X_i, Y_j)\) by Alice and Bob. We call this quantity as guessing probability.

Now, in order to evaluate \( G(\mathbb{E}^{obs}, X, Y) \), we recall Eq. (22) given in the text

\[ \mathbb{E}^{obs} = q_0 (\mathbb{E}^{PR}) + \sum_{i=1}^{8} q_i (\mathbb{E}^{LD}) \] (C1)

Here \( q_j \geq 0 \ \forall \ j = \{0, 1, \ldots, 8\} \) and \( q_0 + \sum_{i=1}^{8} q_i = 1 \). Then using the above Eq. (C1), we obtain

\[ G(\mathbb{E}^{obs}, X, Y) = q_0 G(\mathbb{E}^{PR}, X, Y) + \sum_{i=1}^{8} q_i G(\mathbb{E}^{LD}, X, Y) \] (C2)

Now, using the PR box distributions, \( G(\mathbb{E}^{PR}, X, Y) = \frac{1}{2} \) (see Appendix A of [38]). Further, since any local deterministic distribution is predictable, \( G(\mathbb{E}^{LD}, X, Y) = 1 \). Then Eq. (C2) reduces to

\[ G(\mathbb{E}^{obs}, X, Y) = q_0 \frac{1}{2} + (1 - q_0) = 1 - \frac{q_0}{2} \] (C3)

Next, from Eq. (C1), we see that any observable behaviour can be realised by the convex mixture of 1 PR box behaviour and 8 LD behaviours. This means that, each element, \( P^{obs}(a, b|x, y) \in \mathbb{E}^{obs} \), should then be reproduced by the convex mixture of elements corresponding to the PR and 8 LD behaviours. Thus, we can write

\[ P^{obs}(a, b|x, y) = q_0 P^{PR}(a, b|x, y) + \sum_{i=1}^{8} q_i P^{LD}(a, b|x, y) \] (C4)

It then follows that the observed Hardy and CL parameters can be expressed as

\[ P^{obs}_{Hardy} = q_0 P^{PR}_{Hardy} + \sum_{i=1}^{8} q_i P^{LD}_{Hardy} = \frac{q_0}{2} \] (C5)

\[ P^{obs}_{CL} = q_0 P^{PR}_{CL} + \sum_{i=1}^{8} q_i P^{LD}_{CL} = \frac{q_0}{2} \] (C6)

From the above Eqs. (C5 and C6) we obtain the value of \( q_0 \) as a function of the observable Hardy or CL parameter and then using Eq. (C3), we obtain

\[ G(\mathbb{E}^{obs})_{Hardy} = 1 - P^{obs}_{Hardy} \]

\[ G(\mathbb{E}^{obs})_{CL} = 1 - P^{obs}_{CL} \] (C7)

### D. Computation of DI guaranteed bounds of Genuine Randomness using QM and NS theory

For computing the DI guaranteed bound of Genuine Randomness for both quantum mechanically and using the no-signalling (NS) principle, we proceed as follows.

Let us consider that \( S \) is any convex subset of the set of joint conditional probability distributions \( \mathcal{P} = \{P(a, b|x, y) : a, b \in \{\pm 1\} \text{ and } x, y \in \{1, 2\}\} \). We further assume that all the elements in \( S \) satisfy the NS condition. Then the guaranteed amount of randomness, say \( R^S_{\text{guaranteed}} \), that can be certified, subject to a given nonlocality condition, is given by

\[ R^S_{\text{guaranteed}} = \min_{\mathcal{P} \in S} \left[ -\log_2 \left( \max_{a,b,x,y} P(a, b|x, y) \right) \right] \]

subject to relevant constraints on \( P(a, b|x, y) \) (D1)

This optimisation problem can readily be solved by applying the semi-definite-programming (SDP) technique as this is a case of the convex optimisation problem.

Note that the phrase “relevant constraints on \( P(a, b|x, y) \)” used in Eq. (D1) is explained as follows: First, in order to evaluate the NS bound of \( R^S_{\text{guaranteed}} \) we consider the subset \( S \in \{P(a, b|x, y)\} \) satisfying either the Hardy or CL relations. Secondly, for obtaining the QM computed lower bound
of $R_{\text{guaranteed}}^{\text{QM}}$, we apply the specific QM-constraints\(^7\) on the subset $S$.

Now, for solving the optimisation problem, given by Eq. (D1), using the SDP technique \([22, 23]\), we choose our convex set $S$ as different levels of the NPA-Hierarchy, denoted here by $Q^{(k)}$ where $k \in \{0, 1, 1+ab, 2, 3, \ldots\}$. All these different levels are convex, and form a sequence of outer approximations of the set of quantum behaviours $Q$, i.e., $Q^{(0)} \supseteq Q^{(1)} \supseteq \ldots Q^{(k)} \supseteq \ldots \supseteq Q$. Note that the zeroth level approximation $Q^{(0)}$ is the set of all NS behaviours. Also, note that in the 2-2-2 scenario, the convergence of $Q^{(k)}$ is very fast so that at the level 1+ab (an intermediate level which lies between the levels 1 and 2), $Q^{(1+ab)} \supseteq Q$. Thus, in order to compute the DI guaranteed $QM$ bound of Genuine Randomness from the Hardy relations, the following SDP sub-problem is solved:

$$\max P(a, b|x, y); \quad \text{subject to} \quad \bar{\psi} \in Q^{(1+ab)},$$

$$P(+1, +1 | 1, 1) = P_{\text{Hardy}}, \quad P(-1, +1 | 2, 1) = 0,$$

$$P(+1, -1 | 1, 2) = 0,$$

$$P(+1, +1 | 2, 2) = 0. \quad \text{(D2a)}$$

Next, for computing the DI guaranteed $NS$ bound of certified Genuine Randomness from the Hardy relations, the following SDP sub-problem is solved:

$$\max P(a, b|x, y); \quad \text{subject to} \quad \bar{\psi} \in Q^{0},$$

$$P(+1, +1 | 1, 1) = P_{\text{Hardy}}, \quad P(-1, +1 | 2, 1) = 0,$$

$$P(+1, -1 | 1, 2) = 0,$$

$$P(+1, +1 | 2, 2) = 0. \quad \text{(D3a)}$$

Similarly, in order to compute the DI guaranteed bounds on Genuine Randomness from the CL relations, the following SDP sub-problems are solved:

$$\max P(a, b|x, y); \quad \text{subject to} \quad \bar{\psi} \in Q^{(1+ab)},$$

$$P(+1, +1 | 1, 1) - P(+1, +1 | 2, 2) = p_{\text{CL}}, \quad P(-1, +1 | 2, 1) = 0,$$

$$P(+1, -1 | 1, 2) = 0.$$  \quad \text{(D4a)}$$

$$\text{NS guaranteed bound of Genuine Randomness:}$$

$$\max P(a, b|x, y); \quad \text{subject to} \quad \bar{\psi} \in Q^{0},$$

$$P(+1, +1 | 1, 1) - P(+1, +1 | 2, 2) = p_{\text{CL}}, \quad P(-1, +1 | 2, 1) = 0,$$

$$P(+1, -1 | 1, 2) = 0. \quad \text{(D5a)}$$

$$\text{E. Computation of the maximum achievable amount of Genuine Randomness in QM}$$

Here we compute the maximum achievable amount of Genuine Randomness in a device-dependent way. The maximum amount of Genuine Randomness corresponding to a bipartite quantum state $\rho$ is given by

$$R_{\text{max}}^{DD} = \max_{\{M_{aX}, \{M_{aY}, \rho\}} \left( -\log_2 \max_{[a,b]} P(a, b|x, y) \right) \quad \text{subject to} \quad$$

$$i) P(a, b|x, Y, \rho) = Tr[\rho \sum_a M_{aX} \otimes M_{aY}],$$

$$ii) \text{relevant constraints on } P(a, b|x, Y, \rho) \text{ as given by the Hardy/CL relations.} \quad \text{(E1)}$$

Now, to find this bound numerically, we have to optimise the following function known as the objective function given by

$$\text{objective function :}$$

$$-\log_2 \left( \min_{\{M_{aX}, \{M_{aY}, \rho\}} \left( \max_{[a,b]} P(a, b|x, Y, \rho) \right) \right)$$

$$\text{subject to} \quad$$

$$i) P(a, b|x, Y, \rho) = Tr[\rho \sum_a M_{aX} \otimes M_{aY}],$$

$$ii) \text{relevant constraints on } P(a, b|x, Y, \rho) \text{ as given by the Hardy/CL relations.} \quad \text{(E2)}$$

where $\rho = |\psi\rangle\langle\psi|$ is the density matrix of the pure two-qubit entangled state and $|\psi\rangle$ is given by

$$|\psi\rangle = |01\rangle - \sqrt{1-a^2}|10\rangle \quad \text{subject to} \quad$$

$$P(a, b|x, Y, \rho) = Tr[\rho \sum_a M_{aX} \otimes M_{aY}],$$

$$i) \text{relevant constraints on } P(a, b|x, Y, \rho) \text{ as given by the Hardy/CL relations.} \quad \text{(E3)}$$

The projection operators are

$$\Pi_{\alpha}^{b} = \frac{I + a \hat{a} \varepsilon^b}{2}. \quad \text{(E3)}$$

\(^7\) (i) $P(a, b|X_{i}, Y_{j}, \rho) = Tr[M_{aX} \otimes M_{aY} \rho]$, (ii) $\rho \in H_{A} \otimes H_{B}$ of dimension $d_{A}d_{B}$ and (iii) each of the measurements $X_{i}$ of Alice corresponds to a positive-operator-valued-measure (POVM): $X_{i} = \{M_{aX}\}_{a}$ with $M_{aX} \geq 0$ for all $a$ and $\sum_{a} M_{aX} = I_{d_{A}}$. Similarly, each measurement setting $Y_{j}$ of Bob corresponds to a positive-operator-valued-measure (POVM): $Y_{j} = \{M_{aY}\}_{a}$ with $M_{aY} \geq 0$ for all $b$ and $\sum_{b} M_{aY} = I_{d_{B}}$. \(\Box\)
where \( a \in \{+1, -1\} \) and \( \hat{u} \in \{\hat{x}, \hat{y}\} \) is a unit vector in \( \mathbb{R}^2 \), given by

\[
\hat{u} = \sin \phi_a \cos \phi_u \hat{x} + \sin \phi_u \sin \phi_a \hat{y} + \cos \theta_u \hat{z}
\]

Then, for solving the min-max optimisation problem given by Eq. (E2), we have employed a numerical nonlinear constrained optimisation (fmincon function) technique in MATLAB programming language [64]. Since, throughout our numerical evaluations, we have considered the approximation of numerical values up to \( 4^{th} \) decimal places, we have considered 10,000 iterations subject to the following numerical precision: constraint tolerance - \( 10^{-8} \), function tolerance - \( 10^{-8} \). In this way, the numerical values of \( R_{DD}^{max} \), the non-zero values of the Hardy \((P_{Hardy})/CL\) \((P_{CL})\) parameter, respective measurement settings and state parameters \((\alpha)\) are evaluated. This suffices to obtain a range of states and the required measurement settings which lead to close to the maximum possible amount (2 bits) of Genuine Randomness certified by the CL relations. In particular, we have numerically found suitable measurement settings for yielding greater than or equal to 1.95 bits of Genuine Randomness for which the state parameter \((\alpha)\) of the required pure non-maximally entangled states needs to have a set of specific values, such as \( \alpha = 0.6520.7007.0.7067.0.7095.0.7239 \) (corresponding to the concurrence lying between 0.9887 and 0.9999, see Fig. 4). Interestingly, this is achieved for small amount of non-locality signified by the values of \( P_{CL} \) lying within the range, \( 0 < P_{CL} \leq 0.0050 \), much smaller than the maximum value of \( P_{CL} \) given by 0.1078.

**F. Computation of the maximum achievable amount of Hardy/CL certified Genuine Randomness by characterising the quantum extremal behaviours**

The 24 extremal behaviours (16 LD behaviours and 8 PR-Box nonlocal behaviours) corresponding to the (2-2-2) NS polytope are given in Ref. [38] (Appx. A) where each cell of the 24 Tables (Tables A1 and A2) corresponds to the joint probability \( P(a, b|X, Y) \) and each Table represents the behaviour \( \vec{P} \) comprising 16 joint probabilities.

1. **Computation of \( R_{DD}^{max} \) by characterising the quantum extremal behaviours using the Hardy relations**

From such 24 extremal distributions, it can be shown that out of 8 PR-Box behaviours, only PR-Box 1 (see PR box-1 of Table A1 of [38]) leads to the Hardy type nonlocality, satisfying all the Hardy relations given by Eqs. (6-9). Out of the 16 LD behaviours, using the particular Hardy relations given by Eqs. (6-9), only 5 LD behaviours (LD4, LD8, LD12, LD14, LD15; see Table A2 of [38]) can be shown to be local deterministic. The other 11 LD behaviours can be shown [35] to be local deterministic by using other equivalent forms of the Hardy relations. The same argument holds good for the 7 PR box behaviours.

It, therefore, follows that any NS behaviour satisfying the Hardy relations given by Eqs. (6-9) can be expressed as a convex mixture of five LD and one PR box behaviours. Then the observable NS behaviours satisfying the Hardy relations are given by

\[
\vec{P}_{Hardy}^{obs} = \lambda_1 \vec{P}_1 + \lambda_4 \vec{LD}_4 + \lambda_8 \vec{LD}_8 + \lambda_{12} \vec{LD}_12
\]

\[
+ \lambda_{14} \vec{LD}_14 + \lambda_{15} \vec{LD}_15
\]

where \( 0 \leq \lambda_i \leq 1, \lambda_1 + \lambda_4 + \lambda_8 + \lambda_{12} + \lambda_{14} + \lambda_{15} = 1 \). Note that the value of the Hardy parameter \( P_{Hardy}^{obs} \in [\vec{P}_{Hardy}^{obs}] = \frac{1}{2} \).

Now, by invoking the following criteria [40, 41] (given by Eq. (F2)) for quantum extremality, we numerically obtain the different values of \( \lambda_i \)’s and, thus, the quantum Hardy extremal behaviours:

\[
(i) \left( C_{11} C_{12} - C_{21} C_{22} - \sqrt{(1 - C_{12}^2)(1 - C_{11}^2)} \right) = 0
\]

\[
(ii) \left( C_{xy} C_{x'y'} - C_x C_y \right) \geq 0
\]

Then, from the numerically obtained extremal behaviours, we evaluate the maximum achievable amount of Genuine Randomness for the different values of \( P_{Hardy} \) (see Fig. 5) by solving the following optimisation problem.

\[
R_{DD}^{max} = -\log_2 \left[ \min_{X_i, Y_j} \max_{\vec{P}_{ext}} G(\vec{P}_{ext}, X_i, Y_j) \right]
\]

such that

\[
P_{Hardy} > 0
\]

We find that the maximum Genuine Randomness that can be achieved by the extremal Hardy behaviours is given by 1.6774 bits corresponding to \( P_{Hardy}^{obs} = 0.0642 \).

Note that we obtain the above mentioned results by applying the numerical technique discussed in Appx. E based on suitably defining the objective function. In this computation, in order to estimate the numerical accuracy of our findings, we have used as the testbed the analytical result that the behaviour having the maximum value of \( P_{Hardy} = 0.49511 \) leads to its self-testing [67], and thus is a quantum extremal behaviour [34]. We use this result of extremality of the maximal-Hardy behaviour to estimate the accuracy up to which the criteria given by Eq. (F2) are satisfied.

2. **Computation of \( R_{DD}^{max} \) by characterising the quantum extremal behaviours using the CL relations**

From the 24 extremal distributions, it can be shown that out of 8 PR-Box behaviours, only PR-Box 1 leads to the CL type
The curve shows the variation of the maximum amount of Genuine Randomness ($R_{DD}^{max}$) with the concurrence of the pure entangled two-qubit states.

The curve shows the variation of the maximum achievable amount of Genuine Randomness ($R_{DD}^{max}$) corresponding to a specific range of concurrence values ($[0.9880, 0.9999]$).

It is to be noted that the variation of the quantity $R_{DD}^{max}$ is distinctly non-monotonic. Further, the maximum amount of $R_{DD}^{max}$ is seen to be 1.9995 bits corresponding to the concurrence 0.9999. Fig. (b) shows that 1.8549 bits of $R_{DD}^{max}$ is achieved for the concurrence 0.9880 followed by the value of $R_{DD}^{max}$ increasing to 1.9722 bits for the concurrence 0.9887. Next, $R_{DD}^{max}$ decreases to 1.8230 bits for the concurrence 0.9895. In the oscillating region of the curve, it is seen that there exists a number of pure non-maximally two-qubit entangled states having the concurrence values lying within the range $[0.9887, 0.9999]$ for which $R_{DD}^{max}$ is greater than or equal to 1.95 bits.

The points in the plot show the results for the maximum amount of Genuine Randomness ($R_{DD}^{max}$) numerically evaluated by characterising the quantum extremal behaviours corresponding to the different values of Hardy parameter ($P_{Hardy}$). It is seen that the maximum of 1.6774 bits of $R_{DD}^{max}$ is obtained for $P_{Hardy} = 0.0642$ which is much less than its maximum value, ($P_{Hardy})_{max} = 0.0902$. ($P_{Hardy})_{max}$ = 0.0902 corresponds to 1.3884 bits of $R_{DD}^{max}$. These results, therefore, show the quantitative non-equivalence between $R_{max}^{DD}$ and $P_{Hardy}$.

The points in the plot show the results for the maximum amount of Genuine Randomness ($R_{max}^{DD}$) numerically evaluated by characterising the quantum extremal behaviours corresponding to the different values of CL parameter ($P_{CL}$). It is seen that the maximum of 1.9998 bits of $R_{max}^{DD}$ is obtained for $P_{CL} = 0.0701$ which is much less than its maximum value, ($P_{CL})_{max} = 0.1078$. ($P_{CL})_{max}$ = 0.1078 corresponds to 1.9635 bits of $R_{max}^{DD}$. These results, therefore, show the quantitative non-equivalence between $R_{max}$ and $P_{CL}$.

nonlocality, satisfying all the CL relations given by Eqs. (10-12). Out of the 16 LD behaviours, using the particular CL relations given by Eqs. (10-12), 9 LD behaviours (LD1, LD4, LD6, LD8, LD11, LD12, LD14, LD15, LD16) can be shown to be local deterministic. Like the Hardy case, the other 7 LD behaviours can be shown to be local deterministic by using other equivalent forms of the CL relations. Similarly, the 7 PR box behaviours can be shown to be nonlocal.

It, therefore, follows that any NS behaviour satisfying the CL relations given by Eqs. (10-12) can be expressed as a convex mixture of 9 LD and one PR box behaviours. Then, the observable NS behaviours satisfying the CL relations are...
given by

\[ P_{\text{CL}}^{\text{obs}} = \lambda_1 R_1 + \lambda_4 L_4 + \lambda_6 L_6 + \lambda_8 L_8 + \lambda_{11} L_{11} + \lambda_{12} L_{12} + \lambda_{14} L_{14} + \lambda_{15} L_{15} + \lambda_{16} L_{16} \]  

where \( 0 \leq \lambda_i \leq 1 \), \( \lambda_1 + \lambda_4 + \lambda_6 + \lambda_8 + \lambda_{11} + \lambda_{12} + \lambda_{14} + \lambda_{15} + \lambda_{16} = 1 \). Note that the value of the CL parameter is \( P_{\text{CL}}^{\text{obs}} \in (P_{\text{CL}}^{\text{obs}}) = -\lambda + \lambda_6 + \lambda_{11} + \lambda_{16} \).

Similar to the numerical procedure followed in the Hardy case, by obtaining the quantum extremal behaviours, here also we evaluate the the maximum achievable amount of Genuine Randomness for the different values of \( P_{\text{CL}} \) (see Fig. 6). We find that the maximum Genuine Randomness that can be achieved by the extremal CL behaviours is given by 1.9997 bits corresponding to \( P_{\text{CL}}^{\text{obs}} = 0.0701 \).

G. Relating the Bell-CHSH value with the relevant Hardy (\( P_{\text{Hardy}} \)) and Cabello-Liang (\( P_{\text{CL}} \)) parameters

**Proposition**—For any no-signalling probability distribution \( \{ P(a, b | X, Y) \} \) such that \( a, b \in \{ \pm 1 \} \) and \( i, j \in \{1, 2\} \), the Bell-CHSH expression

\[ B = \langle X_i Y_j \rangle = \sum_{a,b} ab P(a, b | X, Y) \]  

is equal to \( 2 + 4(p_1 - p_2 - p_3 - p_4) \), where

\[ p_1 = P(+1, +1 | X_1 Y_1), \]
\[ p_2 = P(+1, -1 | X_2 Y_1), \]
\[ p_3 = P(-1, +1 | X_1 Y_2), \]
\[ p_4 = P(-1, -1 | X_2 Y_2), \]

are the four joint probabilities appearing in the Hardy and CL relations.

**Proof**: For any \( i, j \in \{1, 2\} \) the correlation function is given by

\[ \langle X_i Y_j \rangle = \sum_{a,b} ab P(a, b | X, Y) \]  

The Bell-CHSH expression is given by

\[ B = \sum_{a,b,i,j} (-1)^{ij} ab P(a, b | X, Y) \]  

Now, using the normalization conditions given by

\[ \sum_{a,b} P(a, b | X, Y) = 1 \]  

one can write

\[ B = 2 \left[ 1 + \sum_{a,b,i,j} (-1)^{ij} P(a, b | X, Y) - \sum_{a,b,i,j} (-1)^{ij} P(a, b | X, Y) \right] \]  

Next, considering the no-signalling conditions \( P(a | X, Y) = P(a | X, Y) \) and \( P(b | X, Y) = P(b | X, Y) \), we express the marginal probabilities \( P(a | X, Y) \) and \( P(b | X, Y) \) in terms of the respective joint probability distributions with the suitable choices of \( a, b \in \{ \pm 1 \} \), \( X \in \{ X_1, X_2 \} \), and \( Y \in \{ Y_1, Y_2 \} \). We then get the following four no-signalling conditions

\[ (1) \ P(+1, +1 | X_1 Y_1) + P(+1, -1 | X_1 Y_2) \]
\[ = P(+1, +1 | X_1 Y_2) + P(+1, -1 | X_1 Y_2), \]
\[ (2) \ P(+1, -1 | X_1 Y_1) + P(-1, -1 | X_1 Y_1) \]
\[ = P(+1, -1 | X_1 Y_1) + P(-1, -1 | X_1 Y_1), \]
\[ (3) \ P(+1, +1 | X_1 Y_1) + P(-1, +1 | X_1 Y_1) \]
\[ = P(+1, +1 | X_1 Y_2) + P(-1, +1 | X_1 Y_2), \]
\[ (4) \ P(-1, +1 | X_1 Y_2) + P(-1, -1 | X_1 Y_2) \]
\[ = P(-1, +1 | X_1 Y_2) + P(-1, -1 | X_1 Y_2). \]

On summing the above equations, we obtain

\[ P(+1, +1 | X_1 Y_1) + P(+1, -1 | X_1 Y_2) \]
\[ + P(-1, -1 | X_1 Y_1) + P(-1, -1 | X_1 Y_2) \]
\[ = P(+1, +1 | X_1 Y_2) + P(-1, -1 | X_1 Y_2), \]
\[ + P(-1, +1 | X_1 Y_1) + P(-1, -1 | X_1 Y_2) \]
\[ = P(+1, +1 | X_1 Y_2) + P(-1, -1 | X_1 Y_2) \]

which implies

\[ P(-1, -1 | X_1 Y_1) = P(+1, -1 | X_1 Y_2) \]
\[ + P(+1, -1 | X_1 Y_1) + P(-1, -1 | X_1 Y_2) \]
\[ - P(+1, +1 | X_1 Y_2) - P(-1, +1 | X_1 Y_2). \]

Using Eq. (G7), the Bell-CHSH value given by Eq. (G4) can then be recast as follows

\[ B = 2 + 4(P(+1, +1 | X_1 Y_1) - P(-1, -1 | X_1 Y_2)) \]
\[ - P(+1, -1 | X_1 Y_2) + P(-1, +1 | X_1 Y_2) \]
\[ = 2 + 4(p_1 - p_2 - p_3 - p_4) \]  

---

[1] L. Masanes, A. Acín, and N. Gisin, General properties of nonsignaling theories, Phys. Rev. A 73, 012112 (2006).
[2] R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450 (2012).
[3] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by bell’s theorem, Nature 464, 1021 (2010).
[4] A. Acín, S. Massar, and S. Pironio, Randomness versus nonlocality and entanglement, Phys. Rev. Lett. 108, 100402 (2012).
[5] L. Hardy, Quantum mechanics, local realistic theories, and lorentz-invariant realistic theories, Phys. Rev. Lett. 68, 2981
[50] N. Gisin, Bell inequalities: many questions, a few answers (2007), arXiv:quant-ph/0702021 [quant-ph].

[51] N. Gisin, Bell inequality for arbitrary many settings of the analyzers, Physics Letters A 260, 1 (1999).

[52] N. Brunner and N. Gisin, Partial list of bipartite bell inequalities with four binary settings, Physics Letters A 372, 3162 (2008).

[53] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. 86, 419 (2014).

[54] P. M. Pearle, Hidden-variable example based upon data rejection, Phys. Rev. D 2, 1418 (1970).

[55] S. L. Braunstein and C. M. Caves, Wringing out better bell inequalities, Annals of Physics 202, 22 (1990).

[56] A. Peres, ed., Bell’s theorem, in Quantum Theory: Concepts and Methods (Springer Netherlands, Dordrecht, 2002) pp. 148–186.

[57] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond bell’s theorem, in Bell’s Theorem, Quantum Theory and Conceptions of the Universe, edited by M. Kafatos (Springer Netherlands, Dordrecht, 1989) pp. 69–72.

[58] D.-L. Deng, Z.-S. Zhou, and J.-L. Chen, Relevant multi-setting tight bell inequalities for qubits and qutrits, Annals of Physics 324, 1996 (2009).

[59] D. Avis, H. Imai, and T. Ito, On the relationship between convex bodies related to correlation experiments with dichotomic observables, Journal of Physics A: Mathematical and General 39, 11283 (2006).

[60] D. Boschi, S. Branca, F. De Martini, and L. Hardy, Ladder proof of nonlocality without inequalities: Theoretical and experimental results, Phys. Rev. Lett. 79, 2755 (1997).

[61] S.-H. Jiang, Z.-P. Xu, H.-Y. Su, A. K. Pati, and J.-L. Chen, Generalized hardy’s paradox, Phys. Rev. Lett. 120, 050403 (2018).

[62] E. A. Fonseca and F. Parisio, Measure of nonlocality which is maximal for maximally entangled qutrits, Phys. Rev. A 92, 030101 (2015).

[63] V. Lipinska, F. J. Curchod, A. Mättar, and A. Acín, Towards an equivalence between maximal entanglement and maximal quantum nonlocality, New Journal of Physics 20, 063043 (2018).

[64] fmincon, mathworks support, MathWorks Support ().

[65] Tolerances and stopping criteria, MathWorks Support ().

[66] How globalsearch and multistart work, MathWorks Support ().

[67] R. Rabelo, L. Y. Zhi, and V. Scarani, Device-independent bounds for hardy’s experiment, Phys. Rev. Lett. 109, 180401 (2012).