

Tilted Hardy paradoxes for device-independent randomness extraction

Shuai Zhao¹, Ravishankar Ramanathan¹, Yuan Liu¹, and Paweł Horodecki^{2,3}

¹Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong

²International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland

³Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland

The device-independent paradigm has had spectacular successes in randomness generation, key distribution and self-testing, however most of these results have been obtained under the assumption that parties hold trusted and private random seeds. In efforts to relax the assumption of measurement independence, Hardy's non-locality tests have been proposed as ideal candidates. In this paper, we introduce a family of tilted Hardy paradoxes that allow to self-test general pure two-qubit entangled states, as well as certify up to 1 bit of local randomness. We then use these tilted Hardy tests to obtain an improvement in the generation rate in the state-of-the-art randomness amplification protocols for Santha-Vazirani (SV) sources with arbitrarily limited measurement independence. Our result shows that device-independent randomness amplification is possible for arbitrarily biased SV sources and from almost separable states. Finally, we introduce a family of Hardy tests for maximally entangled states of local dimension 4, 8 as the potential candidates for DI randomness extraction to certify up to the maximum possible $2 \log d$ bits of global randomness.

1 Introduction

One of the most fundamental features of quantum mechanics is the presence of correlations that cannot be explained by any local hidden variable theory [1, 2]. Apart from being of fundamental interest, this phenomenon of Bell non-locality has led to the powerful idea of device-independent (DI) quantum key distribution [3, 4], randomness generation [5, 6] and certification of quantum systems [7, 8].

The strength of the device-independent paradigm is that no assumption on the nature of the systems subject to measurement needs to be made. Indeed, one may simply consider the systems participating in the Bell experiment to be (two or more) black boxes that parties provide an input to and obtain an outcome from, not taking into account the complex details of the physical implementation at all. The observation of a Bell inequality violation then allows one to make nontrivial deductions about the nature of the systems under study, such as the presence of entanglement, or a lower bound on the system dimension, or the non-determinism of the measurement outputs. In the extreme case, observation

Ravishankar Ramanathan: ravi@cs.hku.hk

Yuan Liu: yuan59@connect.hku.hk

of maximum violation of certain Bell inequalities even permits the device-independent certification (*self-testing*) [8, 9] of the quantum state and measurements performed on the system, i.e., their uniqueness up to irrelevant local equivalences.

Such self-testing has obvious advantages over traditional certification methods such as those based on quantum tomography [10], and a lot of attention has therefore been devoted recently to designing Bell inequalities suited for self-testing different entangled quantum states. However, DI certification based on the violation of Bell inequalities nevertheless still relies upon some assumptions, the foremost being the requirements of no-signaling between the local systems (typically enforced by space-like separation), and that the measurements on the local systems are chosen freely and randomly.

This latter requirement known as measurement independence is typically justified by the assumption that the parties hold independent and trusted random number generators (i.e., trusted and private random seeds). However, this assumption is clearly incongruous with the very framework of device-independence, wherein all devices held by the honest parties may have been tampered with, or even provided by, an adversary. To elaborate, consider the adversarial scenario wherein an adversary Eve has had access to the very devices used by the honest parties in the protocol. If such an adversary was able to influence the local random number generators held by the parties, then she would be able to ensure that the parties only hold imperfect seeds (about which Eve has some side information). In the extreme case, Eve may even be able to prepare devices that only operate according to local hidden variable behaviors, and yet appear non-local to the parties due to the imperfection of their seeds. Indeed, when no measurement independence at all is available, one cannot demonstrate any non-locality. It is therefore of vital importance to extend the studies on device-independent certification (as well as other tasks such as key distribution and random number generation) to the scenario in which only limited (arbitrarily small) measurement independence is available [11, 12, 13, 14, 15, 16].

As a model of an imperfect seed, one may consider the ε -SV source [17], a model of a biased coin where the individual coin tosses are not independent but rather the bits R_i produced by the source obey $\frac{1}{2} - \varepsilon \leq P(R_i = 0 | R_{i-1}, \dots, R_1, W) \leq \frac{1}{2} + \varepsilon$. The parameter $0 \leq \varepsilon < \frac{1}{2}$ described the reliability of the source, with $\varepsilon = 0$ being the ideal random seed and W denotes any side information, possibly held by an adversary. It is worth remarking that more general ‘min-entropy’ sources are also possible, wherein only a lower bound on the min-entropy (the negative logarithm of the maximum probability of any output string) produced by the source is assumed.

With regards to the task of self-testing, an important result was the formulation of a general class of Bell inequalities known as the tilted-CHSH inequalities suitable for self-testing general pure two-qubit entangled states. Specifically, in the simplest bipartite Bell scenario with two binary observables A_0, A_1 for Alice and two binary observables B_0, B_1 for Bob, the following family of tilted CHSH operators was introduced in [18]

$$T_\beta = \beta A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1, \quad (1)$$

where $\beta \in [0, 2)$ is a parameter with $\beta = 0$ corresponding to the well-known CHSH operator. The maximum value of this tilted CHSH quantity in classical theories is easily seen to be $2 + \beta$. In [19], it was shown that the optimal quantum value of $T_\beta^{\max} = \sqrt{8 + 2\beta^2}$ can only be achieved when specific reference observables A_x, B_y are measured on the state $|\psi_\theta\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$ with $\theta = \frac{1}{2} \arctan \sqrt{\frac{2}{\beta^2} - \frac{1}{2}}$. Specifically, it was shown that the observation of the expectation value $\langle T_\beta \rangle \geq T_\beta^{\max} - \epsilon$ for the tilted CHSH operator by measuring a physical state $|\psi'\rangle$ with observables A'_x and B'_y implies the existence of an isometry $\Phi = \Phi_A \otimes \Phi_B$ and a state $|\text{junk}\rangle$ such that $\|\Phi(A'_x \otimes B'_y |\psi'\rangle) - |\text{junk}\rangle \otimes (A_x \otimes B_y) |\psi\rangle\| \leq \epsilon'$,

where $x, y \in \{-1, 0, 1\}$ (with subscript -1 indicating the identity operator) and where $e' = O(\sqrt{e})$. The family of tilted CHSH inequalities has since played a crucial role in several aspects, including (a) showing the quantitative inequivalence between the amount of non-locality and the amount of certified randomness [18], (b) being the building block that enabled the self-testing of all bipartite pure (two-qudit) entangled states [20], (c) enabling the formulation of a device-independent quantum random number generation (DIQRNG) protocol that only requires a sublinear amount of quantum communication [21] (i.e., produces n bits of output randomness with a total of $\Omega(n^k \log n)$ ebits where $\frac{7}{8} < k < 1$), and (d) unbounded randomness certification from a single pair of entangled qubits using a sequence of measurements [22].

A natural question is whether a corresponding family of inequalities can be formulated in the scenario of (arbitrarily) limited measurement independence so that the above (and further such DI) results can be achieved in the setting when the parties are not assumed to possess perfect random seeds. In section 2, we answer this question in the positive by formulating a class of tilted Hardy paradoxes that allow to self-test general pure two-qubit entangled states (except the maximally entangled state). As shown in [23], tests of Hardy paradoxes (in an equivalent formulation as ‘measurement-dependent’ locality inequalities) allow for arbitrary small measurement independence making them ideal candidates for device-independent tasks when only weak seeds are available. In this section 2, we also derive expressions for the amount of randomness that can be certified from the maximum violation of the tilted Hardy tests in terms of the *guessing probability* by an adversary holding a quantum system that is potentially correlated to the devices involved in the test. In section 3, we compute the guessing probability in the noisy scenario of non-maximal violation, here distinguishing between two cases: (a) a scenario of colored noise where the ‘zero’ constraints in the tilted Hardy paradox are satisfied but the non-zero Hardy probability is non-maximal, and (b) a scenario of white noise where we consider the non-maximal violation of a Bell expression derived from the tilted Hardy paradox. While an amount of local randomness up to the maximum possible value of 1 bit can be certified by the tilted Hardy tests, the amount of global randomness is limited to a value of approximately 1.6806 bits. Nevertheless, we show that the derived results present an improvement in generation rate over the state-of-the-art protocols of randomness amplification against quantum adversaries. Meanwhile, we slightly change the coefficients of the expression of Hardy probability and show that the derived Bell expression provides a robust self-testing statement of the corresponding optimal quantum system. In section 3.3, we derive the analytical expression for the guessing probability in the scenario of an adversary that is allowed to prepare bipartite devices for the honest parties constrained only by the no-signaling principle, a result that also finds application in the state-of-the-art protocols for randomness amplification against no-signaling adversaries [15]. Finally, in section 4, we present a class of Hardy paradoxes with more inputs and outputs that potentially allow to certify the maximal amount of global randomness of $2 \log d$ bits for dimensions $d = 4, 8$. To do this, we exploit a recently discovered connection between Hardy paradoxes and substructures of Kochen Specker proofs termed 01-gadgets [24]. We conclude with a discussion on future research directions.

2 A family of Tilted Hardy paradoxes: Self-testing general pure two-qubit entangled states

We work in the simplest bipartite Bell scenario with Alice and Bob performing measurements corresponding to two binary observables each. Specifically, Alice and Bob provide

inputs $x \in \{0, 1\}$ and $y \in \{0, 1\}$ to their respective device, and obtain respective binary outcomes $a \in \{0, 1\}$ and $b \in \{0, 1\}$. The behavior of the device is described by a set of probability distributions $\{P_{A,B|X,Y}(a, b|A_x, B_y)\}$ where $P_{A,B|X,Y}(a, b|A_x, B_y)$ denotes the probability to obtain outputs a, b conditioned on measurement inputs x, y for Alice and Bob. We define a family of tilted Hardy tests in this scenario as given by the following set of constraints:

$$\begin{aligned} P_{A,B|X,Y}(a, b|A_x, B_y) &= 0, \forall (a, b|x, y) \in S_{Hz} := \{(0, 1|0, 1), (1, 0|1, 0), (0, 0|1, 1)\} \\ P_{Hardy}^w &:= P_{A,B|X,Y}(0, 0|A_0, B_0) + w \cdot P_{A,B|X,Y}(1, 1|A_0, B_0) > \max(0, w) \end{aligned} \quad (2)$$

where $w \in (-\frac{1}{4}, 1)$ is a parameter, and $\max(0, w)$ is the maximum value of the Hardy probability P_{Hardy}^w in any classical local hidden variable (LHV) theory. This latter bound can be seen from the fact that the enforcement of the three Hardy ‘zero’ constraints $P_{A,B|X,Y}(a, b|A_x, B_y) = 0$ for $(a, b|x, y) \in S_{Hz}$ implies as in the original Hardy paradox that $P_{A,B|X,Y}(0, 0|A_0, B_0) = 0$ and in any LHV model $P_{A,B|X,Y}(1, 1|A_0, B_0) \leq 1$. As we shall see, quantum theory allows for a value of P_{Hardy}^w larger than this classical bound. Indeed when $w = 0$, we recover the original Hardy paradox [25] for which it is well-known that $P_{Hardy}^{w=0} = P_{A,B|X,Y}(0, 0|A_0, B_0)$ can achieve a maximal value of $\frac{5\sqrt{5}-11}{2}$ in quantum theory. Furthermore, as shown in [26], this quantum behavior is achieved by a unique two-qubit state and measurements up to local isometries.

As anticipated in the Introduction, the motivation for introducing the tilted Hardy paradoxes is that as shown in [23], Hardy paradoxes can be used to certify quantum non-locality even in scenarios when the measurement settings are not chosen completely freely. Specifically, in any scenario where the parties choose their measurement settings using weak sources of randomness that obey $l \leq P_{X,Y}(x, y|\lambda) \leq h$ for $l, h \in (0, 1)$, the tilted Hardy test in Eq. (2) can be converted into a Measurement-Dependent Locality (MDL) inequality as:

$$\begin{aligned} l \cdot [P_{Hardy}^w - \max(0, w)] P_{X,Y}(A_0, B_0) - h \cdot [P_{X,Y}(A_0, B_1) P_{A,B|X,Y}(0, 1|A_0, B_1) \\ + P_{X,Y}(A_1, B_0) P_{A,B|X,Y}(1, 0|A_1, B_0) + P_{X,Y}(A_1, B_1) P_{A,B|X,Y}(0, 0|A_1, B_1)] \leq 0, \end{aligned} \quad (3)$$

where $P_{X,Y}(A_x, B_y)$ denotes the probability of choosing inputs x, y . Furthermore, as the following Prop. 1 shows (we defer its proof to Appendix A), the tilted Hardy tests can be used to self-test every entangled pure two-qubit state other than the maximally entangled state.

Proposition 1. *Suppose that the Hardy zero constraints $P_{A,B|X,Y}(0, 1|A_0, B_1) = P_{A,B|X,Y}(1, 0|A_1, B_0) = P_{A,B|X,Y}(0, 0|A_1, B_1) = 0$ are satisfied. Then in any local hidden variable theory it holds that $P_{Hardy}^{w,LHV} \leq \max(0, w)$. On the other hand, quantum theory allows to achieve $P_{Hardy}^{w,Q} = \frac{(4w+5)\sqrt{4w+5}-(12w+11)}{2(w+1)} > P_{Hardy}^{w,LHV}$ for $w \in (-\frac{1}{4}, 1)$. Furthermore, up to local isometries, $P_{Hardy}^{w,Q}$ is uniquely achieved by the two-qubit state $|\psi_\theta\rangle = \cos(\frac{\theta}{2})|00\rangle - \sin(\frac{\theta}{2})|11\rangle$ with $\theta = \arcsin(3 - \sqrt{4w+5})$ and the measurements $\{A_0, A_1\}, \{B_0, B_1\}$ given as*

$$\begin{aligned} A_0 = B_0 &= \frac{-(2 + \sin \theta)(1 - \sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}} \cdot Z + \frac{-\sqrt{2} \sin \theta (\sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}} \cdot X, \\ A_1 = B_1 &= \frac{-(1 - \sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}} \cdot Z + \frac{\sqrt{2}(\sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}} \cdot X, \end{aligned} \quad (4)$$

where X and Z are the usual Pauli matrices.

Let us briefly observe that no loss of generality is accrued in considering the expression P_{Hardy}^w in Eq. (2) - when the three Hardy zero constraints are satisfied, P_{Hardy}^w constitutes a general (non-zero) Hardy expression, i.e., no additional gain is obtained by considering the quantum value of an expression such as

$$P_{Hardy} = \alpha_{0,0} P_{A,B|X,Y}(0,0|A_0, B_0) + \alpha_{0,1} P_{A,B|X,Y}(0,1|A_0, B_0) \\ + \alpha_{1,0} P_{A,B|X,Y}(1,0|A_0, B_0) + \alpha_{1,1} P_{A,B|X,Y}(1,1|A_0, B_0) \quad (5)$$

for arbitrary coefficients $\alpha_{i,j}$ with $i, j \in \{0, 1\}$. To see this, consider an arbitrary bipartite pure state $|\psi\rangle = \sum_k \lambda_k |k_A\rangle |k_B\rangle$, where $\{|k_A\rangle\}$ and $\{|k_B\rangle\}$ are basis sets of Hilbert spaces $\mathbf{H}_A$ and $\mathbf{H}_B$ respectively and $\lambda_k \geq 0$ are the corresponding Schmidt coefficients. First observe that Jordan's lemma allows for a reduction to the setting where Alice and Bob hold qubit systems, i.e., $\mathbf{H}_A = \mathbf{H}_B = \mathbb{C}^2$. Furthermore, when the Hardy zero constraints are satisfied, as shown in Appendix A, Alice and Bob's measurement observables are identical, i.e., $A_0 = B_0$ and $A_1 = B_1$ giving rise to the symmetry $P(0,1|A_0, B_0) = P(1,0|A_0, B_0)$. Under these conditions, the arbitrary Hardy expression $P_{Hardy} = \sum_{i,j=0,1} \alpha_{i,j} P_{A,B|X,Y}(i,j|A_0, B_0)$ reduces to

$$P_{Hardy} = \frac{\alpha_{0,1} + \alpha_{1,0}}{2} + \left(\alpha_{0,0} - \frac{\alpha_{0,1} + \alpha_{1,0}}{2} \right) P_{A,B|X,Y}(0,0|A_0, B_0) \\ + \left(\alpha_{1,1} - \frac{\alpha_{0,1} + \alpha_{1,0}}{2} \right) P_{A,B|X,Y}(1,1|A_0, B_0). \quad (6)$$

Removing the offset term $\frac{\alpha_{0,1} + \alpha_{1,0}}{2}$ and denoting the ratio of $\left(\alpha_{1,1} - \frac{\alpha_{0,1} + \alpha_{1,0}}{2} \right)$ and $\left(\alpha_{0,0} - \frac{\alpha_{0,1} + \alpha_{1,0}}{2} \right)$ as w reduces the general Hardy expression to P_{Hardy}^w .

The fact that the maximum violation of the tilted Hardy tests is realised by self-testing quantum behaviors implies that one may apply them in schemes to generate certified randomness starting from arbitrarily weak seeds (we elaborate on this in the coming sections). We may quantify the amount of global randomness obtained by the measurement of observables A_x and B_y on a state $|\psi\rangle \in \mathbf{H}_A \otimes \mathbf{H}_B$ through the guessing probability $G_{\psi, A_x, B_y} = \max_{a,b} P_{A,B|X,Y}^{\psi}(a, b|A_x, B_y)$ where $P_{A,B|X,Y}^{\psi}(a, b|A_x, B_y)$ denotes the outcome probabilities obtained by measurements of A_x, B_y on $|\psi\rangle$. The corresponding amount of global randomness (in bits) is then given by the min-entropy $H_{\infty}(|\psi\rangle, A_x, B_y) = -\log_2 G_{\psi, A_x, B_y}$. Similarly, one can quantify the amount of local randomness through the guessing probability of marginal outcomes of each local party. One may then define the maximum global randomness certifiable from any input pair x, y the tilted Hardy tests for any given w as $H_{\infty}^{\text{global}} = \max_{x,y} H_{\infty}(|\psi_{\theta}\rangle, A_x, B_y)$ where $|\psi_{\theta}\rangle, A_x, B_y$ are given by the self-testing quantum behavior from Prop. 1 with $\theta = \arcsin(3 - \sqrt{4w + 5})$. Analogously, one can quantify the amount of local randomness obtained by the measurement of A_x or B_y , the symmetry of the measurement observables of Alice and Bob means that we obtain $H_{\infty}^{\text{local}} = \max_x H_{\infty}(|\psi_{\theta}\rangle, A_x) = \max_y H_{\infty}(|\psi_{\theta}\rangle, B_y)$. As the pure state $|\psi_{\theta}\rangle$ is uncorrelated with any third party's system, the maximal local and global randomness is against quantum eavesdroppers.

We calculate the maximum amount of certifiable local and global randomness from the tilted Hardy tests as:

$$H_{\infty}^{\text{local}} = H_{\infty}(|\psi_{\theta}\rangle, A_1) = H_{\infty}(|\psi_{\theta}\rangle, B_1) = 1 - \log_2 \left[1 + \cos \theta \frac{1 - \tan(\theta/2)}{1 + \tan(\theta/2)} \right] \quad (7)$$

where $\theta = \arcsin(3 - \sqrt{4w + 5})$ from Prop. 1, and

$$H_{\infty}^{\text{global}} = \begin{cases} 1 - \log_2 \left[\frac{(3 - \sqrt{4w + 5})^3}{(\sqrt{4w + 5} - 1)^2} \right] & -\frac{1}{4} < w \leq w_0 \\ 1 - \log_2 \left[\frac{8\sqrt{4w + 5} - 16}{(\sqrt{4w + 5} - 1)^2} \right] & w_0 < w \leq w_1 \\ 1 - \log_2 [3 - \sqrt{4w + 5}] & w_1 < w \leq \frac{1}{9} \\ 1 - \log_2 [2\sqrt{4w + 5} - 4] & \frac{1}{9} < w < 1 \end{cases} \quad (8)$$

where $w_0 = \frac{1}{4}[-5 + (3 + 4(\frac{2}{3(9 + \sqrt{177})})^{\frac{1}{3}} - (4 + \frac{4\sqrt{177}}{9})^{\frac{1}{3}})^2] \approx -0.1546$ and $w_1 = \frac{1}{4}[-5 + (3 + \frac{1}{3}(-4 + 10(\frac{2}{-11 + 3\sqrt{69}})^{\frac{1}{3}} - (12\sqrt{69} - 44)^{\frac{1}{3}})^2] \approx -0.1054$.

Note that the reason why $H_{\infty}^{\text{global}}$ is a piecewise function is that the maximum global randomness is achieved by different measurement inputs x, y for different values of w . We see that the tilted Hardy tests allow to certify up to 1 bit of local randomness in the limit as $w \rightarrow -\frac{1}{4}$ (as the state tends to a maximally entangled state). Similarly, one can obtain up to 1.6806 bits of global randomness for $w = w_0$. In [18], it was observed that the amount of certified randomness is an inequivalent resource to non-locality and entanglement, in that high global randomness (close to 2 bits) may be certified by the tilted CHSH inequality even when using states that are almost unentangled, with the corresponding quantum behaviors being close to the set of local hidden variable behaviors. A similar phenomenon can also be observed in the expression for the global randomness in Eq. (8). While the maximum global randomness is achieved at $w \approx -0.1546$, the largest separation between the quantum and the LHV set occurs at $w = 0$ (when $\sin \theta = 3 - \sqrt{5}$), and the optimal state is close to maximally entangled as $w \rightarrow -\frac{1}{4}$ (when $\sin \theta \rightarrow 1$).

Note that the above self-testing result of Proposition. 1 does not consider an SV-source input distribution per se, since the biased SV-source themselves only give bounds of each input probability $l \leq P_{X,Y}(x, y|\lambda) \leq h$, and in this case it is not possible to even determine the exact quantum value of the corresponding measurement-dependent-locality (MDL) inequality. However, if the input distribution is explicitly known, the tilted Hardy paradoxes can be modified into the MDL version of the tilted Hardy tests and then the corresponding self-testing statement can be derived correspondingly, such that every pure two-qubit entangled state (other than the maximally entangled state) can be self-tested under arbitrary limited of measurement dependence.

3 Applying the Tilted Hardy Test in device-independent randomness generation against Quantum adversaries

In the previous section, we have derived the optimal amount of randomness that can be certified when the maximal violation of the tilted Hardy test is observed for any value of the parameter $w \in (-\frac{1}{4}, 1)$. When using the Hardy paradox in an actual device-independent protocol to certify randomness against a quantum adversary (such as [27]), it is important to consider the noisy scenario of non-maximal violation. Specifically, we consider the three-party scenario of Alice, Bob and Eve holding a tripartite quantum state ρ_{ABE} belonging to the Hilbert spaces $\mathbf{H}_A \otimes \mathbf{H}_B \otimes \mathbf{H}_E$, i.e., Eve holds a quantum system that may be entangled with that held by Alice and Bob. Alice and Bob perform measurements chosen using some ϵ -SV source, observe a certain value in the Hardy test and attempt to generate randomness from their measurement outcomes for some specific setting (A_x, B_y) . Eve performs a single measurement with outcome $e \in \{0, 1\}^2$ which will constitute her guess of the measurement results of Alice and Bob for this setting.

Formally, Eve's guessing probability of Alice and Bob's outputs can be written as the maximization of

$$P_{guess}(A, B|A_x, B_y, E) = \sum_{a,b \in \{0,1\}} P_{A,B,E|X,Y}(a, b, (e = a, b)|A_x, B_y) \quad (9)$$

subject to some given constraints. Here $P_{A,B,E|X,Y}(a, b, e|A_x, B_y) = \text{Tr} [A_{a|x} \otimes B_{b|y} \otimes \Pi_e \rho_{ABE}]$ where $A_{a|x}$ and $B_{b|y}$ are the projectors corresponding to the outcomes a and b for Alice and Bob respectively, and Π_e denotes the projector corresponding to Eve's measurement outcome e . The min-entropy is denoted as $H_\infty(A, B|A_x, B_y, E) = -\log_2 P_{guess}(A, B|A_x, B_y, E)$. A similar expression holds when Eve attempts to guess the local outcomes of one of the parties alone.

We consider two noise models that we term (1) colored noise and (2) white noise - in the former, we consider the scenario where the observed behavior $\{P_{A,B|X,Y}\}$ stays on the boundary of the quantum set (i.e., the three Hardy zero constraints are satisfied, while the non-zero Hardy probability takes on some intermediate value between the local and the quantum maximum), while in the latter, we consider the scenario where the observed behavior $\{P_{A,B|X,Y}\}$ is in the interior of the quantum set (i.e., the honest parties simply observe some non-optimal value for a Bell expression derived from the Hardy test).

1. Colored Noise: In this case, we consider that Alice and Bob's reduced system ρ_{AB} satisfies the three Hardy zero constraints, while the P_{Hardy}^w is non-maximal, that is P_{Hardy}^w lies in the intermediate range between $\max(0, w)$ and $P_{Hardy}^{w,Q}$.
2. White Noise: In this case, we slightly change the coefficients of Hardy probability in Eq. (5) to $\alpha_{0,0} = 1, \alpha_{0,1} = \alpha_{1,0} = \frac{1-\alpha}{2}, \alpha_{1,1} = 0$, and consider that Alice and Bob's reduced system ρ_{AB} achieves some (non-maximal) value of the corresponding derived Bell expression (by subtracting the Hardy zero constraints from the non-zero Hardy probability):

$$\begin{aligned} I_\alpha^{Hardy} = & [P_{A,B|X,Y}(0, 0|A_0, B_0) + \frac{1-\alpha}{2} P_{A,B|X,Y}(0, 1|A_0, B_0) \\ & + \frac{1-\alpha}{2} P_{A,B|X,Y}(1, 0|A_0, B_0) - \max(0, \frac{1-\alpha}{2})] - [P_{A,B|X,Y}(0, 1|A_0, B_1) \\ & + P_{A,B|X,Y}(1, 0|A_1, B_0) + P_{A,B|X,Y}(0, 0|A_1, B_1)]. \end{aligned} \quad (10)$$

It is worth noting that a similar expression for $\alpha = 1$ (in which case we recover the original Hardy paradox and $I_{\alpha=1}^{Hardy}$ corresponds to the CHSH inequality) has found application in the state-of-the-art device-independent randomness amplification protocol against an adversary holding quantum side information [16].

3.1 Colored Noise

In this subsection, we show the guessing probability for the value of w that results in the largest min-entropy in the noiseless setting, i.e., we set $w = w_0$ (in this case we note that the randomness is certified from the input (A_0, B_0)). Suppose that Alice and Bob observe a value of the Hardy probability $P_{Hardy}^w =: p$ that lies between the classical value $\max(0, w_0) = 0$ and the quantum maximum $P_{Hardy}^{w=w_0,Q} = \frac{(4w_0+5)\sqrt{4w_0+5}-(12w_0+11)}{2(w_0+1)}$. We

compute the analytical bound of the guessing probability as a function of p for the input (A_0, B_0) (the detailed computation is deferred to Appendix B) as

$$P_{\text{guess}}(A, B|A_0, B_0, E) = \begin{cases} \frac{([P_{A,B|X,Y}(0,1|A_0, B_0)]_{\theta_2^{p^*, w_0}})^{-1}}{\widetilde{p^*}} \cdot p + 1, & 0 \leq p \leq p^*, \\ [P_{A,B|X,Y}(1,1|A_0, B_0)]_{\theta_1^{p, w_0}}, & p^* < p \leq P_{\text{Hardy}}^{w_0, Q}, \end{cases} \quad (11)$$

where $p^* \approx 0.01366$, $\widetilde{p^*} \approx 0.01563$, θ_i^{p, w_0} for $i = 1, 2$ are the two solutions of Eq. (26) for $P_{\text{Hardy}}^{w_0} = p$ when the three zero constraints are satisfied.

3.2 White Noise

In this subsection, we consider the scenario in which Alice and Bob's system ρ_{AB} achieves a non-maximal value of the Bell expression I_α derived from the tilted Hardy test. To simplify matters, we formulate this Bell expression in terms of the correlators $\langle A_x B_y \rangle = \sum_{a,b=0,1} (-1)^{a+b} P_{A,B|X,Y}(a,b|A_x, B_y)$, $\langle A_x \rangle = \sum_{a=0,1} (-1)^a P_{A|X}(a|A_x)$ (and similar for $\langle B_y \rangle$). To this end, let us subtract the three zero terms from the Hardy non-zero probability (5) (with coefficients $\alpha_{0,0} = 1, \alpha_{0,1} = \alpha_{1,0} = \frac{1-\alpha}{2}, \alpha_{1,1} = 0$):

$$\begin{aligned} I_\alpha^{\text{Hardy}} &= [P_{A,B|X,Y}(0,0|A_0, B_0) + \frac{1-\alpha}{2} P_{A,B|X,Y}(0,1|A_0, B_0) + \frac{1-\alpha}{2} P_{A,B|X,Y}(1,0|A_0, B_0) \\ &\quad - \max(0, \frac{1-\alpha}{2})] - [P_{A,B|X,Y}(0,1|A_0, B_1) + P_{A,B|X,Y}(1,0|A_1, B_0) + P_{A,B|X,Y}(0,0|A_1, B_1)] \\ &= \frac{\alpha \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle + (-\alpha - 1)}{4} - \max(0, \frac{1-\alpha}{2}) \\ &= \frac{1}{4} [\langle I_\alpha \rangle + (-\alpha - 1)] - \max(0, \frac{1-\alpha}{2}), \end{aligned} \quad (12)$$

where $I_\alpha := \alpha A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1$, which is termed as α -CHSH expression in Appendix C. And in Appendix C, We analytically compute the maximum values of this Bell expression I_α in quantum and classical theories, and show it provides a robust self-testing statement for the optimal quantum strategy. With the optimal quantum strategy, one can obtain $H_\infty^{\text{global}} = 2$ bits of global randomness when $\alpha = \frac{1}{2}$ (See Fig. 1 for details on the relation between the global randomness and violation of the inequality $I_{\alpha=\frac{1}{2}} \leq \frac{5}{2}$). It is in the form of I_α that Hardy tests find application in testing non-locality with arbitrarily limited measurement independence, using the so-called measurement-dependent locality (MDL) inequalities (see following Eq. (13) for our case)[23].

To elaborate, consider the scenario in which the measurement settings (x, y) are chosen using a weak seed such as an ϵ -SV source which obeys $l \leq P_{X,Y}(x, y|\lambda) \leq h$, where λ denotes any side information that may be held by an adversary about the source. Here $0 < l \leq h < 1$, and for the specific case of the ϵ -SV source, $l = (\frac{1}{2} - \epsilon)^2$ and $h = (\frac{1}{2} + \epsilon)^2$. The

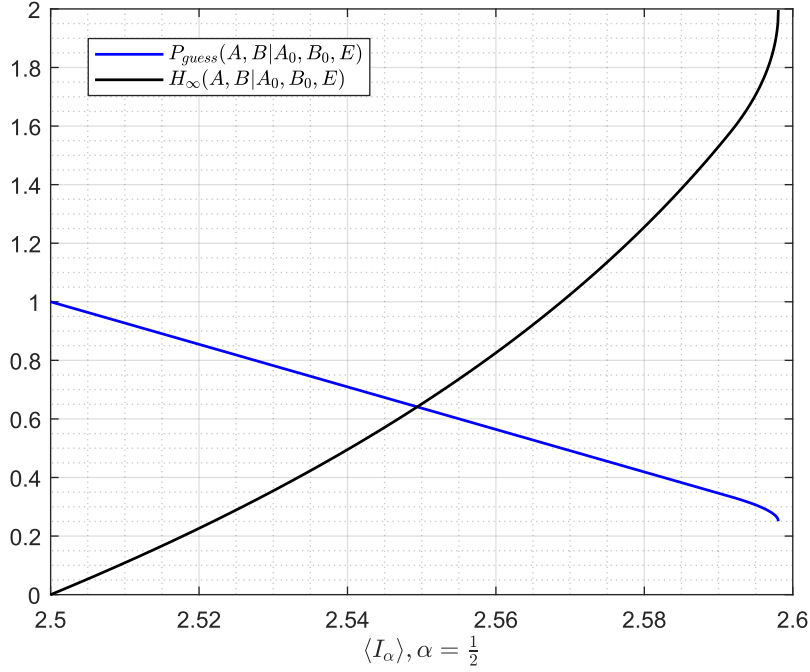


Figure 1: At the optimal point, $I_{\alpha=1/2}$, the inequality allows to certify up to $H_{\infty}(A, B|A_0, B_0, E) = 2$ bits global randomness. The guessing probability $P_{\text{guess}}(A, B|A_0, B_0, E)$ and corresponding Min-entropy $H_{\infty}(A, B|A_0, B_0, E)$ (bits per round) versus $I_{\alpha=1/2}$ calculated at the second level of the NPA hierarchy is shown.

expression I_{α} gives rise to the following tilted measurement-dependent-locality expression

$$\begin{aligned}
I_{\alpha}^{MDL} &= l[P_{A,B,X,Y}(0, 0, A_0, B_0) + \frac{1-\alpha}{2}P_{A,B,X,Y}(0, 1, A_0, B_0) \\
&\quad + \frac{1-\alpha}{2}P_{A,B,X,Y}(1, 0, A_0, B_0) - \max(0, \frac{1-\alpha}{2})P_{X,Y}(A_0, B_0)] \\
&\quad - h[P_{A,B,X,Y}(0, 1, A_0, B_1) + P_{A,B,X,Y}(1, 0, A_1, B_0) + P_{A,B,X,Y}(0, 0, A_1, B_1)] \\
&\leq lh[P_{A,B|X,Y}(0, 0|A_0, B_0) + \frac{1-\alpha}{2}P_{A,B|X,Y}(0, 1|A_0, B_0) \\
&\quad + \frac{1-\alpha}{2}P_{A,B|X,Y}(1, 0|A_0, B_0) - \max(0, \frac{1-\alpha}{2})] \\
&\quad - hl[P_{A,B|X,Y}(0, 1|A_0, B_1) + P_{A,B|X,Y}(1, 0|A_1, B_0) + P_{A,B|X,Y}(0, 0|A_1, B_1)] \\
&= lh \cdot I_{\alpha}^{\text{Hardy}} = \frac{lh}{4}[\langle I_{\alpha} \rangle + (-\alpha - 1)] - lh \cdot \max(0, \frac{1-\alpha}{2})
\end{aligned} \tag{13}$$

with $\alpha \in (1/3, +\infty)$. The corresponding classical bound is readily seen to be $I_{\alpha}^{MDL} \stackrel{LHV}{\leq} 0$, and the quantum bound is directly obtained from the optimal quantum strategy for the Bell expression I_{α} in Eq. (12). From Eq. (13) we get:

$$\begin{aligned}
I_{\alpha}^{\text{Hardy}} &\geq \frac{I_{\alpha}^{MDL}}{lh}, \\
\langle I_{\alpha} \rangle &\geq 4 \left(\frac{I_{\alpha}^{MDL}}{lh} + \max(0, \frac{1-\alpha}{2}) \right) + (\alpha + 1).
\end{aligned} \tag{14}$$

By numerically calculating the guessing probability $P_{\text{guess}}(A_0, B_0|E)$ and corresponding min-entropy $H_{\infty}(A, B|A_0, B_0, E)$ versus the $\langle I_{\alpha} \rangle$ using the NPA hierarchy (of level 2), one

can then use them with the relation in Eq. (14) to bound the min-entropy versus I_α^{MDL} in the MDL scenarios. We show the three cases for $\alpha = \frac{1}{2}, \alpha = \frac{4}{5}$ and $\alpha = 1$ in Fig. 2(a), from which and the quantum-classical value gap we calculate in Appendix C, one can see there is a trade-off between the maximal randomness one can certify from the MDL inequality I_α^{MDL} and the robustness of this MDL inequality I_α^{MDL} . $I_{\alpha=\frac{1}{2}}^{MDL}$ gives the highest randomness (2 bits) but it is not very robust, and $I_{\alpha=1}^{MDL}$ is the most robust one in this whole family of MDL inequality. $I_{\alpha=\frac{4}{5}}^{MDL}$ is one choice that balances the randomness and robustness between these two extreme cases.

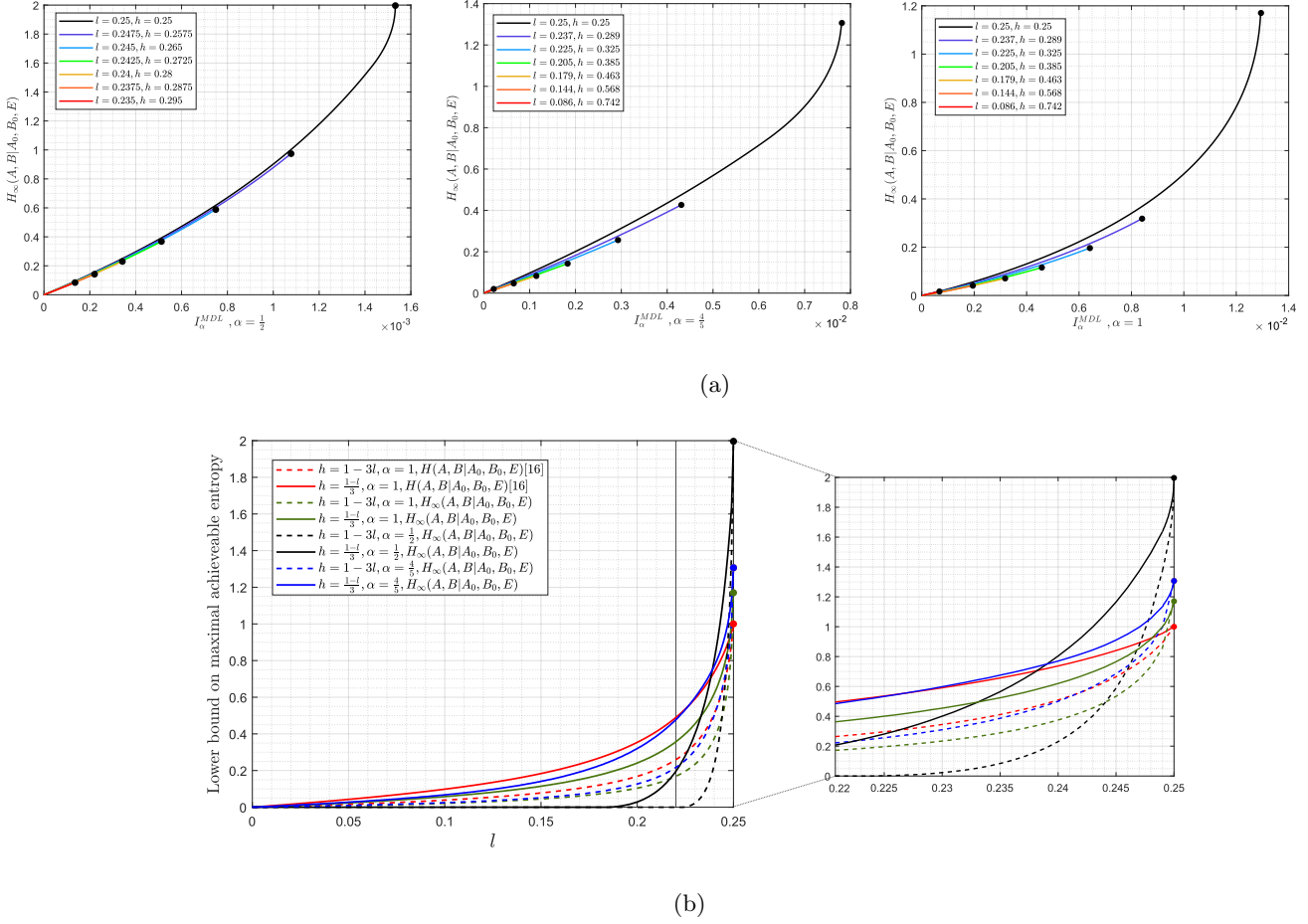


Figure 2: (a) Min-entropy bound in the MDL scenario versus I_α^{MDL} for $\alpha = \frac{1}{2}, \alpha = \frac{4}{5}, \alpha = 1$ with the given lower and higher bounds l, h of a weak SV-source. The black dots denote the lower bound on the maximal possible quantum value of I_α^{MDL} with the given lower and higher bounds l, h of the SV-source. (b) Lower bound on the maximal achievable entropy of I_α^{MDL} ($\alpha = \frac{1}{2}, \alpha = \frac{4}{5}, \alpha = 1$) versus the lower bound l of a weak SV-source. Here for the weak SV-source with fixed l , we consider two extreme cases of the input distribution (1) three settings are chosen with probability h and the remaining one is l , i.e. $l = 1 - 3h$ ($h = \frac{1-l}{3}$), and (2) three settings are chosen with probability l and the remaining one is h , i.e. $h = 1 - 3l$. As a comparison, we also plot the results in [16], in which the authors calculated the von Neumann entropy in the MDL scenario for $\alpha = 1$.

Since only the lower and higher bounds l, h of each input are known instead of the explicitly input distribution, the MDL inequality I_α^{MDL} is not fixed, thus the maximal quantum value cannot be calculated. Nevertheless one can derive a lower bound of the maximal quantum value of I_α^{MDL} by considering the worst-case input distribution, i.e.

$P_{X,Y}(A_0, B_0) = l$, and $P_{X,Y}(A_x, B_y) = h$ for $(x, y) \neq (0, 0)$, then we get:

$$\begin{aligned} I_\alpha^{MDL} &\geq l^2[P_{A,B|X,Y}(0, 0|A_0, B_0) + \frac{1-\alpha}{2}P_{A,B|X,Y}(0, 1|A_0, B_0) \\ &\quad + \frac{1-\alpha}{2}P_{A,B|X,Y}(1, 0|A_0, B_0) - \max(0, \frac{1-\alpha}{2})] - h^2[P_{A,B|X,Y}(0, 1|A_0, B_1) \\ &\quad + P_{A,B|X,Y}(1, 0|A_1, B_0) + P_{A,B|X,Y}(0, 0|A_1, B_1)] =: \tilde{I}_\alpha^{MDL} \end{aligned} \quad (15)$$

We use the NPA hierarchy of level 2 to numerically calculate the maximal quantum value of $\tilde{I}_\alpha^{MDL}$ which is the lower bound of the maximal quantum value of I_α^{MDL} . In Fig. 2(b), we then use this lower bound of I_α^{MDL} to show the lower bound on the maximal achievable min-entropy of I_α^{MDL} for $\alpha = \frac{1}{2}, \alpha = \frac{4}{5}, \alpha = 1$ versus the lower bound l of the SV-source, in which for a fixed l , we consider two extreme cases of the input distribution (1) three settings are chosen with probability h and the remaining one is l , i.e. $l = 1 - 3h$ ($h = \frac{1-l}{3}$), and (2) three settings are chosen with probability l and the remaining one is h , i.e. $h = 1 - 3l$.

It is worth noting that the randomness calculated for $I_{\alpha=1}^{MDL}$ found direct application in the state-of-the-art device-independent protocol for randomness amplification of arbitrarily weak seeds against adversaries holding quantum side information [16]. We illustrate the usefulness of the tilted Hardy test in randomness amplification by showing that an improvement in the generation rate of the DI protocol in [16] can be achieved by considering the tilted Hardy tests for $\alpha \neq 1$. Specifically, for $\alpha = \frac{1}{2}$ global randomness of up to $H_\infty(A, B|A_0, B_0, E) = 2$ bits can be certified as compared to the corresponding value of ≈ 1.23 bits from the CHSH expression ($\alpha = 1$) used in [18, 16]. However, the robustness performance for $\alpha = \frac{1}{2}$ is not very good as seen in Fig. 2(b). The robustness property for $\alpha = \frac{4}{5}$ is comparable with $\alpha = 1$, and from Fig. 2(b) we see that the certified min-entropy at $I_{\alpha=\frac{4}{5}}^{MDL}$ exceeds that derived for $I_{\alpha=1}^{MDL}$ for the whole range of $l \in [0, \frac{1}{4}]$ in either case. Therefore, plugging this min-entropy per round into the state-of-the-art DI protocol against quantum adversaries in [16] leads to a concomitant improvement in the generation rate of that protocol.

3.3 The guessing probability of a classical adversary allowed to prepare arbitrary no-signaling boxes for Alice and Bob

In this section, we compute the upper bound of the guessing probability of a classical adversary allowed to prepare arbitrary no-signaling boxes $P_{A,B|X,Y}$ in the scenario where Alice and Bob observe some (noisy) value $I_\alpha^{MDL}(P_{A,B|X,Y}) = \delta$. This scenario has direct applicability to the fully general scenario of arbitrary no-signaling adversaries, i.e., in the scenario of arbitrary tripartite no-signaling boxes $P_{A,B,E|X,Y,Z}$ with a concomitant loss in the generation rate as shown in [14].

Proposition 2. *Suppose that the honest parties observe a value $I_\alpha^{MDL}(P_{A,B|X,Y}) = \delta$ for the MDL quantity defined in (13) using a SV-source with $l \leq P_{X,Y}(x, y|\lambda) \leq h, \forall x, y \in \{0, 1\}$. Then for any pair of inputs x, y and outcomes a, b , their shared box satisfies*

$$\begin{aligned} P_{A,B|X,Y}(a, b|A_x, B_y) &\leq 1 - \frac{\delta}{lh\alpha} & \alpha \in (\frac{1}{3}, 1] \\ P_{A,B|X,Y}(a, b|A_x, B_y) &\leq 1 - \frac{\delta}{lh} & \alpha \in (1, +\infty) \end{aligned} \quad (16)$$

The proof of this proposition can be found in Appendix D. As mentioned earlier, the above bound finds direct applicability in the state-of-the-art protocol for randomness amplification of arbitrary ϵ -SV sources against general no-signaling adversaries. An optimization

over α and the amount of shared entanglement is then required to identify the best protocol for randomness amplification against no-signaling adversaries in terms of these two parameters.

4 Achieving Global randomness of $2 \log d$ bits with arbitrarily limited measurement independence

In this section, we present candidate Hardy paradoxes that potentially allow for the certification of the maximal amount of $H_\infty^{\text{global}} = 2 \log d$ bits of global randomness for quantum systems of local Hilbert space dimensions 2, 4 or 8. The candidate Hardy test for systems of local dimension 2 is the well-known ladder Hardy test [30] while the candidate Hardy tests for systems of dimensions 4, 8 are novel constructions based on a connection to sub-structures of Kochen-Specker tests in [31].

We first recall the Ladder version of the Hardy test. Here, Alice and Bob perform measurements corresponding to $N+1$ inputs $x, y \in \{0, 1, \dots, N\}$ and obtain binary outputs $a, b \in \{0, 1\}$ respectively. The Ladder Hardy test is comprised of $2N+1$ Hardy zero constraints:

$$\begin{aligned} P_{A,B|X,Y}(0, 1|A_k, B_{k-1}) &= 0 & \forall k \in \{1, \dots, N\} \\ P_{A,B|X,Y}(1, 0|A_{k-1}, B_k) &= 0 & \forall k \in \{1, \dots, N\} \\ P_{A,B|X,Y}(0, 0|A_0, B_0) &= 0 \end{aligned} \quad (17)$$

and the (non-zero) Hardy probability is $P_{\text{Hardy}} = P_{A,B|X,Y}(0, 0|A_N, B_N)$. In classical (LHV) theories, the $2N+1$ Hardy constraints imply that the Hardy probability is zero, i.e., $P_{\text{Hardy}} = 0$. However, quantum theory allows to reach $P_{\text{Hardy}} \rightarrow \frac{1}{2}$ under the following optimal quantum strategy [32]. Alice and Bob share the two-qubit state $|\psi\rangle = \alpha|00\rangle - \beta|11\rangle$, where α, β are parameters depending on N with $|\alpha|^2 + |\beta|^2 = 1$, we denote their ratio as $t = \frac{\alpha}{\beta}$. The projectors for the two parties correspond to $\{|A_k^0\rangle = \cos a_k|0\rangle + \sin a_k|1\rangle, |A_k^1\rangle = -\sin a_k|0\rangle + \cos a_k|1\rangle\}$ and $\{|B_k^0\rangle = \cos b_k|0\rangle + \sin b_k|1\rangle, |B_k^1\rangle = -\sin b_k|0\rangle + \cos b_k|1\rangle\}$ respectively, where $a_k, b_k \in [0, 2\pi)$ are the angles for Alice and Bob's k -th measurement. For the state satisfying all the Hardy constraints and achieving the optimal Hardy probability, one can calculate the probability distributions for any measurement setting x, y as

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_x, B_y) &= \frac{t^2}{1+t^2} \frac{(1 - (-1)^{2N-x-y} \cdot t^{x+y})^2}{(1+t^{2x+1})(1+t^{2y+1})} \\ P_{A,B|X,Y}(0, 1|A_x, B_y) &= \frac{t^2}{1+t^2} \frac{(1 + (-1)^{y-x} \cdot t^{x-y-1})^2 \cdot t^{2y+1}}{(1+t^{2x+1})(1+t^{2y+1})} \\ P_{A,B|X,Y}(1, 0|A_x, B_y) &= \frac{t^2}{1+t^2} \frac{(1 + (-1)^{x-y} \cdot t^{y-x-1})^2 \cdot t^{2x+1}}{(1+t^{2x+1})(1+t^{2y+1})} \\ P_{A,B|X,Y}(1, 1|A_x, B_y) &= \frac{1}{1+t^2} \frac{(1 - (-1)^{2N-x-y} \cdot t^{x+y+2})^2}{(1+t^{2x+1})(1+t^{2y+1})} \end{aligned} \quad (18)$$

The Hardy probability is then given by

$$\begin{aligned} P_{\text{Hardy}} &= P_{A,B|X,Y}(0, 0|A_N, B_N) \\ &= \max_{0 \leq t \leq 1} \frac{t^2}{1+t^2} \left(\frac{1-t^{2N}}{1+t^{2N+1}} \right) \rightarrow \frac{1}{2} \quad (N \rightarrow \infty, t \rightarrow 1_-) \end{aligned} \quad (19)$$

Under the (as yet unproven) assumption that this optimal quantum strategy ($N \rightarrow \infty, t \rightarrow 1_-$) is self-testing, we see that one may certify arbitrarily close to the maximum possible

value of 2 bits of global randomness from the measurement setting $x = N, y = 0$ (or $x = 0, y = N$), i.e., $P_{A,B|X,Y}(a, b|A_N, B_0) \rightarrow \frac{1}{4}$ for all $a, b \in \{0, 1\}$ (note that both the two limits $N \rightarrow \infty, t \rightarrow 1_-$ need to be taken.)

The second family of Hardy tests (for certifying $2 \log_2 d$ bits of global randomness in $d = 4, 8$) is based on a novel construction using sub-structures of Kochen-Specker sets, that were termed 01-gadgets in [31]. A 01-gadget is a graph $G = (V_G, E_G)$ with a faithful orthogonal representation in $\mathbb{C}^{\omega(G)}$, where $\omega(G)$ denotes the clique number of the graph. Here, a faithful orthogonal representation is a mapping of the vertices of the graph to (unit) vectors such that adjacent vertices are mapped to orthogonal vectors, and distinct vertices are assigned distinct vectors. Kochen-Specker sets concern $\{0, 1\}$ -colorings of the graph (i.e., mappings $f : V_G \rightarrow \{0, 1\}$) that satisfy the conditions that (i) any two adjacent vertices cannot be assigned value 1 simultaneously; and that (ii) in any maximal clique, there is a unique vertex that is assigned value 1. A defining property of a 01-gadget G is that there exist two distinct *non-adjacent* vertices $v_1 \approx v_2$ that cannot be assigned value 1 simultaneously in any feasible $\{0, 1\}$ -coloring of G , while at the same time, a faithful orthogonal representation of G exists in $\mathbb{C}^{\omega(G)}$ in which v_1 and v_2 are assigned non-orthogonal vectors.

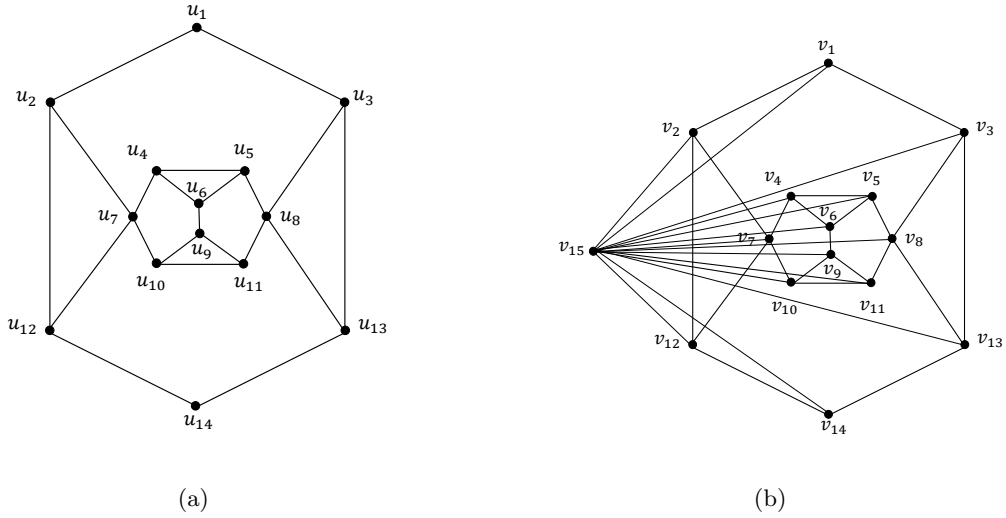


Figure 3: The graph in (a) is a 01-gadget that has a faithful orthogonal representation in $\mathbb{R}^3$, and the overlap of the two distinguished vectors $|\langle u_1 | u_{14} \rangle| \leq \frac{1}{2}$. The graph in (b) is a 01-gadget constructed by adding an additional vector $|v_{15}\rangle$ that is orthogonal with all of the vectors in the faithful representation of (a). The graph in (b) has an orthogonal representation in $\mathbb{R}^4$, and the maximal overlap of the two distinguished vectors is still $\frac{1}{2}$, i.e., $|\langle v_1 | v_{14} \rangle| \leq \frac{1}{2}$.

The figure shown in Fig. 3(a) is an example of 01-gadget, which has an orthogonal representation in $\mathbb{R}^3$, and the maximal overlap of the two distinguished vectors $|u_1\rangle, |u_{14}\rangle$ is $\frac{1}{2}$, i.e., $|\langle u_1 | u_{14} \rangle| \leq \frac{1}{2}$ [31]. The 01-gadget shown in Fig. 3(b) has an orthogonal representation in $\mathbb{R}^4$ which is constructed by adding an extra vector $|v_{15}\rangle$ to the first 01-gadget and making this vector $|v_{15}\rangle$ orthogonal to all of the other vectors. Specifically, since the first 01-gadget has an orthogonal representation in $\mathbb{R}^3$, one can keep the structure of the first 01-gadget in the first three dimensions of $\mathbb{R}^4$ and the extra vector is the basis vector on the fourth dimension $(0, 0, 0, 1)^T$. It is easy to verify that the two distinguished vectors of this new 01-gadget are still $|v_1\rangle, |v_{14}\rangle$ and their maximal overlap is still $\frac{1}{2}$. Specifically, an orthogonal representation of the 01-gadget Fig. 3(b) for which the maximal overlap of the two special distinguished vertices is $|\langle v_1 | v_{14} \rangle| = \frac{1}{2}$ is given as (excluding normalization

factors):

$$\begin{aligned}
\langle v_1| &= (1, 0, 0, 0), \quad \langle v_2| = (0, 4, 1, 1), \quad \langle v_3| = (0, 0, 1, 1), \\
\langle v_4| &= (-3 - \sqrt{3}, -5 + \sqrt{3}, 1 + \sqrt{3}, 1 + \sqrt{3}), \quad \langle v_5| = (3 + \sqrt{3}, -3 - \sqrt{3}, 3 - \sqrt{3}, 3 - \sqrt{3}), \\
\langle v_6| &= (3 - \sqrt{3}, 1 + \sqrt{3}, 1 + \sqrt{3}, 1 + \sqrt{3}), \quad \langle v_7| = (-3, 1, -2, -2), \quad \langle v_8| = (1, 1, 0, 0), \\
\langle v_9| &= (3 + \sqrt{3}, 1 - \sqrt{3}, 1 - \sqrt{3}, 1 - \sqrt{3}), \quad \langle v_{10}| = (-3 + \sqrt{3}, -5 - \sqrt{3}, 1 - \sqrt{3}, 1 - \sqrt{3}), \\
\langle v_{11}| &= (-3 + \sqrt{3}, 3 - \sqrt{3}, -3 - \sqrt{3}, -3 - \sqrt{3}), \\
\langle v_{12}| &= (3, 1, -2, -2), \quad \langle v_{13}| = (-1, 1, 0, 0), \quad \langle v_{14}| = (1, 1, 1, 1), \quad \langle v_{15}| = (0, 0, 1, -1).
\end{aligned} \tag{20}$$

In order to certify 4 bits of global randomness for the quantum system of dimension 4, we create four copies of this 01-gadget $G^{(1)}, G^{(2)}, G^{(3)}, G^{(4)}$ in $\mathbb{C}^4$ such that the corresponding vectors in each copy are mutually orthogonal, i.e., $|v_k^{(1)}\rangle, |v_k^{(2)}\rangle, |v_k^{(3)}\rangle, |v_k^{(4)}\rangle$ form a complete basis (the vertices form a maximal clique). This is achieved by rotating each vector $(a, b, c, d) \in \mathbb{R}^4$ in the original 01-gadget Fig. 3(b) into the orthogonal vectors $(b, -a, -d, c), (c, d, -a, -b), (d, -c, b, -a)$ in the copies while preserving the orthogonality structure. Note that such a construction is also possible in dimension 8, because there exist division algebras (the quaternions and octonions) in dimensions 4 and 8 [33]. Let G in Fig. 4 denote the orthogonality graph of these four copies with vertices $V(G) = V(G^{(1)}) \cup V(G^{(2)}) \cup V(G^{(3)}) \cup V(G^{(4)})$ and edges formed by the orthogonality constraints.

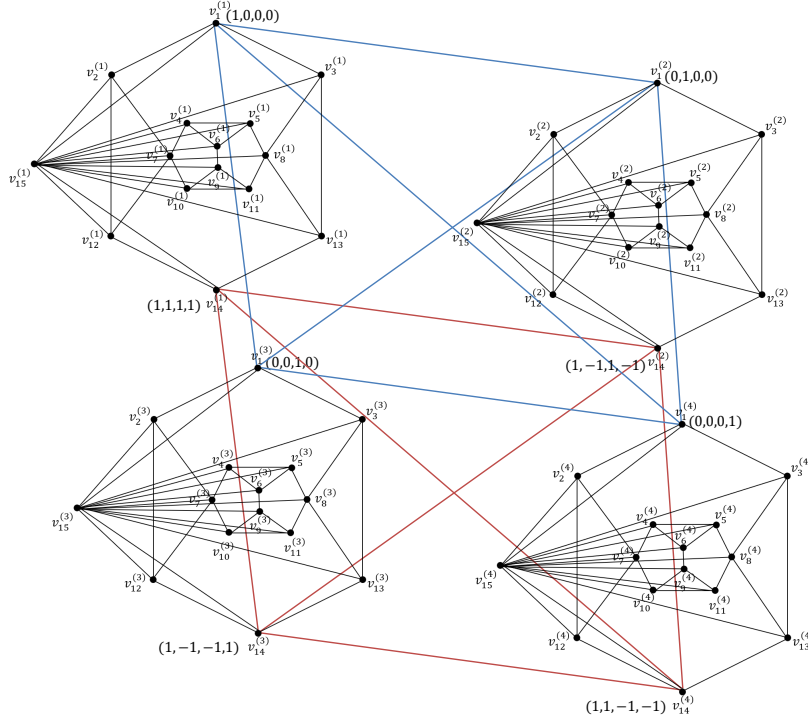


Figure 4: As explained in the text, one can rotate the vectors in the 01-gadget Fig. 3(b) to create four copies of it. The corresponding vectors in each copy are mutually orthogonal, i.e., $|v_k^{(1)}\rangle, |v_k^{(2)}\rangle, |v_k^{(3)}\rangle, |v_k^{(4)}\rangle$ form a complete basis (the vertices form a maximal clique).

Some of us showed in [24] that there exists a one-to-one correspondence between 01-gadget in dimension d and two-player Hardy paradoxes for the maximally entangled state

in $\mathbb{C}^d \otimes \mathbb{C}^d$. We now proceed to construct the Hardy paradox for the maximally entangled state $|\psi\rangle = \frac{1}{2} \sum_{i=0}^3 |i, i\rangle$. To do this, we first complete all the possible measurement bases (maximal cliques in the graph), these bases will serve as the measurement inputs x, y for both players. In particular, let us denote by x^*, y^* the respective maximal cliques formed by the distinguished vertices $v_1^{(1)}, v_1^{(2)}, v_1^{(3)}, v_1^{(4)}$ (the blue clique in Fig. 4) and $v_{14}^{(1)}, v_{14}^{(2)}, v_{14}^{(3)}, v_{14}^{(4)}$ (the red clique in Fig. 4). The outcomes of each measurement are labeled by $a, b \in \{1, 2, 3, 4\}$ for the two players respectively, and correspond to the vertices in the clique. For convenience, let us rewrite the notation of the orthogonal representations of G as $\{|v_{z,c}\rangle\}$ $z \in \{x, y\}, c \in \{a, b\}$. We define the set S_{Hz} of Hardy ‘zero’ constraints in this case as

$$S_{Hz} := \{((x, a), (y, b)) : \langle v_{(x,a)} | v_{(y,b)} \rangle = 0\} \quad \forall x, y, a, b \quad (21)$$

The Hardy probability is then given by the sum of the probabilities of the input-output pairs in the set S_{exp} defined as $S_{exp} := \cup_{k=1}^4 \{((x^*, v_1^{(k)}), (y^*, v_{14}^{(k)}))\}$. Note that these input-output pairs correspond to the four pairs of distinguished vertices of the four copies of the 01-gadget. It is readily seen that in any deterministic classical (LHV) behavior, by the property of the 01-gadget that the distinguished vertices cannot be assigned value 1 simultaneously, it holds that the sum of the probabilities of the input-output pairs in S_{exp} is always 0.

On the other hand, we present a quantum strategy that satisfies all the zero constraints while simultaneously achieving the Hardy probability of 1. In the strategy, the two players share a two-ququart maximally entangled state $|\psi\rangle = \frac{1}{2} \sum_{i=0}^3 |i, i\rangle$ and upon receiving the input x, y they measure in the corresponding bases given by the orthogonal representation: $\Pi_x = \{|v_{(x,a)}\rangle\langle v_{(x,a)}|\}_{a=1,\dots,4}$ and $\Sigma_y = \{|v_{(y,b)}\rangle\langle v_{(y,b)}|\}_{b=1,\dots,4}$ and return the outcomes $a, b \in \{1, \dots, 4\}$. We see that for all $((x, a), (y, b)) \in S_{Hz}$:

$$\langle \psi | (|v_{(x,a)}\rangle \otimes |v_{(y,b)}\rangle) = \frac{1}{2} \overline{\langle v_{(x,a)} | v_{(y,b)} \rangle} = 0 \quad (22)$$

which correspond to the zero constraints in the Hardy paradox. While, for the input-output pairs in S_{exp} , we obtain

$$P_{A,B|X,Y} (v_1^{(k)}, v_{14}^{(k)} | x^*, y^*) = \frac{1}{4} |\langle v_1^{(k)} | \bar{v}_{14}^{(k)} \rangle|^2 = \frac{1}{16} \quad \text{for } k = 1, \dots, 4 \quad (23)$$

which correspond to the non-zero Hardy expressions in the Hardy paradox. Furthermore, from the orthogonal representation shown in (20), we also see that the outcomes of the measurement settings x^*, y^* are uniform:

$$P_{A,B|X,Y} (v_1^{(i)}, v_{14}^{(j)} | x^*, y^*) = \frac{1}{4} |\langle v_1^{(i)} | \bar{v}_{14}^{(j)} \rangle|^2 = \frac{1}{16} \quad \forall i, j = 1, \dots, 4$$

Thus, the presented Hardy test is a good candidate to certify the maximum possible value (using systems of local Hilbert space dimension $d = 4$) of 4 bits of global randomness and 2 bits of local randomness from the measurement settings x^*, y^* . We defer the detailed self-testing statement of the above Hardy test and the corresponding test using systems of local dimension $d = 8$ to forthcoming work.

5 Conclusions

The generalisation of device-independent protocols for randomness generation, key distribution and self-testing to the scenario when the honest parties do not have trusted, fully

uniform private seeds remains an interesting open question. In this paper, we have proposed a class of tilted Hardy tests in the simplest Bell scenario of two players performing a pair of binary measurements on two-qubit states that serve as ideal candidates for this generalisation. Our derived results on the amount of certifiable randomness from these tests against different sets of adversaries find immediate application in the state-of-the-art protocols for randomness amplification of weak SV seeds against quantum and no-signaling adversaries. While the tests allow to certify the maximum possible amount of 1 bit of local randomness for each player, they fall short of the ideal global randomness of 2 bits from the measurement outputs of both players. To remedy this defect, we proposed a class of Hardy tests in systems of local Hilbert space dimensions 4, 8 that can allow to certify up to the maximum possible $2 \log_2 d$ bits of randomness under arbitrarily limited measurement independence. It is an interesting task for future research to utilize the proposed tests to improve the generation rates of fully device-independent protocols against general adversaries.

6 Acknowledgments

We acknowledge support from the Start-up Fund "Device-Independent Quantum Communication Networks" from The University of Hong Kong, the Seed Fund "Security of Relativistic Quantum Cryptography" (Grant No. 201909185030), the Early Career Scheme (ECS) grant "Device-Independent Random Number Generation and Quantum Key Distribution with Weak Random Seeds" (Grant No. 27210620), the General Research Fund (GRF) grant "Semi-device-independent cryptographic applications of a single trusted quantum system" (Grant No. 17211122) and the Research Impact Fund (RIF) "Trustworthy quantum gadgets for secure online communication" (Grant No. R7035-21). P.H. acknowledges support from the Foundation for Polish Science (IRAP project, ICTQT, contract no. 2018/MAB/5, co-financed by EU within the Smart Growth Operational Programme).

References

- [1] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" [Phys. Rev. **47**, 777](#) (1935).
- [2] Erwin Schrödinger. "Discussion of probability relations between separated systems." [Cambridge University Press](#). (1935).
- [3] Jonathan Barrett, Lucien Hardy, and Adrian Kent. "No signaling and quantum key distribution." [Phys. Rev. Lett. **95**, 010503](#) (2005).
- [4] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. "Device-independent security of quantum cryptography against collective attacks." [Phys. Rev. Lett. **98**, 230501](#) (2007).
- [5] Stefano Pironio, Antonio Acín, Serge Massar, A. Boyer de La Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T. Andrew Manning, and C. Monroe. "Random numbers certified by Bell's theorem." [Nature **464**, 1021–1024](#) (2010) (2010).
- [6] Stefano Pironio and Serge Massar. "Security of practical private randomness generation." [Phys. Rev. A **87**, 012336](#) (2013).

- [7] Dominic Mayers and Andrew Yao. “Quantum cryptography with imperfect apparatus.” [Proceedings 39th Annual Symposium on Foundations of Computer Science](#), pages 503–509 (1998).
- [8] Dominic Mayers and Andrew Yao. “Self testing quantum apparatus.” [Quantum Info. Comput.](#) **4**(4), 273–286 (2004).
- [9] Ivan Šupić and Joseph Bowles. “Self-testing of quantum systems: a review.” [Quantum](#) **4**, 337 (2020).
- [10] Koon Tong Goh, Chithrabhanu Perumangatt, Zhi Xian Lee, Alexander Ling, and Valerio Scarani. “Experimental comparison of tomography and self-testing in certifying entanglement.” [Phys. Rev. A](#) **100**, 022305 (2019).
- [11] Roger Colbeck and Renato Renner. “Free randomness can be amplified.” [Nat. Phys.](#) **8**, 450–453 (2012).
- [12] Rodrigo Gallego, Lluís Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. “Full randomness from arbitrarily deterministic events.” [Nat. Commun.](#) **4**, 2654 (2013).
- [13] Ravishankar Ramanathan, Fernando G. S. L. Brandão, Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Hanna Wojewódka. “Randomness amplification under minimal fundamental assumptions on the devices.” [Phys. Rev. Lett.](#) **117**, 230501 (2016).
- [14] Fernando G. S. L. Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek, and Hanna Wojewódka. “Realistic noise-tolerant randomness amplification using finite number of devices.” [Nat. Commun.](#) **7**, 11345 (2016).
- [15] Ravishankar Ramanathan, Michał Horodecki, Hammad Anwer, Stefano Pironio, Karol Horodecki, Marcus Grünfeld, Sadiq Muhammad, Mohamed Bourennane, and Paweł Horodecki. “Practical no-signalling proof randomness amplification using Hardy paradoxes and its experimental implementation.” [arXiv:1810.11648](#) (2018).
- [16] Max Kessler and Rotem Arnon-Friedman. “Device-independent randomness amplification and privatization.” [IEEE Journal on Selected Areas in Information Theory](#) **1**(2), 568–584 (2020).
- [17] Miklos Santha and Umesh V. Vazirani. “Generating quasi-random sequences from semi-random sources.” [Journal of Computer and System Sciences](#) **33**(1), 75–87 (1986).
- [18] Antonio Acín, Serge Massar, and Stefano Pironio. “Randomness versus nonlocality and entanglement.” [Phys. Rev. Lett.](#) **108**, 100402 (2012).
- [19] Cédric Bamps and Stefano Pironio. “Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing.” [Phys. Rev. A](#) **91**, 052111 (2015).
- [20] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. “All pure bipartite entangled states can be self-tested.” [Nat. Commun.](#) **8**, 15485 (2017).
- [21] Cédric Bamps, Serge Massar, and Stefano Pironio. “Device-independent randomness generation with sublinear shared quantum resources.” [Quantum](#) **2**, 86 (2018).
- [22] Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín. “Unbounded randomness certification using sequences of measurements.” [Phys. Rev. A](#) **95**, 020102 (2017).

- [23] Gilles Pütz, Denis Rosset, Tomer Jack Barnea, Yeong-Cherng Liang, and Nicolas Gisin. “Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality.” *Phys. Rev. Lett.* **113**, 190402 (2014).
- [24] Ravishankar Ramanathan, Yuan Liu, and Paweł Horodecki. “Large violations in Kochen Specker contextuality and their applications.” *New J. Phys.* **24**, 033035 (2022).
- [25] Lucien Hardy. “Nonlocality for two particles without inequalities for almost all entangled states.” *Phys. Rev. Lett.* **71**, 1665 (1993).
- [26] Rafael Rabelo, Law Yun Zhi, and Valerio Scarani. “Device-independent bounds for Hardy’s experiment.” *Phys. Rev. Lett.* **109**, 180401 (2012).
- [27] Hong-Wei Li, Marcin Pawłowski, Ramij Rahaman, Guang-Can Guo, and Zheng-Fu Han. “Device-and semi-device-independent random numbers based on noninequality paradox.” *Phys. Rev. A* **92**, 022327 (2015).
- [28] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. “Proposed experiment to test local hidden-variable theories.” *Phys. Rev. Lett.* **23**, 880 (1969).
- [29] Miguel Navascués, Stefano Pironio, and Antonio Acín. “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations.” *New J. Phys.* **10**, 073013 (2008).
- [30] Danilo Boschi, S Branca, Francesco De Martini, and Lucien Hardy. “Ladder proof of nonlocality without inequalities: Theoretical and experimental results.” *Phys. Rev. Lett.* **79**, 2755 (1997).
- [31] Ravishankar Ramanathan, Monika Rosicka, Karol Horodecki, Stefano Pironio, Michał Horodecki, and Paweł Horodecki. “Gadget structures in proofs of the Kochen-Specker theorem.” *Quantum* **4**, 308 (2020).
- [32] Ravishankar Ramanathan, Paweł Horodecki, and Michał Banacki. “No-signaling-proof randomness extraction from public weak sources.” *arXiv:2108.08819* (2021).
- [33] Paul Moritz Cohn. “Basic algebra: groups, rings and fields”. *Springer London* (2012).
- [34] Camille Jordan. “Essai sur la géométrie à n dimensions.” *Bulletin de la S. M. F.* **3**, 103-174 (1875).
- [35] Ravishankar Ramanathan, Dardo Goyeneche, Sadiq Muhammad, Piotr Mironowicz, Marcus Grünfeld, Mohamed Bourennane, and Paweł Horodecki. “Steering is an essential feature of non-locality in quantum theory.” *Nat. Commun.* **9**, 4244 (2018).

A Self-testing general pure two-qubit entangled states with the tilted Hardy test

In this section, we provide the proof of Prop. 1. For convenience, we review this Proposition here.

Proposition. *Suppose that the Hardy zero constraints $P_{A,B|X,Y}(0,1|A_0,B_1) = P_{A,B|X,Y}(1,0|A_1,B_0) = P_{A,B|X,Y}(0,0|A_1,B_1) = 0$ are satisfied. Then in any local hidden variable theory it holds that $P_{\text{Hardy}}^{w,LHV} \leq \max(0,w)$. On the other hand, quantum theory allows to achieve $P_{\text{Hardy}}^{w,Q} = \frac{(4w+5)\sqrt{4w+5}-(12w+11)}{2(w+1)}$. Furthermore, up to local isometries,*

the value is uniquely achieved by the two-qubit state $|\psi_\theta\rangle = \cos(\frac{\theta}{2})|00\rangle - \sin(\frac{\theta}{2})|11\rangle$ with $\theta = \arcsin(3 - \sqrt{4w+5})$ and the measurement $\{A_0, A_1\}$, $\{B_0, B_1\}$ given by

$$\begin{aligned} A_0 = B_0 &= \frac{-(2 + \sin \theta)(1 - \sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}} \cdot Z + \frac{-\sqrt{2} \sin \theta (\sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}} \cdot X, \\ A_1 = B_1 &= \frac{-(1 - \sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}} \cdot Z + \frac{\sqrt{2} (\sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}} \cdot X, \end{aligned} \quad (24)$$

where X and Z are Pauli matrices.

Proof. The proof consists of the following three statements.

- The classical value $P_{Hardy}^{w,LHV} \leq \max(0, w)$.

Any local hidden variable behavior can be written as a convex combination of deterministic non-signaling behaviors $\{P_{A,B|X,Y}(a,b|x,y)\}$. In the Bell scenario under consideration, it is well known that there are 16 deterministic behaviors in total (where each party deterministically outputs a specific value of $a, b \in \{0, 1\}$ for each input). Of these, there are five deterministic non-signaling behaviors that meet the Hardy ‘zero’ constraints $P_{A,B|X,Y}(0, 1|A_0, B_1) = P_{A,B|X,Y}(1, 0|A_1, B_0) = P_{A,B|X,Y}(0, 0|A_1, B_1) = 0$, shown in Table 1 and 2. As is easily seen, the three Hardy zero constraints force $P_{A,B|X,Y}(0, 0|A_0, B_0) = 0$ in each of the deterministic non-signaling boxes. $P_{A,B|X,Y}(1, 1|A_0, B_0) \leq 1$ leads to the bound of the non-zero Hardy probability term: $P_{Hardy}^{w,LHV} = P_{A,B|X,Y}(0, 0|A_0, B_0) + wP_{A,B|X,Y}(1, 1|A_0, B_0) \leq \max(0, w)$.

Table 1: Local boxes that lead to the upper bound of tilted Hardy’s paradox when $w \geq 0$.

	B_0	B_1	B_0	B_1	B_0	B_1
	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$
$A_0 \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$
$A_1 \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}$	$\begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}$

Table 2: Local boxes that lead to the upper bound of tilted Hardy’s paradox when $w \leq 0$.

	B_0	B_1	B_0	B_1
	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$	$\begin{smallmatrix} 0 & 1 \end{smallmatrix}$
$A_0 \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$	$\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}$	$\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$
$A_1 \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$	$\begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}$	$\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}$	$\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array}$	$\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}$

- The quantum value $P_{Hardy}^{w,Q} = \frac{(4w+5)\sqrt{4w+5} - (12w+11)}{2(w+1)}$.

In the Bell scenario under consideration where each party performs measurements of two binary observables, the well-known Jordan’s Lemma [34] states that arbitrary Hermitian observables can be block diagonalized into blocks of size at most 2×2 .

That is, for Alice and Bob's measurement observables A_x, B_y and $x, y \in \{0, 1\}$, the corresponding projectors can be decomposed as $A_{a|x} = \bigoplus_i A_{a|x}^i$ and $B_{b|y} = \bigoplus_j B_{b|y}^j$, where $A_{a|x}^i, B_{b|y}^j$ are the corresponding projectors acting on Hilbert spaces $\mathbf{H}_A^i$ and $\mathbf{H}_B^j$ of dimensions $d \leq 2$ for all a, b and x, y . The joint probability of outcomes a, b given measurements x, y performed on the quantum system can be decomposed as

$$\begin{aligned} P_{A,B|X,Y}(a, b|A_x, B_y) &= \text{Tr}[(A_{a|x} \otimes B_{b|y})\rho] \\ &= \sum_{i,j} q_{i,j} \text{Tr}[(A_{a|x}^i \otimes B_{b|y}^j)\rho_{i,j}] \\ &= \sum_{i,j} q_{i,j} P_{A,B|X,Y}^{i,j}(a, b|A_x, B_y), \end{aligned} \quad (25)$$

where $\rho_{i,j}$ is a (two-qubit) projection of the shared quantum state ρ on Hilbert spaces $\mathbf{H}_A^i \otimes \mathbf{H}_B^j$, $q_{i,j}$ is the corresponding coefficient with $\sum_{i,j} q_{i,j} = 1$. When the three Hardy zero constraints $P_{A,B|X,Y}(0, 1|A_0, B_1) = P_{A,B|X,Y}(1, 0|A_1, B_0) = P_{A,B|X,Y}(0, 0|A_1, B_1) = 0$ are satisfied, following [25], it is easy to calculate the quantum state and measurements which achieve the maximal value of the Hardy probability $P_{Hardy}^{w,Q}$. For an arbitrary partially entangled state $|\psi_\theta\rangle = \cos(\frac{\theta}{2})|00\rangle - \sin(\frac{\theta}{2})|11\rangle$ with $\theta \in (0, \frac{\pi}{2})$, $P_{Hardy}^{w,Q}$ is given by:

$$\begin{aligned} P_{Hardy}^{w,Q} &= P_{A,B|X,Y}(0, 0|A_0, B_0) + w \cdot P_{A,B|X,Y}(1, 1|A_0 B_0) \\ &= \left[\frac{(\cos(\frac{\theta}{2}) \sin(\frac{\theta}{2}))(\cos(\frac{\theta}{2}) - \sin(\frac{\theta}{2}))}{1 - \cos(\frac{\theta}{2}) \sin(\frac{\theta}{2})} \right]^2 + w \left[\frac{1 - 2 \cos(\frac{\theta}{2}) \sin(\frac{\theta}{2})}{(\cos(\frac{\theta}{2}) - \sin(\frac{\theta}{2}))(1 - \cos(\frac{\theta}{2}) \sin(\frac{\theta}{2}))} \right]^2 \\ &= \frac{(\sin^2 \theta + 4 \cdot w)(1 - \sin \theta)}{(2 - \sin \theta)^2}. \end{aligned} \quad (26)$$

Setting $\frac{dP_{Hardy}^{w,Q}}{d \sin \theta} = 0$ gives $\sin \theta = 3 - \sqrt{4w + 5}$. It is then readily checked that this point gives the maximum of the Hardy probability as:

$$P_{Hardy}^{w,Q} = \frac{(4w + 5)\sqrt{4w + 5} - (12w + 11)}{2(w + 1)} \quad (27)$$

for any $w \in (-\frac{1}{4}, 1)$. For each pure two-qubit entangled state $|\psi_\theta\rangle$ other than the singlet (with $\theta = \pi/2$), we see that there exists a corresponding w (and thus, a corresponding tilted Hardy test) such that $|\psi_\theta\rangle$ gives the optimal violation of that test.

- Self-testing of $|\psi_\theta\rangle$ and $\{A_x\}, \{B_y\}$.

Without loss of generality, choosing the computational basis $\{|2i\rangle\langle 2i|, |2i+1\rangle\langle 2i+1|\}$ on Hilbert space $\mathbf{H}_A^i$ for Alice and the computational basis $\{|2j\rangle\langle 2j|, |2j+1\rangle\langle 2j+1|\}$ on Hilbert space $\mathbf{H}_B^j$ for Bob, the shared quantum state can be expressed as $\rho_{i,j,\theta} = |\psi_{i,j,\theta}\rangle\langle\psi_{i,j,\theta}|$, where $|\psi_{i,j,\theta}\rangle = \cos(\frac{\theta}{2})|2i, 2j\rangle - \sin(\frac{\theta}{2})|2i+1, 2j+1\rangle$. According to the above discussion, the Hardy zero constraints are satisfied and the upper bound of the Hardy expression $P_{Hardy}^{w,Q}$ is attained if and only if $\sin \theta = 3 - \sqrt{4w + 5}$ and the

operators are:

$$\begin{aligned}
A_1^i &= c_{1z} \cdot (|2i\rangle\langle 2i| - |2i+1\rangle\langle 2i+1|) + c_{1x} \cdot (|2i\rangle\langle 2i+1| + |2i+1\rangle\langle 2i|) \\
B_1^j &= c_{1z} \cdot (|2j\rangle\langle 2j| - |2j+1\rangle\langle 2j+1|) + c_{1x} \cdot (|2j\rangle\langle 2j+1| + |2j+1\rangle\langle 2j|) \\
A_0^i &= c_{0z} \cdot (|2i\rangle\langle 2i| - |2i+1\rangle\langle 2i+1|) + c_{0x} \cdot (|2i\rangle\langle 2i+1| + |2i+1\rangle\langle 2i|) \\
B_0^j &= c_{0z} \cdot (|2j\rangle\langle 2j| - |2j+1\rangle\langle 2j+1|) + c_{0x} \cdot (|2j\rangle\langle 2j+1| + |2j+1\rangle\langle 2j|)
\end{aligned} \tag{28}$$

with

$$\begin{aligned}
c_{1z} &= \frac{-(1 - \sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}}, & c_{1x} &= \frac{\sqrt{2}(\sin \theta)^{\frac{1}{2}}}{(1 + \sin \theta)^{\frac{1}{2}}} \\
c_{0z} &= \frac{-(2 + \sin \theta)(1 - \sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}}, & c_{0x} &= \frac{-\sqrt{2} \sin \theta (\sin \theta)^{\frac{1}{2}}}{(2 - \sin \theta)(1 + \sin \theta)^{\frac{1}{2}}}
\end{aligned} \tag{29}$$

As such, the actual experiment quantum system can satisfy all the Hardy zero constraints and achieve the bound $P_{Hardy}^{w,Q}$, if and only if the state is given by $|\widetilde{\psi_\theta}\rangle = \bigoplus_{i,j} \sqrt{q_{i,j}} |\psi_{i,j,\theta}\rangle$ with the measurements being $\widetilde{A}_1 = \bigoplus_i A_1^i$, $\widetilde{A}_0 = \bigoplus_i A_0^i$, $\widetilde{B}_1 = \bigoplus_j B_1^j$ and $\widetilde{B}_0 = \bigoplus_j B_0^j$, with coefficients $q_{i,j}$ satisfying $q_{i,j} \geq 0$, $\sum_{i,j} q_{i,j} = 1$. The isometry is given by $\Phi = \Phi_A \otimes \Phi_B$ [26] with $\Phi_C(|2k\rangle_C \otimes |0\rangle_{C'}) \mapsto |2k\rangle_C \otimes |0\rangle_{C'}$ and $\Phi_C(|2k+1\rangle_C \otimes |0\rangle_{C'}) \mapsto |2k\rangle_C \otimes |1\rangle_{C'}$ for $C = A, B$. With ancillary qubits $|00\rangle_{A'B'}$, the reference state $|\psi_\theta\rangle$ and reference measurements A_1, B_1, A_0, B_0 can be self-tested from the physical state $|\widetilde{\psi_\theta}\rangle$ and physical measurements $\widetilde{A}_1, \widetilde{A}_0, \widetilde{B}_1, \widetilde{B}_0$:

$$\begin{aligned}
&\Phi(|\widetilde{\psi_\theta}\rangle_{AB} \otimes |00\rangle_{A'B'}) \\
&= \Phi\left(\bigoplus_{i,j} \sqrt{q_{i,j}} \left(\cos\left(\frac{\theta}{2}\right)|2i, 2j\rangle - \sin\left(\frac{\theta}{2}\right)|2i+1, 2j+1\rangle\right)_{AB} \otimes |00\rangle_{A'B'}\right) \\
&= \bigoplus_{i,j} \sqrt{q_{i,j}} \left(\cos\left(\frac{\theta}{2}\right)|2i, 2j\rangle_{AB} \otimes |00\rangle_{A'B'} - \sin\left(\frac{\theta}{2}\right)|2i, 2j\rangle_{AB} \otimes |11\rangle_{A'B'}\right) \\
&= \bigoplus_{i,j} \sqrt{q_{i,j}} |2i, 2j\rangle_{AB} \otimes \left(\cos\left(\frac{\theta}{2}\right)|00\rangle_{A'B'} - \sin\left(\frac{\theta}{2}\right)|11\rangle_{A'B'}\right) \\
&= |\sigma\rangle_{AB} \otimes |\psi_\theta\rangle_{A'B'}
\end{aligned} \tag{30}$$

$$\begin{aligned}
& \Phi(\widetilde{A_1}|\widetilde{\psi_\theta}\rangle_{AB} \otimes |00\rangle_{A'B'}) \\
&= \Phi(\bigoplus_{i,j} \sqrt{q_{ij}} [c_{2z} \cdot (|2i\rangle\langle 2i| - |2i+1\rangle\langle 2i+1|) + c_{2x} \cdot (|2i\rangle\langle 2i+1| + |2i+1\rangle\langle 2i|)] \\
&\quad (\cos(\frac{\theta}{2})|2i, 2j\rangle - \sin(\frac{\theta}{2})|2i+1, 2j+1\rangle)_{AB} \otimes |00\rangle_{A'B'}) \\
&= \Phi(\bigoplus_{i,j} \sqrt{q_{ij}} [\cos(\frac{\theta}{2})(c_{2z}|2i, 2j\rangle + c_{2x}|2i+1, 2j\rangle) \\
&\quad - \sin(\frac{\theta}{2})(-c_{2z}|2i+1, 2j+1\rangle + c_{2x}|2i, 2j+1\rangle)]_{AB} \otimes |00\rangle_{A'B'}) \\
&= \bigoplus_{i,j} \sqrt{q_{ij}} [\cos(\frac{\theta}{2})(c_{2z}|2i, 2j\rangle_{AB} \otimes |00\rangle_{A'B'} + c_{2x}|2i, 2j\rangle \otimes |10\rangle_{A'B'}) \\
&\quad - \sin(\frac{\theta}{2})(-c_{2z}|2i, 2j\rangle_{AB} \otimes |11\rangle_{A'B'} + c_{2x}|2i, 2j\rangle_{AB} \otimes |01\rangle_{A'B'})] \\
&= \bigoplus_{i,j} \sqrt{q_{ij}} |2i, 2j\rangle_{AB} \otimes [\cos(\frac{\theta}{2})(c_{2z}|00\rangle_{A'B'} + c_{2x}|10\rangle_{A'B'}) \\
&\quad - \sin(\frac{\theta}{2})(-c_{2z}|11\rangle_{A'B'} + c_{2x}|01\rangle_{A'B'})] \\
&= \bigoplus_{i,j} \sqrt{q_{ij}} |2i, 2j\rangle_{AB} \otimes (c_{2z} \cdot Z + c_{2x} \cdot X)(\cos(\frac{\theta}{2})|00\rangle_{A'B'} - \sin(\frac{\theta}{2})|11\rangle_{A'B'}) \\
&= |\sigma\rangle_{AB} \otimes A_1|\psi_\theta\rangle_{A'B'}
\end{aligned} \tag{31}$$

and

$$\begin{aligned}
& \Phi(\widetilde{A_0}|\widetilde{\psi_\theta}\rangle_{AB} \otimes |00\rangle_{A'B'}) \\
&= \Phi(\bigoplus_{i,j} \sqrt{q_{ij}} [c_{1z} \cdot (|2i\rangle\langle 2i| - |2i+1\rangle\langle 2i+1|) + c_{1x} \cdot (|2i\rangle\langle 2i+1| + |2i+1\rangle\langle 2i|)] \\
&\quad (\cos(\frac{\theta}{2})|2i, 2j\rangle - \sin(\frac{\theta}{2})|2i+1, 2j+1\rangle)_{AB} \otimes |00\rangle_{A'B'}) \\
&= \bigoplus_{i,j} \sqrt{q_{ij}} |2i, 2j\rangle_{AB} \otimes (c_{1z} \cdot Z + c_{1x} \cdot X)(\cos(\frac{\theta}{2})|00\rangle_{A'B'} - \sin(\frac{\theta}{2})|11\rangle_{A'B'}) \\
&= |\sigma\rangle_{AB} \otimes A_0|\psi_\theta\rangle_{A'B'}
\end{aligned} \tag{32}$$

where $|\sigma\rangle_{AB}$ is a bipartite ‘junk’ state. Analogous self-testing equations hold for B_1 , B_0 as well as $A_x B_y$ for $x, y \in \{0, 1\}$.

□

B The guessing probability of a quantum adversary under Colored Noise

As a quantum adversary, Eve holds a quantum system that may be entangled with the device held by Alice and Bob. Let us denote the tripartite quantum state of Alice, Bob and Eve by $|\Psi\rangle_{ABE}$. In this section, we will calculate the guessing probability of such an adversary Eve, when Alice and Bob perform the tilted Hardy test on their reduced system ρ_{AB} and observe that the three Hardy zero constraints are perfectly satisfied while the Hardy probability achieves some non-maximal value $0 < p \leq P_{Hardy}^{w=w_0, Q} = \frac{(4w_0+5)\sqrt{4w_0+5}-(12w_0+11)}{2(w_0+1)}$.

Here we fix $w = w_0$, in which case as discussed in Section 2, one can certify the most global randomness from the measurement setting (A_0, B_0) , when the optimal quantum behaviour is observed. The problem we want to solve is to maximize the guessing probability under the constraint that (i) Alice, Bob and Eve's system is quantum, (ii) the reduced system of Alice and Bob satisfies the three Hardy zero constraints, and (iii) the reduced system of Alice and Bob achieves some value $0 < p \leq P_{Hardy}^{w=w_0, Q}$ for the Hardy probability, i.e.,

$$\begin{aligned} & \max P_{guess}(A, B|A_0, B_0, E) \\ & s.t. \quad P_{A,B|X,Y}(0, 1|A_0, B_1) = P_{A,B|X,Y}(1, 0|A_1, B_0) = P_{A,B|X,Y}(0, 0|A_1, B_1) = 0, \\ & \quad P_{A,B|X,Y}(0, 0|A_0, B_0) + w_0 P_{A,B|X,Y}(1, 1|A_0, B_0) = p, \\ & \quad P_{A,B,E|X,Y,Z} \in \mathcal{Q}, \end{aligned} \quad (33)$$

where $\mathcal{Q}$ denotes the set of three-party quantum boxes.

When the three zero constraints are satisfied, solving Eq. (26) for $P_{A,B|X,Y}(0, 0|A_0, B_0) + w_0 P_{A,B|X,Y}(1, 1|A_0, B_0) = p$ gives rise to two different values of θ , namely

$$\begin{aligned} \theta_1^{p,w_0} &= \arcsin \left(\frac{1-p}{3} + \frac{2}{3} \sqrt{1+10p+p^2-12w_0} \sin \left[\frac{\pi}{6} \right. \right. \\ & \quad \left. \left. - \frac{1}{3} \arccos \left(\frac{p^3+15p^2+p(39-18w_0)-36w_0-1}{\sqrt{(1+10p+p^2-12w_0)^3}} \right) \right] \right), \\ \theta_2^{p,w_0} &= \arcsin \left(\frac{1-p}{3} + \frac{2}{3} \sqrt{1+10p+p^2-12w_0} \sin \left[\frac{\pi}{6} \right. \right. \\ & \quad \left. \left. + \frac{1}{3} \arccos \left(\frac{p^3+15p^2+p(39-18w_0)-36w_0-1}{\sqrt{(1+10p+p^2-12w_0)^3}} \right) \right] \right). \end{aligned} \quad (34)$$

Importantly, the measurements on Alice and Bob's system for the two corresponding states $|\psi_\theta\rangle$ are also fixed (and different) as specified in Eq. (24) so that the zero constraints cannot be satisfied by mixed states on Alice and Bob's system.

Therefore, Eve's strategy in this case just consists of a mixture of extreme quantum boxes (for which the state of Alice and Bob's system is pure and decoupled from that of Eve) under the constraint that the observed Hardy probability is p . For any extreme quantum behavior $\{P_{A,B|X,Y}\}_{\theta^{p,w_0}}$ parameterized by the value θ^{p,w_0} , one can readily calculate the guessing probability directly from the behavior as

$$\begin{aligned} [P_{guess}(A, B|A_0, B_0, E)]_{\theta^{p,w_0}} &= \max_{\{a,b\}} [P_{A,B|X,Y}(a, b|A_0, B_0)]_{\theta^{p,w_0}} \\ &= \begin{cases} [P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta^{p,w_0}}, & 0 < \theta^{p,w_0} \leq \theta^{w_0} \\ [P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta^{p,w_0}}, & \theta^{w_0} < \theta^{p,w_0} \leq \frac{\pi}{2} \end{cases} \end{aligned} \quad (35)$$

where $\theta^{w_0} = \arcsin \left(-4 \left(\frac{2}{3(9+\sqrt{177})} \right)^{\frac{1}{3}} + \frac{2}{3} \left(9 + \sqrt{177} \right)^{\frac{1}{3}} \right) \approx 1.1356$ which corresponds to the optimal quantum behaviour $P_{Hardy}^{w_0, Q}$. Here $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_\theta =$

$[P_{A,B|X,Y}(1, 0|A_0, B_0)]_\theta = \frac{\sin^3 \theta}{2(2-\sin \theta)^2}$ and $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_\theta = \frac{1}{2} + \frac{\cos \theta (2+\sin \theta)(1-\sin \theta)^{\frac{1}{2}}}{2(2-\sin \theta)(1+\sin \theta)^{\frac{1}{2}}} - \frac{\sin^3 \theta}{2(2-\sin \theta)^2}$. Note that $\theta_1^{p,w_0} < \theta^{w_0} < \theta_2^{p,w_0}$ for all $p \in (0, P_{Hardy}^{w=w_0, Q})$ and the corresponding guessing probabilities for these two extreme boxes are related as $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}} \geq$

$\left[P_{A,B|X,Y}(0,1|A_0,B_0)\right]_{\theta_2^{p,w_0}}, \forall p \in (0, P_{Hardy}^{w_0,Q}]$. Furthermore, as a function of p , the probabilities $\left[P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{\theta_1^{p,w_0}}$ and $\left[P_{A,B|X,Y}(0,1|A_0,B_0)\right]_{\theta_2^{p,w_0}}$ are both concave and monotonically decreasing (see Fig. 5).

The general strategy of any adversary Eve is thus to provide Alice and Bob with (a mixture of) extreme quantum boxes $\{P_{A,B|X,Y}\}$ that achieve the Hardy probability p . To do this, she may admix some local deterministic boxes (which allow a guessing probability of 1) with quantum behaviors that achieve a Hardy probability in the range $(p, P_{Hardy}^{w_0,Q}]$. Solving for the optimal admixture of extreme boxes for which the guessing probability is given by the equation (35) with local boxes from the Tables 1 and 2 gives the guessing probability for any given $p \in [0, P_{Hardy}^{w_0,Q}]$.

From Appendix A, we know there are totally 5 local hidden variable deterministic behaviours which satisfy the three Hardy zero constraints. The local boxes shown in Table 1 satisfy $\left[P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{LHV_I} = 1$, and these boxes achieve a Hardy probability $\left[P_{A,B|X,Y}(0,0|A_0,B_0) + w_0 P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{LHV_I} = w_0 < 0$. Thus, when Eve chooses a probabilistic mixture of a deterministic box from Table 1 and any pure quantum behaviour $(\theta_1^{\tilde{p},w_0})$ with $p < \tilde{p} \leq P_{Hardy}^{w_0,Q}$, the following equation holds (from the constraint that $P_{Hardy} = p$):

$$r \cdot \tilde{p} + (1 - r) \cdot w_0 = p \quad \Rightarrow \quad r = \frac{p - w_0}{\tilde{p} - w_0}. \quad (36)$$

Such a mixture can not increase the guessing probability, due to the fact that

$$\begin{aligned} \frac{p - w_0}{\tilde{p} - w_0} \cdot \left[P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{\theta_1^{\tilde{p},w_0}} + \left(1 - \frac{p - w_0}{\tilde{p} - w_0}\right) \cdot 1 &\leq \left[P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{\theta_1^{p,w_0}} \\ \forall p, \tilde{p} \text{ with } 0 \leq p < \tilde{p} &\leq P_{Hardy}^{w_0,Q}. \end{aligned} \quad (37)$$

Therefore, the admixture of local deterministic boxes from Table 1 does not increase the guessing probability.

On the other hand, any local deterministic box from Table 2 satisfies $\left[P_{A,B|X,Y}(0,1|A_0,B_0)\right]_{LHV_{II}} = 1$ and achieves the zero Hardy probability $\left[P_{A,B|X,Y}(0,0|A_0,B_0) + w_0 P_{A,B|X,Y}(1,1|A_0,B_0)\right]_{LHV_{II}} = 0$. When Eve chooses a probabilistic mixture of a deterministic box from Table 2 and any pure quantum behavior $(\theta_2^{\tilde{p},w_0})$ with $p < \tilde{p} \leq P_{Hardy}^{w_0,Q}$, the following equation holds (from the constraint that $P_{Hardy} = p$)

$$r \cdot \tilde{p} + (1 - r) \cdot 0 = p \quad \Rightarrow \quad r = \frac{p}{\tilde{p}} \quad (38)$$

We can find the optimal $\tilde{p}$ which maximizes the guessing probability of Eve:

$$\begin{aligned} \max_{\tilde{p}} \quad & \frac{p}{\tilde{p}} \cdot \left[P_{A,B|X,Y}(0,1|A_0,B_0)\right]_{\theta_2^{\tilde{p},w_0}} + \left(1 - \frac{p}{\tilde{p}}\right) \cdot 1 \\ \text{s.t.} \quad & p < \tilde{p} \leq P_{Hardy}^{w_0,Q}, \\ & \forall p \in (0, P_{Hardy}^{w_0,Q}). \end{aligned} \quad (39)$$

The above problem is equivalent to find the $\tilde{p}$ on the curve of the function $\left[P_{A,B|X,Y}(0,1|A_0,B_0)\right]_{\theta_2^{p,w_0}}$ (as the function of p) where the tangent intersects the de-

terministic strategy point $(0, 1)$. That means

$$\left. \frac{\partial [P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}}{\partial p} \right|_{\tilde{p}} \cdot \tilde{p} + 1 = [P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{\tilde{p},w_0}} \quad (40)$$

The solution of the above optimization on $\tilde{p}$ is denoted as $\tilde{p}^* \approx 0.01563$. From the results, we obtain the tangent curve of $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$ (as the function of p),

$$\frac{([P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{\tilde{p}^*,w_0}}) - 1}{\tilde{p}^*} \cdot p + 1 \quad (41)$$

As shown in Fig. 5, the relation $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}} \geq [P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$ holds for $p \in (0, P_{Hardy}^{w_0,Q}]$. The tangent curve of $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$ must intersect the curve of $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}}$ at a certain point for which we denote the horizontal ordinate as p^* . Therefore, in any Eve's mixed strategy for the value $p \in [0, P_{Hardy}^{w_0,Q}]$, Eve's guessing probability is given as

$$P_{guess}(A, B|A_0, B_0, E) = \begin{cases} \frac{([P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{\tilde{p}^*,w_0}}) - 1}{\tilde{p}^*} \cdot p + 1 & 0 \leq p \leq p^* \\ [P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}} & p^* < p \leq P_{Hardy}^{w_0,Q} \end{cases} \quad (42)$$

where $p^* \approx 0.01366$.

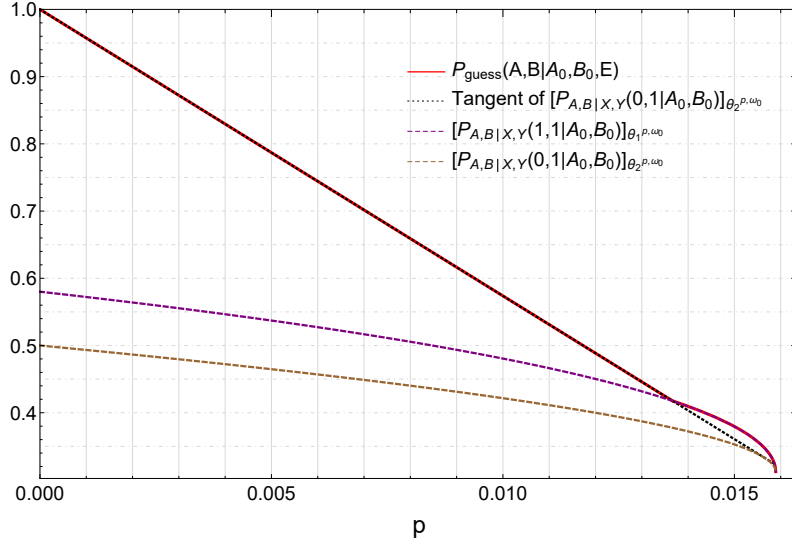


Figure 5: $P_{guess}(A, B|A_0, B_0, E)$, $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}}$, $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$ and the tangent of $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$ versus the Hardy probability p . The solid red line denotes the guessing probability $P_{guess}(A, B|A_0, B_0, E)$. The dotted black line denotes the tangent of the probability $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$. The dashed purple and brown lines denote the probabilities $[P_{A,B|X,Y}(1, 1|A_0, B_0)]_{\theta_1^{p,w_0}}$, $[P_{A,B|X,Y}(0, 1|A_0, B_0)]_{\theta_2^{p,w_0}}$, respectively.

C α -CHSH and its robust self-testing statement

In this section, We first introduce a family of bipartite Bell expressions named α -CHSH (used in Eq. (12)) with a parameter $\alpha > \frac{1}{3}$:

$$I_\alpha = \alpha A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \quad (43)$$

where A_0, A_1 are two binary observables for Alice and B_0, B_1 are two binary observables for Bob.

The maximum value of I_α in quantum theory is $I_\alpha^Q = (\alpha + 1)\sqrt{\frac{\alpha+1}{\alpha}}$, and it's achieved by the specific reference quantum system (up to a local isometry) :

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ A_0 &= \sigma_z, \quad A_1 = \frac{\alpha-1}{2\alpha}\sigma_z + \frac{\sqrt{(\alpha+1)(3\alpha-1)}}{2\alpha}\sigma_x \\ B_0 &= \frac{2\alpha-1}{2\alpha}\sqrt{\frac{\alpha+1}{\alpha}}\sigma_z + \frac{1}{2\alpha}\sqrt{\frac{3\alpha-1}{\alpha}}\sigma_x, \quad B_1 = \frac{1}{2}\sqrt{\frac{\alpha+1}{\alpha}}\sigma_z - \frac{1}{2}\sqrt{\frac{3\alpha-1}{\alpha}}\sigma_x \end{aligned} \quad (44)$$

The maximum value of I_α in classical theory is easily verified to be:

$$I_\alpha^{LHV} \leq \begin{cases} 3 - \alpha, & \frac{1}{3} < \alpha \leq 1 \\ 1 + \alpha, & 1 < \alpha \end{cases} \quad (45)$$

Let define the shifted Bell operator as $\overline{I}_\alpha := I_\alpha^Q \mathbb{I} - I_\alpha = I_\alpha^Q \mathbb{I} - \alpha A_0 B_0 - A_0 B_1 - A_1 B_0 + A_1 B_1$, and take a trivial monomials basis $R = [R_1 = A_0, R_2 = A_1, R_3 = B_0, R_4 = B_1]^T$ to do the sum of squares (SOS) decomposition of the shifted operator Bell $\overline{I}_\alpha = R^\dagger M_\alpha R$. Obviously, $\overline{I}_\alpha$ is inherently positive semidefinite, and we get:

$$M_\alpha = \begin{bmatrix} \frac{\sqrt{\alpha(\alpha+1)}}{2} & 0 & -\frac{\alpha}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2}\sqrt{\frac{\alpha+1}{\alpha}} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{\alpha}{2} & -\frac{1}{2} & \frac{\sqrt{\alpha(\alpha+1)}}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2}\sqrt{\frac{\alpha+1}{\alpha}} \end{bmatrix} \geq 0 \quad (46)$$

One can do Cholesky Decomposition of M_α to get two polynomials P_1, P_2 and the shifted Bell operator is expressed as $\overline{I}_\alpha = P_1^\dagger P_1 + P_2^\dagger P_2$.

$$\begin{aligned} P_1 &= \frac{[\alpha(1+\alpha)]^{\frac{1}{4}}}{\sqrt{2}}A_0 - \frac{\alpha^{\frac{3}{4}}}{\sqrt{2}(1+\alpha)^{\frac{1}{4}}}B_0 - \frac{1}{\sqrt{2}[\alpha(1+\alpha)]^{\frac{1}{4}}}B_1, \\ P_2 &= \frac{(1+\alpha)^{\frac{1}{4}}}{\sqrt{2}\alpha^{\frac{1}{4}}}A_1 - \frac{\alpha^{\frac{1}{4}}}{\sqrt{2}(1+\alpha)^{\frac{1}{4}}}B_0 + \frac{\alpha^{\frac{1}{4}}}{\sqrt{2}(1+\alpha)^{\frac{1}{4}}}B_1. \end{aligned} \quad (47)$$

Due to the experimental noise, usually the ideal maximum quantum value I_α^Q cannot be observed in the experiments but up to some error term e . To distinguish the notations used by the reference quantum system above, we will refer to the physical state and observables (hermitian and dichotomic) to prime notations $|\psi'\rangle, A'_0, A'_1, B'_0, B'_1$.

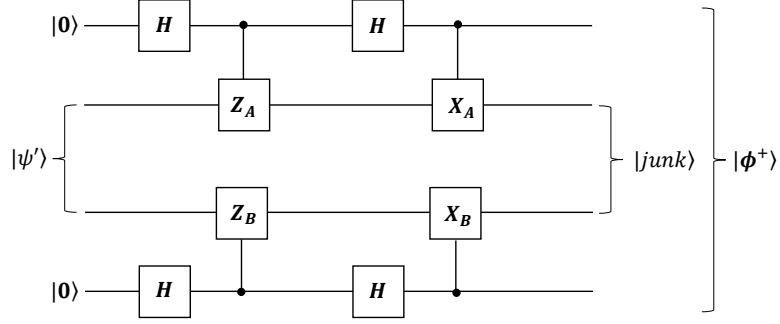


Figure 6: The local isometry $\Phi = \Phi_A \otimes \Phi_B$ used to self-test the reference state and measurements.

This Bell expression I_α provides a robust self-test for its reference state $|\phi^+\rangle$ and reference observables A_0, A_1, B_0, B_1 , to prove this robust self-testing statement, we show there exist a local isometry $\Phi = \Phi_A \otimes \Phi_B$, as shown in Fig. 6 acting on the physical system and its output state is close to the corresponding reference system in a noise-tolerant way (the error term is of order $O(\sqrt{e})$) with some $|junk\rangle$ state. More precisely:

$$\left\| \Phi \left(A'_x \otimes B'_y |\psi'\rangle \right) - \left(A_x \otimes B_y |\phi^+\rangle \right) \otimes |junk\rangle \right\| \leq O(\sqrt{e}) \quad (48)$$

where $x, y \in \{-1, 0, 1\}$, the subscript -1 refers to $\mathbb{I}$ and the operators X_A, X_B, Z_A, Z_B in the isometry are defined in terms of A'_x, B'_y , $x, y \in \{0, 1\}$.

Proof. The proof of the robust self-testing statement includes the following 4 steps.

Step. 1 Defining the operators in the isometry.

Firstly, we define the following four local operators (with the prime notation) in terms of A'_x, B'_y , $x, y \in \{0, 1\}$:

$$\begin{aligned} X'_A &= \frac{2\alpha}{(\alpha+1)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} A'_1 - \frac{\alpha-1}{(\alpha+1)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} A'_0, & Z'_A &= A'_0. \\ X'_B &= \frac{\alpha^{\frac{1}{2}}}{(3\alpha-1)^{\frac{1}{2}}} B'_0 - \frac{2\alpha-1}{\alpha^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} B'_1, & Z'_B &= \frac{\alpha^{\frac{1}{2}}}{(\alpha+1)^{\frac{1}{2}}} B'_0 + \frac{1}{\alpha^{\frac{1}{2}}(\alpha+1)^{\frac{1}{2}}} B'_1. \end{aligned} \quad (49)$$

In order to make the operators in the isometry unitary, we play the regularisation trick [19] on these operators. For operator X'_A , we first replace the zero eigenvalues into 1 and denote the new operator as X_A^* , then normalize the eigenvalues by $X_A = \frac{X_A^*}{|X_A^*|}$, such that the resulting operator X_A is Hermitian and unitary and has the property $X_A = \frac{X'_A}{|X'_A|}$. Then play the same regularisation trick to define X_B, Z_A, Z_B . Note that $Z'_A = A'_0$ is already unitary, so $Z_A = Z'_A$.

Step. 2 Deriving some useful bounds for physical operators.

According to the SOS decomposition (47), suppose the observation of the quantum value is $\langle I_\alpha \rangle \geq I_\alpha^Q - e$, i.e., $\langle \overline{I_\alpha} \rangle = \|P'_1|\psi'\rangle\|^2 + \|P'_2|\psi'\rangle\|^2 \leq e$, we have the following two bounds:

$$\|P'_1|\psi'\rangle\| = \left\| \frac{1}{\sqrt{2}\alpha^{\frac{1}{4}}(1+\alpha)^{\frac{1}{4}}} \left[\alpha^{\frac{1}{2}}(1+\alpha)^{\frac{1}{2}} A'_0 - \alpha B'_0 - B'_1 \right] |\psi'\rangle \right\| \leq \sqrt{e} \quad (50)$$

$$\|P'_2|\psi'\rangle\| = \left\| \frac{1}{\sqrt{2}\alpha^{\frac{3}{4}}(1+\alpha)^{\frac{1}{4}}} \left[\alpha^{\frac{1}{2}}(1+\alpha)^{\frac{1}{2}}A'_1 - \alpha B'_0 + \alpha B'_1 \right] |\psi'\rangle \right\| \leq \sqrt{e} \quad (51)$$

From (50) and (51), directly we get:

$$\|(Z'_A - Z'_B)|\psi'\rangle\| = \left\| \frac{\sqrt{2}\alpha^{\frac{1}{4}}(1+\alpha)^{\frac{1}{4}}}{\alpha^{\frac{1}{2}}(1+\alpha)^{\frac{1}{2}}} P'_1 |\psi'\rangle \right\| \leq \frac{\sqrt{2}}{\alpha^{\frac{1}{4}}(1+\alpha)^{\frac{1}{4}}} \sqrt{e} \equiv \delta_1 \quad (52)$$

$$\begin{aligned} \|(X'_A - X'_B)|\psi'\rangle\| &= \left\| \left[\frac{2\sqrt{2}\alpha^{\frac{5}{4}}}{(3\alpha-1)^{\frac{1}{2}}(1+\alpha)^{\frac{3}{4}}} P'_2 - \frac{\sqrt{2}(\alpha-1)}{\alpha^{\frac{1}{4}}(3\alpha-1)^{\frac{1}{2}}(1+\alpha)^{\frac{3}{4}}} P'_1 \right] |\psi'\rangle \right\| \\ &\leq \frac{2\sqrt{2}\alpha^{\frac{3}{2}} + \sqrt{2}|\alpha-1|}{\alpha^{\frac{1}{4}}(3\alpha-1)^{\frac{1}{2}}(1+\alpha)^{\frac{3}{4}}} \sqrt{e} \equiv \delta_2 \end{aligned} \quad (53)$$

To derive the bounds for anti-coummuting operators $\|\{X'_A, Z'_A\}|\psi'\rangle\|$ and $\|\{X'_B, Z'_B\}|\psi'\rangle\|$, we will need the following relations:

$$\begin{aligned} X_A'^2 &= \left[\frac{2\alpha A'_1 - (\alpha-1)A'_0}{(\alpha+1)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} \right]^2 = \frac{4\alpha^2 + (\alpha-1)^2}{(\alpha+1)(3\alpha-1)} \mathbb{I} - \frac{2\alpha(\alpha-1)}{(\alpha+1)(3\alpha-1)} \{A'_0, A'_1\}, \\ Z_A'^2 &= A_0'^2 = \mathbb{I}, \\ X_B'^2 &= \left[\frac{\alpha B'_0 - (2\alpha-1)B'_1}{\alpha^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} \right]^2 = \frac{\alpha^2 + (2\alpha-1)^2}{\alpha(3\alpha-1)} \mathbb{I} - \frac{2\alpha-1}{3\alpha-1} \{B'_0, B'_1\}, \\ Z_B'^2 &= \left[\frac{\alpha B'_0 + B'_1}{\alpha^{\frac{1}{2}}(\alpha+1)^{\frac{1}{2}}} \right]^2 = \frac{\alpha^2 + 1}{\alpha(\alpha+1)} \mathbb{I} + \frac{1}{\alpha+1} \{B'_0, B'_1\}. \end{aligned} \quad (54)$$

Thus, the following equations holds true:

$$\begin{aligned} &\|[\{X'_A, Z'_A\} - \{X'_B, Z'_B\}]|\psi'\rangle\| \\ &\leq \|X'_A(Z'_A - Z'_B)|\psi'\rangle\| + \|X'_B(Z'_A - Z'_B)|\psi'\rangle\| + \|Z'_A(X'_A - X'_B)|\psi'\rangle\| + \|Z'_B(X'_A - X'_B)|\psi'\rangle\| \\ &= \|(X'_A - X'_B)|\psi'\rangle\| + \sqrt{\langle\psi'| (Z'_A - Z'_B) X_A'^2 (Z'_A - Z'_B) |\psi'\rangle} \\ &\quad + \sqrt{\langle\psi'| (Z'_A - Z'_B) X_B'^2 (Z'_A - Z'_B) |\psi'\rangle} + \sqrt{\langle\psi'| (X'_A - X'_B) Z_B'^2 (X'_A - X'_B) |\psi'\rangle} \\ &\leq \delta_2 + \sqrt{\frac{4\alpha^2 + (\alpha-1)^2}{(\alpha+1)(3\alpha-1)} \delta_1^2 + \frac{2\alpha|\alpha-1|}{(\alpha+1)(3\alpha-1)} \|(A'_0 - A'_1)(Z'_A - Z'_B)|\psi'\rangle\|^2} \\ &\quad + \sqrt{\frac{\alpha^2 + (2\alpha-1)^2}{\alpha(3\alpha-1)} \delta_1^2 + \frac{|2\alpha-1|}{3\alpha-1} \|(B'_0 - B'_1)(Z'_A - Z'_B)|\psi'\rangle\|^2} \\ &\quad + \sqrt{\frac{\alpha^2 + 1}{\alpha(\alpha+1)} \delta_2^2 + \frac{1}{\alpha+1} \|(B'_0 + B'_1)(X'_A - X'_B)|\psi'\rangle\|^2} \\ &\leq \delta_2 + \sqrt{\frac{4\alpha^2 + (\alpha-1)^2}{(\alpha+1)(3\alpha-1)} + \frac{8\alpha|\alpha-1|}{(\alpha+1)(3\alpha-1)}} \delta_1 \\ &\quad + \sqrt{\frac{\alpha^2 + (2\alpha-1)^2}{\alpha(3\alpha-1)} + \frac{4|2\alpha-1|}{3\alpha-1}} \delta_1 + \sqrt{\frac{\alpha^2 + 1}{\alpha(\alpha+1)} + \frac{4}{\alpha+1}} \delta_2 \\ &\equiv \delta_3 \end{aligned} \quad (55)$$

The left side of (55) can also be expressed as:

$$\begin{aligned}
& \|[\{X'_A, Z'_A\} - \{X'_B, Z'_B\}]|\psi'\rangle\| \\
&= \left\| \left[\frac{2}{(1+\alpha)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} [\alpha\{A'_0, A'_1\} - (1-\alpha)\{B'_0, B'_1\}] - \frac{2(\alpha-1)(2\alpha-1)}{\alpha(3\alpha-1)^{\frac{1}{2}}(1+\alpha)^{\frac{1}{2}}} \mathbb{I} \right] |\psi'\rangle \right\| \\
&= \left\| \left[\frac{2\sqrt{2}\alpha^{\frac{3}{4}}}{(1+\alpha)^{\frac{3}{4}}(3\alpha-1)^{\frac{1}{2}}} (A'_1 P'_1 + \alpha^{\frac{1}{2}} A'_0 P'_2) + \frac{2\sqrt{2}\alpha^{\frac{3}{4}}}{(1+\alpha)^{\frac{5}{4}}(3\alpha-1)^{\frac{1}{2}}} (\alpha B'_0 P'_2 + B'_1 P'_2 + \alpha^{\frac{1}{2}} B'_0 P'_1 - \alpha^{\frac{1}{2}} B'_1 P'_1) \right. \right. \\
&\quad \left. \left. + \frac{2(\alpha-1)}{(1+\alpha)^{\frac{3}{2}}(3\alpha-1)^{\frac{1}{2}}} \{B'_0, B'_1\} - \frac{2(\alpha-1)^2}{\alpha(1+\alpha)^{\frac{3}{2}}(3\alpha-1)^{\frac{1}{2}}} \mathbb{I} \right] |\psi'\rangle \right\| \\
&\geq \frac{2|\alpha-1|}{(1+\alpha)^{\frac{3}{2}}(3\alpha-1)^{\frac{1}{2}}} \left\| \left(\{B'_0, B'_1\} - \frac{\alpha-1}{\alpha} \mathbb{I} \right) |\psi'\rangle \right\| - \frac{2\sqrt{2}\alpha^{\frac{3}{4}}(1+\alpha^{\frac{1}{2}}) \left[(1+\alpha)^{\frac{1}{2}} + (1+\alpha^{\frac{1}{2}}) \right]}{(1+\alpha)^{\frac{5}{4}}(3\alpha-1)^{\frac{1}{2}}} \sqrt{e} \\
&\hspace{25em} (56)
\end{aligned}$$

From the above two inequalities (55) and (56), we have:

$$\begin{aligned}
\left\| \left(\{B'_0, B'_1\} - \frac{\alpha-1}{\alpha} \mathbb{I} \right) |\psi'\rangle \right\| &\leq \frac{(1+\alpha)^{\frac{3}{2}}(3\alpha-1)^{\frac{1}{2}}}{2|\alpha-1|} \delta_3 \\
&\quad + \frac{\sqrt{2}\alpha^{\frac{3}{4}}(1+\alpha^{\frac{1}{2}})(1+\alpha)^{\frac{1}{4}} \left[(1+\alpha)^{\frac{1}{2}} + (1+\alpha^{\frac{1}{2}}) \right]}{|\alpha-1|} \sqrt{e} \\
&\equiv \delta_4
\end{aligned} \tag{57}$$

Then we can get:

$$\begin{aligned}
\|\{X'_B, Z'_B\}|\psi'\rangle\| &= \frac{2|\alpha-1|}{(3\alpha-1)^{\frac{1}{2}}(\alpha+1)^{\frac{1}{2}}} \left\| \left(\frac{\alpha-1}{\alpha} \mathbb{I} - \{B'_0, B'_1\} \right) |\psi'\rangle \right\| \\
&\leq \frac{2|\alpha-1|}{(3\alpha-1)^{\frac{1}{2}}(\alpha+1)^{\frac{1}{2}}} \delta_4 \equiv \delta_5
\end{aligned} \tag{58}$$

$$\begin{aligned}
\|\{X'_A, Z'_A\}|\psi'\rangle\| &= \frac{2\alpha}{(\alpha+1)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}} \left\| \left(\frac{\alpha-1}{\alpha} \mathbb{I} - \{A'_0, A'_1\} \right) |\psi'\rangle \right\| \\
&\leq \delta_3 + \|\{X'_B, Z'_B\}|\psi'\rangle\| \\
&\leq \delta_3 + \delta_5 \equiv \delta_6
\end{aligned} \tag{59}$$

From (59), we can also get

$$\left\| \left(\{A'_0, A'_1\} - \frac{\alpha-1}{\alpha} \mathbb{I} \right) |\psi'\rangle \right\| \leq \frac{(\alpha+1)^{\frac{1}{2}}(3\alpha-1)^{\frac{1}{2}}}{2\alpha} \delta_6 \equiv \delta_7 \tag{60}$$

Note that $\delta_1 \sim \delta_7$ are all of order $O(\sqrt{e})$.

Step. 3 Deriving the bounds for regularized operators.

Next, we will derive the similar bounds like (52), (53), (58) and (59) for regularized operators:

$$\begin{aligned}
\|(Z_A - Z_B)|\psi'\rangle\| &= \|(Z_A - Z'_B) + (Z'_B - Z_B)|\psi'\rangle\| \\
&\leq \|(Z'_A - Z'_B)|\psi'\rangle\| + \|Z_B(\mathbb{I} - |Z'_B\rangle\langle Z'_B|)|\psi'\rangle\| \\
&= \|(Z'_A - Z'_B)|\psi'\rangle\| + \|(\mathbb{I} - |Z'_A\rangle\langle Z'_A|)|\psi'\rangle\| \\
&\leq \|(Z'_A - Z'_B)|\psi'\rangle\| + \|(\mathbb{I} - Z'_A Z'_B)|\psi'\rangle\| \\
&= 2\|(Z'_A - Z'_B)|\psi'\rangle\| = 2\delta_1 \equiv \epsilon_1
\end{aligned} \tag{61}$$

$Z_A = Z'_A$ is an unitary operator. In the forth line, we use the operator inequality $A \leq |A|$.

$$\begin{aligned}
\|(X_A - X_B)|\psi'\rangle\| &\leq \|(X_A - X'_A)|\psi'\rangle\| + \|(X_B - X'_B)|\psi'\rangle\| + \|(X'_A - X'_B)|\psi'\rangle\| \\
&= \|X_A(\mathbb{I} - |X'_A\rangle\langle X'_A|)|\psi'\rangle\| + \|X_B(\mathbb{I} - |X'_B\rangle\langle X'_B|)|\psi'\rangle\| + \|(X'_A - X'_B)|\psi'\rangle\| \\
&\leq \|(\mathbb{I} - |X'_A\rangle\langle X'_A| + |X'_B\rangle\langle X'_B|)|\psi'\rangle\| + \|(\mathbb{I} - |X'_B\rangle\langle X'_B|)|\psi'\rangle\| + \|(X'_A - X'_B)|\psi'\rangle\| \\
&\leq 2\|(\mathbb{I} - |X'_B\rangle\langle X'_B|)|\psi'\rangle\| + 2\|(X'_A - X'_B)|\psi'\rangle\| \\
&\leq 2\|(\mathbb{I} + |X'_B\rangle\langle X'_B|)(\mathbb{I} - |X'_B\rangle\langle X'_B|)|\psi'\rangle\| + 2\delta_2 \\
&= 2\left\|\left(\mathbb{I} - \frac{\alpha^2 + (2\alpha - 1)^2}{\alpha(3\alpha - 1)}\mathbb{I} + \frac{2\alpha - 1}{3\alpha - 1}\{B'_0, B'_1\}\right)|\psi'\rangle\right\| + 2\delta_2 \\
&= \frac{2|2\alpha - 1|}{3\alpha - 2}\left\|\left(\{B'_0, B'_1\} - \frac{\alpha - 1}{\alpha}\mathbb{I}\right)|\psi'\rangle\right\| + 2\delta_2 \\
&\leq \frac{2|2\alpha - 1|}{3\alpha - 2}\delta_4 + 2\delta_2 \equiv \epsilon_2
\end{aligned} \tag{62}$$

In the fifth line, we use the operator inequality $\mathbb{I} + |A| \geq \mathbb{I}$.

$$\begin{aligned}
\|\{X_A, Z_A\}|\psi'\rangle\| &\leq \|X_A(Z_A - Z'_A)|\psi'\rangle\| + \|Z_A(X_A - X'_A)|\psi'\rangle\| + \|(Z_A - Z'_A)X'_A|\psi'\rangle\| \\
&\quad + \|(X_A - X'_A)Z'_A|\psi'\rangle\| + \|\{X'_A, Z'_A\}|\psi'\rangle\| \\
&= \|(\mathbb{I} - |X'_A\rangle\langle X'_A|)|\psi'\rangle\| + \|(\mathbb{I} - |X'_A\rangle\langle X'_A|)Z'_A|\psi'\rangle\| + \|\{X'_A, Z'_A\}|\psi'\rangle\| \\
&\leq \frac{|2\alpha - 1|}{3\alpha - 2}\delta_4 + \delta_2 + \delta_6 + \|(\mathbb{I} - X_A'^2)Z'_A|\psi'\rangle\| \\
&= \frac{|2\alpha - 1|}{3\alpha - 2}\delta_4 + \delta_2 + \delta_6 \\
&\quad + \frac{2|\alpha - 1|}{\alpha(\alpha + 1)(3\alpha - 1)}\left\|\left(\{A'_0, A'_1\} - \frac{\alpha - 1}{\alpha}\mathbb{I}\right)Z'_A|\psi'\rangle\right\| \\
&\leq \frac{|2\alpha - 1|}{3\alpha - 2}\delta_4 + \delta_2 + \delta_6 + \frac{2|\alpha - 1|}{\alpha(\alpha + 1)(3\alpha - 1)}\delta_7 \equiv \epsilon_3
\end{aligned} \tag{63}$$

In the third line, we use the intermediate result of (62) and play the same trick as line 5 of (62). In the last line, we use the bound (60).

$$\begin{aligned}
\|\{X_B, Z_B\}|\psi'\rangle\| &\leq \|X_B(Z_B - Z_A)|\psi'\rangle\| + \|Z_B(X_B - X_A)|\psi'\rangle\| + \|X_A(Z_B - Z_A)|\psi'\rangle\| \\
&\quad + \|Z_A(X_B - X_A)|\psi'\rangle\| + \|\{X_A, Z_A\}|\psi'\rangle\| \\
&\leq 2\epsilon_1 + 2\epsilon_2 + \epsilon_3 \equiv \epsilon_4
\end{aligned} \tag{64}$$

Similarly, $\epsilon_1 \sim \epsilon_4$ are all of order $O(\sqrt{e})$.

Step. 4 Using the derived bounds to prove the robust self-testing statements.

With these conditions (61), (62), (63) and (64), it's easy to see the following statement holds:

$$\left\|\Phi\left(A'_x \otimes B'_y|\psi'\rangle\right) - \left(A_x \otimes B_y|\phi^+\rangle\right) \otimes |junk\rangle\right\| \leq O(\sqrt{e}) \tag{65}$$

where $x, y \in \{-1, 0, 1\}$, the subscript -1 refers to $A_{-1} = B_{-1} = \mathbb{I}$ and the isometry is shown as Fig. 6. The output of the isometry is:

$$\begin{aligned} \Phi(A'_x \otimes B'_y |\psi'\rangle) = & \frac{1}{4} \left[|00\rangle \otimes (\mathbb{I} + Z_A)(\mathbb{I} + Z_B) A'_x \otimes B'_y |\psi'\rangle \right. \\ & + |01\rangle \otimes X_B(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) A'_x \otimes B'_y |\psi'\rangle \\ & + |10\rangle \otimes X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B) A'_x \otimes B'_y |\psi'\rangle \\ & \left. + |11\rangle \otimes X_A X_B (\mathbb{I} - Z_A)(\mathbb{I} - Z_B) A'_x \otimes B'_y |\psi'\rangle \right] \end{aligned} \quad (66)$$

1. **Robust self-testing the state $|\psi'\rangle$.**

When $x = y = -1$, the second and third terms of (66) are bounded by:

$$\begin{aligned} \|(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi'\rangle\| &= \|(\mathbb{I} - Z_A)(\mathbb{I} + Z_B) |\psi'\rangle\| \\ &\leq \|(Z_A - Z_B) |\psi'\rangle\| + \|(\mathbb{I} - Z_A Z_B) |\psi'\rangle\| \\ &\leq 2 \|(Z_A - Z_B) |\psi'\rangle\| = 2\epsilon_1 \end{aligned} \quad (67)$$

The difference of the first and fourth terms of (66) is:

$$\begin{aligned} & \| [X_A X_B (\mathbb{I} - Z_A)(\mathbb{I} - Z_B) - (\mathbb{I} + Z_A)(\mathbb{I} + Z_B)] |\psi'\rangle \| \\ & \leq \| [(\mathbb{I} + Z_A)(\mathbb{I} + Z_B)(X_A X_B - \mathbb{I})] |\psi'\rangle \| \\ & \quad + 2 \|\{X_B, Z_B\} |\psi'\rangle\| + 2 \|\{X_A, Z_A\} |\psi'\rangle\| \\ & \leq 4 \|(X_A - X_B) |\psi'\rangle\| + 2(\epsilon_3 + \epsilon_4) \\ & = 4\epsilon_2 + 2\epsilon_3 + 2\epsilon_4 \end{aligned} \quad (68)$$

Thus $\|\Phi(|\psi'\rangle) - |\phi^+\rangle \otimes \frac{\sqrt{2}}{4}(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi'\rangle\| \leq 4\epsilon_1 + 4\epsilon_2 + 2\epsilon_3 + 2\epsilon_4 = O(\sqrt{e})$.

2. **Robust self-testing the local measurements A'_x , $x \in \{0, 1\}$ on Alice's side.**

Since A'_x , $x \in \{0, 1\}$ is the linear combination of Z'_A and X'_A , here we take the local operator to be either Z'_A or X'_A , and the corresponding reference operators is σ_z^A or σ_x^A (the Pauli operators).

When $A'_x = Z'_A$, $y = -1$, the second and third terms of (66) are bounded by:

$$\begin{aligned} \|X_B(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) Z'_A |\psi'\rangle\| &= \|X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B) Z'_A |\psi'\rangle\| \\ &= \|(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi'\rangle\| \leq 2\epsilon_1. \end{aligned} \quad (69)$$

The difference of the fourth term and the negative of the first term in (66) is:

$$\begin{aligned} & \| [X_A X_B (\mathbb{I} - Z_A)(\mathbb{I} - Z_B) Z'_A - (-\mathbb{I} + Z_A)(\mathbb{I} + Z_B) Z'_A] |\psi'\rangle \| \\ & = \| [(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) - X_A X_B (\mathbb{I} - Z_A)(\mathbb{I} - Z_B)] |\psi'\rangle \| \\ & \leq 4\epsilon_2 + 2\epsilon_3 + 2\epsilon_4. \end{aligned} \quad (70)$$

Thus $\|\Phi(Z'_A |\psi'\rangle) - \sigma_z^A |\phi^+\rangle \otimes \frac{\sqrt{2}}{4}(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) Z'_A |\psi'\rangle\| \leq 4\epsilon_1 + 4\epsilon_2 + 2\epsilon_3 + 2\epsilon_4 = O(\sqrt{e})$.

For $A'_x = X'_A$, $y = -1$, we will use the fact that Φ is linear and preserves the norms, $\|\Phi(X'_A |\psi'\rangle) - \Phi(X_A |\psi'\rangle)\| = \|(X'_A - X_A) |\psi'\rangle\| = \frac{\epsilon_2}{2}$. This allows us to bound the (65) with $A'_x = X'_A$, $y = -1$ by $A'_x = X_A$, $y = -1$.

When $A'_x = X_A, y = -1$, the difference of the second and third terms of (66) is bounded by:

$$\begin{aligned}
& \left\| [X_B(\mathbb{I} + Z_A)(\mathbb{I} - Z_B)X_A - X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B)X_A] |\psi'\rangle \right\| \\
& \leq \left\| (\mathbb{I} + Z_A)(\mathbb{I} + Z_B)(X_A X_B - \mathbb{I}) |\psi'\rangle \right\| \\
& \quad + 2 \left\| \{X_B, Z_B\} X_A |\psi'\rangle \right\| + 2 \left\| \{X_A, Z_A\} X_A |\psi'\rangle \right\| \\
& \leq 4 \left\| (X_A - X_B) |\psi'\rangle \right\| + 2 \left\| \{X_B, Z_B\} |\psi'\rangle \right\| + 2 \left\| \{X_A, Z_A\} |\psi'\rangle \right\| \\
& \leq 4\epsilon_2 + 2\epsilon_3 + 2\epsilon_4.
\end{aligned} \tag{71}$$

And the first term and the fourth term of (66) are bounded by:

$$\begin{aligned}
\left\| (\mathbb{I} + Z_A)(\mathbb{I} + Z_B)X_A |\psi'\rangle \right\| & \leq \left\| \{X_A, Z_A\}(\mathbb{I} + Z_B) |\psi'\rangle \right\| + \left\| X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B) |\psi'\rangle \right\| \\
& \leq 2 \left\| \{X_A, Z_A\} |\psi'\rangle \right\| + \left\| (\mathbb{I} - Z_A)(\mathbb{I} + Z_B) |\psi'\rangle \right\| \\
& \leq 2\epsilon_1 + 2\epsilon_3, \\
\left\| X_A X_B (\mathbb{I} - Z_A)(\mathbb{I} - Z_B)X_A |\psi'\rangle \right\| & \leq \left\| X_B(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi'\rangle \right\| + \left\| X_A X_B \{X_A, Z_A\}(\mathbb{I} - Z_B) |\psi'\rangle \right\| \\
& \leq \left\| (\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi'\rangle \right\| + 2 \left\| \{X_A, Z_A\} |\psi'\rangle \right\| \\
& \leq 2\epsilon_1 + 2\epsilon_3.
\end{aligned} \tag{72}$$

Thus $\left\| \Phi(X_A |\psi'\rangle) - \sigma_x^A |\phi^+\rangle \otimes \frac{\sqrt{2}}{4} X_B (\mathbb{I} + Z_A)(\mathbb{I} - Z_B)X_A |\psi'\rangle \right\| \leq 4\epsilon_1 + 4\epsilon_2 + 6\epsilon_3 + 2\epsilon_4$. Then:

$$\begin{aligned}
& \left\| \Phi(X'_A |\psi'\rangle) - \sigma_x^A |\phi^+\rangle \otimes \frac{\sqrt{2}}{4} X_B (\mathbb{I} + Z_A)(\mathbb{I} - Z_B)X_A |\psi'\rangle \right\| \\
& \leq 4\epsilon_1 + 4\epsilon_2 + 6\epsilon_3 + 2\epsilon_4 + \left\| \Phi(X'_A |\psi'\rangle) - \Phi(X_A |\psi'\rangle) \right\| \\
& \leq 4\epsilon_1 + \frac{9}{2}\epsilon_2 + 6\epsilon_3 + 2\epsilon_4 = O(\sqrt{\epsilon})
\end{aligned} \tag{73}$$

3. Robust self-testing the local measurements B'_y , $y \in \{0, 1\}$ on Bob's side .

The proof is similar as the above case on Alice's side.

□

D The guessing probability of a classical adversary allowed to prepare arbitrary no-signaling boxes for Alice and Bob

Suppose Alice and Bob share an arbitrary bipartite no-signaling box $P_{A,B|X,Y}$ that achieves a value I_α^{Hardy} for the Bell expression (10) derived from the tilted Hardy test. The following proposition derives a bound on the probability $P_{A,B|X,Y}(a, b|A_x, B_y)$ for any pair of outcomes a, b and any pair of inputs x, y . The corresponding bound for the MDL quantity I_α^{MDL} is then readily derived by the relationship between these two quantities that $I_\alpha^{Hardy} \geq \frac{I_\alpha^{MDL}}{lh}$ (see Eq. (13)) for l, h being the lower and upper bounds on the probability of choosing measurement inputs x, y respectively. Note that when measurement inputs are chosen using an ϵ -SV source, we have $l = \left(\frac{1}{2} - \epsilon\right)^2$ and $h = \left(\frac{1}{2} + \epsilon\right)^2$.

Proposition. *Consider any bipartite no-signaling box $P_{A,B|X,Y}$ that achieves the value I_α^{Hardy} for the expression in (10). For any pair of measurement settings x, y and outcomes a, b , the following upper bound holds:*

$$P_{A,B|X,Y}(a, b|A_x, B_y) \leq 1 - \frac{1}{\alpha} I_\alpha^{Hardy} \quad \text{for } \alpha \in \left(\frac{1}{3}, 1\right] \tag{74}$$

and

$$P_{A,B|X,Y}(a, b|A_x, B_y) \leq 1 - I_\alpha^{Hardy} \quad \text{for } \alpha \in (1, +\infty). \quad (75)$$

Proof. In the bipartite Bell scenario with each party choosing two binary measurements Fig. 7 (a) illustrates the following relations:

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_0, B_0) + x &= c + \delta_1, \\ d &\geq c - \delta_2, \\ e' &\geq d - \delta_3, \\ P_{A,B|X,Y}(1, 1|A_0, B_0) &\geq e' - x. \end{aligned} \quad (76)$$

We derive

$$P_{A,B|X,Y}(1, 1|A_0, B_0) \geq P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_1 - \delta_2 - \delta_3. \quad (77)$$

In the following, we will discuss the two cases $\alpha \in (\frac{1}{3}, 1]$ and $\alpha \in (1, +\infty)$ respectively.

Case 1. $\alpha \in (\frac{1}{3}, 1]$. In this case, we observe that $\max(0, \frac{1-\alpha}{2}) = \frac{1-\alpha}{2}$ and derive the bounds

$$\begin{aligned} \frac{1-\alpha}{2} + I_\alpha^{Hardy} &\leq P_{A,B|X,Y}(0, 0|A_0, B_0) \leq \frac{1+\alpha}{2} - I_\alpha^{Hardy}, \\ \frac{1-\alpha}{2} + I_\alpha^{Hardy} &\leq P_{A,B|X,Y}(1, 1|A_0, B_0) \leq \frac{1+\alpha}{2} - I_\alpha^{Hardy}, \\ \frac{1}{\alpha} I_\alpha^{Hardy} &\leq P_{A,B|X,Y}(a, b|A_x, B_y) \leq 1 - \frac{1}{\alpha} I_\alpha^{Hardy}, \quad \forall a \oplus b = x \cdot y, ((x, y) \neq (0, 0)), \\ P_{A,B|X,Y}(a, b|A_x, B_y) &\leq 1 - \frac{2}{\alpha} I_\alpha^{Hardy}, \quad \forall a \oplus b \neq x \cdot y. \end{aligned} \quad (78)$$

Firstly, we show that the following bounds hold:

From the definition of I_α^{Hardy} and the normalization constraint $P_{A,B|X,Y}(0, 0|A_0, B_0) + P_{A,B|X,Y}(1, 1|A_0, B_0) \leq 1$, we can get:

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_0, B_0) &\geq \frac{1-\alpha}{2} + I_\alpha^{Hardy} \\ P_{A,B|X,Y}(1, 1|A_0, B_0) &\leq \frac{1+\alpha}{2} - I_\alpha^{Hardy} \end{aligned} \quad (79)$$

In order to calculate the bounds of other probabilities, from Fig. 7 (b), we get the following inequalities:

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_1 &\leq c \\ P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_3 &\leq e \end{aligned} \quad (80)$$

Since $c - \delta_2 \leq d, e - \delta_2 \leq d'$, we get:

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_1 - \delta_2 &\leq d \\ P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_2 - \delta_3 &\leq d' \end{aligned} \quad (81)$$

Since $d - \delta_3 \leq e', d' - \delta_1 \leq c'$, we get:

$$\begin{aligned} P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_1 - \delta_2 - \delta_3 &\leq e' \\ P_{A,B|X,Y}(0, 0|A_0, B_0) - \delta_1 - \delta_2 - \delta_3 &\leq c' \end{aligned} \quad (82)$$

Thus, combining Eq. (77) and the definition of I_α^{Hardy} , these probabilities c, c', d, d', e, e' are larger than or equal to $\frac{1}{\alpha}I_\alpha^{Hardy}$. Using the normalization constraints for different measurement settings, one can get corresponding upper bounds for these probabilities. For example, from $c + c' + \delta_1 + s = 1$, one can get the upper bounds of c, c' :

$$\begin{aligned} c &\leq 1 - c' - \delta_1 \leq 1 - P_{A,B|X,Y}(0,0|A_0, B_0) + \delta_2 + \delta_3 \\ c' &\leq 1 - c - \delta_1 \leq 1 - P_{A,B|X,Y}(0,0|A_0, B_0) \end{aligned} \quad (83)$$

Thus, the entries c, c', d, d', e, e' are smaller than or equal to $1 - \frac{1}{\alpha}I_\alpha^{Hardy}$. For entry δ_i , it is simply bounded by $\delta_i \leq \delta_1 + \delta_2 + \delta_3$. From Fig. 7 (c), one can obtain the following inequalities:

$$\begin{aligned} P_{A,B|X,Y}(0,0|A_0, B_0) - \delta_1 - \delta_2 &\leq d \\ P_{A,B|X,Y}(0,0|A_0, B_0) - \delta_2 - \delta_3 &\leq d' \end{aligned} \quad (84)$$

Together with $d + d' + \delta_2 \leq 1$, we get:

$$P_{A,B|X,Y}(0,0|A_0, B_0) \leq \frac{1}{2}(1 + \delta_1 + \delta_2 + \delta_3). \quad (85)$$

Thus, combining Eq. (77) and the definition of I_α^{Hardy} , we get:

$$\delta_1 + \delta_2 + \delta_3 \leq \alpha - 2I_\alpha^{Hardy} \quad (86)$$

and

$$P_{A,B|X,Y}(0,0|A_0, B_0) \leq \frac{1 + \alpha}{2} - I_\alpha^{Hardy}. \quad (87)$$

Together with the normalization constraint, we get $P_{A,B|X,Y}(1,1|A_0, B_0) \geq \frac{1-\alpha}{2} + I_\alpha^{Hardy}$. For the remaining entries x, x', s, s', t , their upper bounds can directly found by using no-signaling or normalization conditions as shown in Fig. 7 (d). In general, we obtain the upper bound

$$P_{A,B|X,Y}(a,b|A_x, B_y) \leq 1 - \frac{1}{\alpha}I_\alpha^{Hardy}, \quad (88)$$

for $w \in (\frac{1}{3}, 1]$.

Case 2. $\alpha \in (1, +\infty)$. In this case, we observe that $\max(0, \frac{1-\alpha}{2}) = 0$ and derive the bounds

$$\begin{aligned} I_\alpha^{Hardy} &\leq P_{A,B|X,Y}(a,b|A_x, B_y) \leq 1 - I_\alpha^{Hardy} & \forall a \oplus b = x \cdot y \\ P_{A,B|X,Y}(a,b|A_x, B_y) &\leq 1 - 2I_\alpha^{Hardy} & \forall a \oplus b \neq x \cdot y \end{aligned} \quad (89)$$

The proof in this case is similar to the proof of Case 1, we omit the details here. For any given $\alpha \in (1, +\infty)$, we obtain the upper bound

$$P_{A,B|X,Y}(a,b|A_x, B_y) \leq 1 - I_\alpha^{Hardy} \quad (90)$$

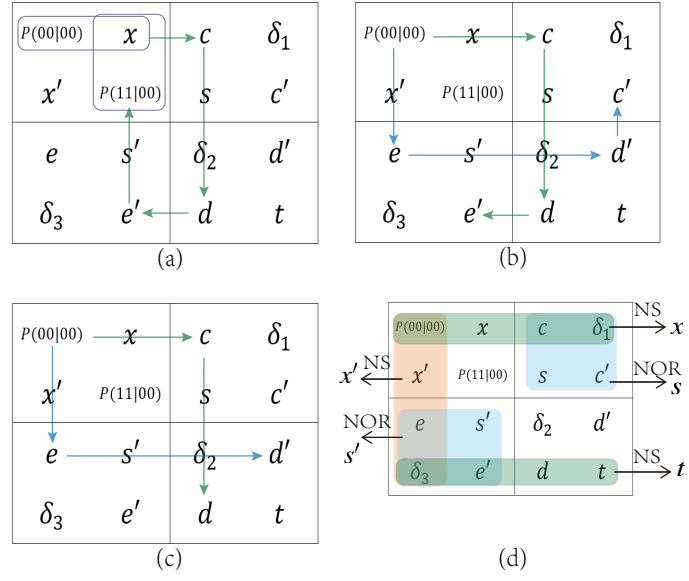


Figure 7: (a), (b) and (c): Chains of inequalities under the no-signaling conditions. (d): No-signaling and normalization constraints used for calculating the upper bounds of x, x', s, s', t . (NS: no-signaling constraint; NOR: normalization constraint.)

□