White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of York.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/191751/

Version: Accepted Version

Article:
Wooltorton, Lewis, Brown, Peter and Colbeck, Roger (2022) Tight Analytic Bound on the Trade-Off between Device-Independent Randomness and Nonlocality. Physical Review Letters. 150403. ISSN: 1079-7114

https://doi.org/10.1103/PhysRevLett.129.150403

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

UNIVERSITY OF LEEDS
University of Sheffield
UNIVERSITY of York

Tight analytic bound on the trade-off between device-independent randomness and nonlocality

Lewis Wooltorton,[1,2,*] Peter Brown,[3,†] and Roger Colbeck[1,‡]

[1] *Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom*
[2] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical & Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom*
[3] *Télécom Paris, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France*

(Dated: 5th October, 2022)

Two parties sharing entangled quantum systems can generate correlations that cannot be produced using only shared classical resources. These *nonlocal* correlations are a fundamental feature of quantum theory but also have practical applications. For instance, they can be used for *device-independent* (DI) random number generation, whose security is certified independently of the operations performed inside the devices. The amount of certifiable randomness that can be generated from some given non-local correlations is a key quantity of interest. Here we derive tight analytic bounds on the maximum certifiable randomness as a function of the nonlocality as expressed using the Clauser-Horne-Shimony-Holt (CHSH) value. We show that for every CHSH value greater than the local value (2) and up to $3\sqrt{3}/2 \approx 2.598$ there exist quantum correlations with that CHSH value that certify a maximal two bits of global randomness. Beyond this CHSH value the maximum certifiable randomness drops. We give a second family of Bell inequalities for CHSH values above $3\sqrt{3}/2$, and show that they certify the maximum possible randomness for the given CHSH value. Our work hence provides an achievable upper bound on the amount of randomness that can be certified for any CHSH value. We illustrate the robustness of our results, and how they could be used to improve randomness generation rates in practice, using a Werner state noise model.

I. INTRODUCTION

Nonlocality is the phenomenon where measurements of certain quantum systems, by isolated observers, generate correlations inaccessible to any local systems that behave classically [1, 2]. Nonlocal correlations can be used to make statements about the underlying quantum system without characterizing the devices used [3–7], and constitute a resource for information processing [8]. In particular, they give rise to the possibility of DI information processing which allows, for instance, the intrinsic randomness of nonlocal correlations to be exploited for randomness expansion [9–13], amplification [14], and key distribution protocols [15–20].

Given some experimental conditions in a particular input-output scenario, what is the optimal way to generate randomness device-independently? Since the values of extremal Bell inequalities quantify the distance of the observed correlations from the local boundary, one might expect these to be optimal for randomness. However, the relationship between nonlocality and maximum randomness is nontrivial [21], and it has been shown that non-extremal Bell inequalities can certify more randomness in some cases [22].

A substantial literature has developed investigating the maximum achievable randomness in different DI scenarios. In particular, the existence of Bell tests that can certify maximum global randomness was shown in [23] by adding extra measurements. Constructions achieving maximal randomness in the bipartite scenario for non-projective measurements were given in [24] and for greater than two projective measurements per party in [25–28]. In [22] a construction that tends towards the maximum 2 random bits is presented, based on the violation of tilted-CHSH inequalities [22, 29]. This provides a key example where non-extremal Bell inequalities certify more randomness (maximum violation of the CHSH inequality, the only extremal Bell inequality in the 2-input, 2-output scenario up to symmetry, can certify $5/2 - \log_2(1+\sqrt{2})/\sqrt{2} \approx 1.601$ bits of global randomness by comparison — see, e.g., [30]). Based on [22] one might expect that achieving 2 bits of randomness requires the CHSH violation (or entanglement) of the strategy to tend to 0. If this were the case, there would be a problem with the robustness of the construction, and the result suggests a trade-off between certifiable randomness and distance from the local set. Ref. [22] left open whether two bits of randomness is actually attainable using a single statistic in the 2-input 2-output scenario, and how non-local a strategy achieving this can be.

Our work gives conclusive answers to these questions. We consider the maximum amount of DI randomness that can be certified from the set of quantum correlations achieving a particular CHSH value. In other words, we investigate how much randomness is achievable when the generating system is required to exhibit a particular amount of nonlocality. To do so, we introduce two fami-

* lewis.wooltorton@york.ac.uk
† peter.brown@telecom-paris.fr
‡ roger.colbeck@york.ac.uk

lies of Bell expressions that self-test families of two qubit strategies. Our first family (see Proposition 1) certifies exactly 2 random bits for all CHSH values in the interval $(2, 3\sqrt{3}/2]$, showing 2 random bits are achievable without tending towards the local set [22], requiring extra measurements [25, 27, 28] or constraining the full distribution [31]. Our second family (see Proposition 2) covers the range of values $[3\sqrt{3}/2, 2\sqrt{2}]$, coinciding with the CHSH inequality for $2\sqrt{2}$, and the certifiable randomness achieved is a smooth, monotonically decreasing function of the value. We show in Proposition 3 that this is the true maximum randomness achievable for this range of CHSH values, illustrating how one only needs to sacrifice randomness when approaching the maximum quantum value of CHSH. Finally, we analyse the robustness of our construction under a Werner state noise model [32], and compare it to that of the tilted CHSH inequalities. We find both constructions to be robust, and at any given noise level there exists an optimal statistic for practical DI randomness generation that can outperform CHSH.

II. DI SCENARIO

We consider the bipartite 2-input 2-output Bell scenario. Let two isolated devices each receive an input $x, y \in \{0, 1\}$, from which they produce an output $a, b \in \{0, 1\}$, stored in the classical registers A and B. The devices are characterised by the joint conditional probability distribution $\mathrm{p}(ab|xy)$, which, due to the isolation of the devices, must be no-signalling.

We refer to a quantum strategy when the devices share a bipartite density operator $\rho_{Q_A Q_B}$ on the Hilbert space $\mathcal{H}_{Q_A} \otimes \mathcal{H}_{Q_B}$, and measure observables $A_x = M_{0|x} - M_{1|x}, B_y = N_{0|y} - N_{1|y}$, where $\{M_{a|x}\}_a, \{N_{b|y}\}_b$ are projective measurements on the associated Hilbert space (projective measurements can be assumed without loss of generality according to Naimark's dilation theorem [33]). We also include the possibility of an adversary Eve, who wishes to guess the outputs. In the DI scenario, Eve may have supplied the devices used by the user (Alice) and may hold a purifying system E with associated Hilbert space $\mathcal{H}_E$ such that the post-measurement system AB and E are correlated. We describe this using a tripartite density operator, $\rho_{Q_A Q_B E}$ such that $\rho_{Q_A Q_B} = \mathrm{Tr}_E[\rho_{Q_A Q_B E}]$. Following measurement with inputs $X = x$ and $Y = y$, we obtain the classical-quantum state $\rho_{ABE} = \sum_{ab} |ab\rangle\langle ab|_{AB} \otimes \rho_E^{(a,b,x,y)}$, where $\rho_E^{(a,b,x,y)} = \mathrm{Tr}_{Q_A Q_B}[\rho_{Q_A Q_B E}(M_{a|x} \otimes N_{b|y} \otimes \mathbb{I}_E)]$ is proportional to Eve's state conditioned on the joint measurement outcomes, and the distribution is recovered via $\mathrm{p}(ab|xy) = \mathrm{Tr}[\rho_E^{(a,b,x,y)}]$.

III. NONLOCALITY AND SELF-TESTS

To quantify the distance of an observed distribution $\mathrm{p}(ab|xy)$ from the local boundary in this scenario, we consider the CHSH expression $I_{\mathrm{CHSH}} = \langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle$, where $\langle A_x B_y\rangle = \sum_{ab}(-1)^{a+b}\,\mathrm{p}(ab|xy) = \langle\Psi|A_x \otimes B_y \otimes \mathbb{I}|\Psi\rangle$ when $\mathrm{p}(ab|xy)$ admits a quantum representation with purified state and observables $\left(|\Psi\rangle_{Q_A Q_B E}, A_x, B_y\right)$. The local bound is given by $I_{\mathrm{CHSH}} \leq 2$, and the maximum quantum value is $2\sqrt{2}$ [34]. Any distribution that violates the local bound is said to be nonlocal.

It is known that the CHSH inequality self-tests the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ and the measurements that achieve its maximum quantum violation [7, 29, 35, 36] in the sense that there is only one state and set of measurements that can achieve $I_{\mathrm{CHSH}} = 2\sqrt{2}$ up to local isometries. One can also define a robust self test, in which close to maximum violation certifies a state and measurements close to the optimal ones up to local isometries.

IV. ENTROPY BOUNDS

The quantity of interest for calculating the DI global randomness is the conditional von Neumann entropy when the devices receive inputs $X = Y = 0$, $H(AB|X = 0, Y = 0, E)$, evaluated for the post-measurement state ρ_{ABE}. This is the relevant quantity for spot-checking DI random number generation [30]. For DI randomness expansion we require lower bounds on this quantity that hold for all states and measurements compatible with the observed distribution P_{obs}, or some linear functions f_i of P_{obs}, e.g., the CHSH value. This gives the asymptotic rate of randomness generation r, in bits per round:

$$r = \inf_{\substack{\rho_{Q_A Q_B E},\\ \{M_{a|x}\}_a, \{N_{b|y}\}_b \\ \text{compatible with } f_i(P_{\mathrm{obs}})}} H(AB|X = 0, Y = 0, E)_{\rho_{ABE}}. \quad (1)$$

The asymptotic rate can also be used as a basis for rates with finite statistics using tools such as the entropy accumulation theorem [37–39].

In the noiseless scenario, we prove a self-testing statement that certifies a state and measurements that generate two bits of randomness. In this case, $f(P_{\mathrm{obs}})$ is a self-testing Bell expression, and there is only one state and set of measurements that can achieve the maximal quantum value (up to symmetries), from which the conditional entropy can be evaluated. For the noisy case, we use the recently developed numerical technique from [31] to compute lower bounds on Eq. (1) using semidefinite programming.

V. MAIN RESULTS

Our first main result is the family of Bell expressions that works for CHSH values in the range $(2, 3\sqrt{3}/2]$.

Proposition 1. Let $0 < \delta \leq \pi/6$, and define the family of Bell expressions parameterized by δ, labelled I_δ:

$$\langle A_0 B_0\rangle + \frac{1}{\sin\delta}\left(\langle A_0 B_1\rangle + \langle A_1 B_0\rangle\right) - \frac{1}{\cos 2\delta}\langle A_1 B_1\rangle. \quad (2)$$

Then we have the following:

(i) The local bound is given by $I_\delta^{\mathrm{L}} = -1 + \frac{2}{\sin\delta} + \frac{1}{\cos 2\delta}$.

(ii) The quantum bound is given by $I_\delta^{\mathrm{Q}} = \frac{2\cos^3\delta}{\cos 2\delta \sin\delta}$.

(iii) Up to local isometries there is a unique strategy that achieves $I_\delta = I_\delta^{\mathrm{Q}}$:

$$\begin{aligned} \rho_{Q_A Q_B} &= |\psi\rangle\langle\psi| \text{ where } |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ A_0 &= \sigma_Z, \quad B_0 = \sigma_X, \\ A_1 &= -\sin\delta\,\sigma_Z + \cos\delta\,\sigma_X, \\ B_1 &= \cos\delta\,\sigma_Z - \sin\delta\,\sigma_X. \end{aligned} \quad (3)$$

By the previous discussion of the noiseless case, Proposition 1 shows that there exists a family of two-qubit strategies that can achieve exactly two bits of global DI randomness in the bipartite, 2-input 2-output case; this follows from self-testing measurements A_0, B_0 together with the maximally entangled state $|\psi\rangle$. We now explore some implications of this. The strategy in Eq. (3) has a CHSH value $I_{\mathrm{CHSH}} = 2\cos\delta\,(\sin\delta + 1)$ and by sweeping $0 < \delta \leq \pi/6$ the interval of values $(2, 3\sqrt{3}/2]$ is achieved. Hence for every CHSH value in this interval, there exists a two-qubit strategy achieving this value, that can certify exactly 2 bits of randomness. In fact $3\sqrt{3}/2 \approx 2.598$ is the largest CHSH value for which exactly two bits of randomness can be achieved, corresponding to the $\delta = \pi/6$ strategy in Eq. (3) (see the Supplemental Material [40]). This strategy can be derived by fixing $\mathrm{p}(ab|00) = 1/4$, and optimising the the remaining measurement angles for the maximum CHSH value. This improves upon the results in [22] (cf. the introduction): rather than needing low CHSH violation to get close to maximal randomness, maximum randomness is achieved well into the nonlocal region.

Next we derive the maximum randomness for strategies achieving a CHSH value in the interval $[3\sqrt{3}/2, 2\sqrt{2}]$. Up to local isometries, the only strategy that can achieve $I_{\mathrm{CHSH}} = 2\sqrt{2}$ is given by the maximally entangled state with measurements $A_0 = \sigma_Z$, $B_0 = (\sigma_Z + \sigma_X)/\sqrt{2}$, $A_1 = \sigma_X$, and $B_1 = (\sigma_Z - \sigma_X)/\sqrt{2}$, since the CHSH inequality self-tests this state and measurements [29]. This strategy gives roughly 1.601 bits of randomness. There must therefore be a transition between $I_{\mathrm{CHSH}} = 3\sqrt{3}/2$ and $I_{\mathrm{CHSH}} = 2\sqrt{2}$, where in order to achieve a larger CHSH value, randomness must be sacrificed. This transition is given by the following proposition.

Proposition 2. Let $0 \leq \gamma \leq \pi/12$, and define the family of Bell expressions parameterized by γ, labelled J_γ:

$$\langle A_0 B_0\rangle + c(\gamma)\big(\langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle\big), \quad (4)$$

where $c(\gamma) = 4\cos^2\left(\gamma + \frac{\pi}{6}\right) - 1$. Then we have the following:

(i) The local bound is given by $J_\gamma^{\mathrm{L}} = 12\cos^2\left(\gamma + \frac{\pi}{6}\right) - 4$.

(ii) The quantum bound is given by $J_\gamma^{\mathrm{Q}} = 8\cos^3\left(\gamma + \frac{\pi}{6}\right)$.

(iii) Up to local isometries there is a unique strategy that achieves $J_\gamma = J_\gamma^{\mathrm{Q}}$:

$$\begin{aligned} \rho_{Q_A Q_B} &= |\psi\rangle\langle\psi| \text{ where } |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ A_0 &= \sigma_Z, \quad B_0 = \sin 3\gamma\,\sigma_Z + \cos 3\gamma\,\sigma_X, \\ A_1 &= \cos\left(\frac{2\pi}{3} - 2\gamma\right)\sigma_Z + \sin\left(\frac{2\pi}{3} - 2\gamma\right)\sigma_X, \\ B_1 &= \cos\left(\frac{\pi}{6} + \gamma\right)\sigma_Z - \sin\left(\frac{\pi}{6} + \gamma\right)\sigma_X. \end{aligned} \quad (5)$$

When $\gamma = 0$, this corresponds to the expression in Eq. (2) for $\delta = \pi/6$, and when $\gamma = \pi/12$ we recover the CHSH expression. The CHSH value for this family is given by $I_{\mathrm{CHSH}} = \sin 3\gamma + 3\cos(\gamma + \pi/6)$, and monotonically decreases in the interval $[3\sqrt{3}/2, 2\sqrt{2}]$. The randomness certified by these self-tests is maximum for each CHSH value, summarized in our final proposition.

Proposition 3. *The maximum randomness for strategies achieving a CHSH value in the range $s \in (2, 3\sqrt{3}/2]$ is 2 bits, and is generated by the family of strategies in Eq. (3). For the range $s \in [3\sqrt{3}/2, 2\sqrt{2}]$, the maximum is given by*

$$1 + H_{\mathrm{bin}}\left[\frac{1}{2} + \frac{s}{2} - \frac{3}{\sqrt{2}}\cos\left(\frac{1}{3}\arccos\left[-\frac{s}{2\sqrt{2}}\right]\right)\right], \quad (6)$$

where $H_{\mathrm{bin}}[\cdot]$ is the binary entropy, and is generated by the family of strategies in Eq. (5).

Propositions 1–3 are proven in the Appendices. In Fig. 1, we illustrate our results and compare them to a reliable lower bound on the minimum amount of randomness guaranteed by the same CHSH value [31]. These two curves represent tight upper and lower bounds on the amount of DI randomness that can be certified by strategies achieving a particular CHSH value.

In Fig. 2 we explore the robustness of our constructions. We consider a Werner state noise model [32], i.e., $\rho_{Q_A Q_B} = (1-p)|\psi\rangle\langle\psi| + p\,\mathbb{I}_{AB}/4$, where $p \in [0, 1]$ is the weight of the uniform noise. For simplicity, we assume noiseless measurements. We use this state and measurements to simulate statistics from which reliable DI lower bounds can be generated using the techniques of [31]. At

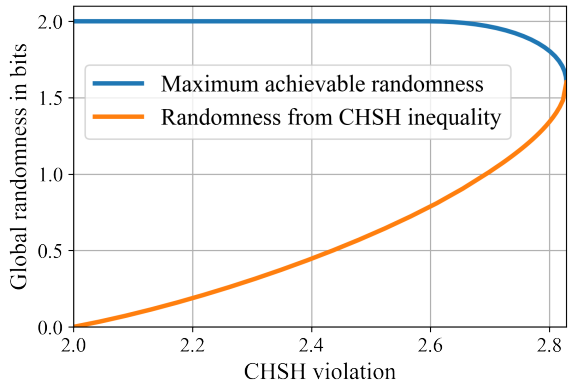

FIG. 1. The relationship between maximum randomness and CHSH value in the noiseless bipartite 2-input 2-output scenario. Plotted is the maximum achievable randomness for all quantum strategies that achieve a particular CHSH value (blue), and a reliable lower bound certified by the same CHSH value (orange) using analysis from [31]. For the interval of values $(2, 3\sqrt{3}/2]$ two bits of randomness are certified by the family of strategies in Eq. (3), and for the region $[3\sqrt{3}/2, 2\sqrt{2}]$ the maximum is certified by the family of strategies in Eq. (5). Note that it is not the case that a CHSH value guarantees rates given by the blue curve; the blue curve gives a tight upper bound on achievable rates in a noiseless scenario.

each noise level, the randomness is optimized over the choice of self-test from Eq. (4). This is compared to the tilted CHSH expressions [22, 29], where the tilting parameter is similarly optimized.

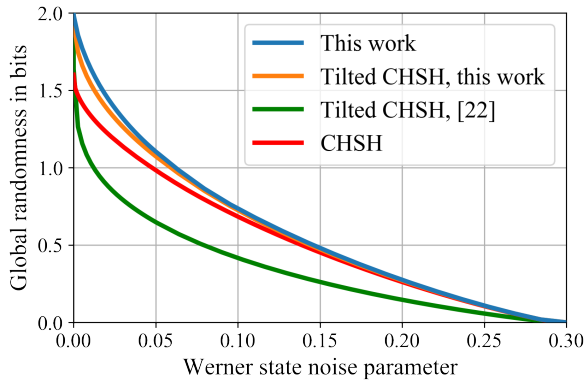

FIG. 2. Noise comparison for Bell expressions that certify maximum randomness in the bipartite 2-input 2-output scenario. Our constructions (blue) are compared to the tilted Bell inequalities from [22], using both the numerical technique from [31] (orange), and the min-entropy [22] (green). All these curves have been generated by optimizing the Bell expression (within the relevant families) at each value of the noise, and the new analysis shows improved rates of randomness generation over the CHSH statistic (red).

VI. DISCUSSION

Our tight upper bound on the achievable DI randomness conditioned on the CHSH value shows that only when one approaches Tsirelson's bound does one need to sacrifice randomness for nonlocality. This comes from the fact that the optimal measurements needed to achieve $I_{\text{CHSH}} = 2\sqrt{2}$ have correlated outcomes, whereas correlations that satisfy $I_{\text{CHSH}} \leq 3\sqrt{3}/2$ can have uniform measurement outcomes. When there is zero noise, such a distribution can be used to generate 2 bits of randomness (using the $\gamma = 0$ strategy in Eq. (5)). As noise is added, using the family of Bell inequalities that self-test a distribution with a CHSH value greater than $3\sqrt{3}/2$ (obtained by increasing γ), we can continue to certify more randomness than would be possible using CHSH inequality at that noise level. Taking the optimal value of γ at each level of noise we find that the Bell expressions tend to the CHSH statistic as the noise approaches the boundary where no randomness can be certified. In this sense, CHSH is the most robust statistic, which is natural since it defines a facet of the local polytope and so becomes the only Bell inequality that can be violated with high enough noise. We also remark that the robustness of the tilted CHSH inequalities presented here is higher than that of [22] (cf. the orange vs green curves in Fig. 2). This is a result of using improved numerical techniques to bound the conditional von Neumann entropy directly rather than the min-entropy that is used in [22].

Based on an experimental estimate of the noise, a Bell inequality from one of our families could be chosen that maximises the certifiable randomness (along the lines of Fig. 2). Knowledge of the full distribution could also boost the noise performance or be used to search for improved protocols in the presence of noise. However, the use of more parameters would lead to a penalty when finite size effects are accounted for. We leave the question of how our construction performs in other noise models, such as detector efficiency, to future work, and pose an open question as to if our construction is truly optimal in the noisy regime.

One other potential application of our constructions is to blind randomness expansion [41–43], where Alice tries to certify local randomness from one device without trusting the other. Since their outputs are uncorrelated following a self-test from Proposition 1, such a statistic could be used to generate the optimal 1 bit of local randomness in the blind setting.

Finally, it would be interesting to further investigate analogous results in multi-partite scenarios [44, 45] or those with more inputs or outputs [46]. Indeed, [45] showed maximal randomness for the outputs of two parties based on a three party Mermin-Ardehali-Belinskii-Klyshko inequality [47], and with advancements in computational efficiency from new numerical techniques [31, 48] alongside self-testing results [49, 50], multi-partite DI-RG has many avenues to explore.

ACKNOWLEDGMENTS

This work was supported by EPSRC via the Quantum Communications Hub (Grant No. EP/T001011/1) and Grant No. EP/SO23607/1.

[1] J. S. Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, 1987).

[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," Reviews of Modern Physics **86**, 419–478 (2014).

[3] D. Mayers and A. Yao, "Self testing quantum apparatus," (2004), arXiv:quant-ph/0307205 [quant-ph].

[4] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet," Journal of Physics A: Mathematical and Theoretical **45**, 455304 (2012).

[5] T. H. Yang and M. Navascués, "Robust self-testing of unknown quantum systems into any entangled two-qubit states," Physical Review A **87**, 050102 (2013).

[6] J. Kaniewski, "Self-testing of binary observables based on commutation," Physical Review A **95**, 062323 (2017).

[7] I. Šupić and J. Bowles, "Self-testing of quantum systems: a review," Quantum **4**, 337 (2020).

[8] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, "Nonlocal correlations as an information-theoretic resource," Physical Review A **71**, 022101 (2005).

[9] R. Colbeck, *Quantum and Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis, University of Cambridge (2007), also available as arXiv:0911.3814.

[10] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[11] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," Journal of Physics A **44**, 095305 (2011).

[12] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, NY, USA, 2014) pp. 417–426.

[13] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol," SIAM Journal of Computing **46**, 1304–1335 (2017).

[14] R. Colbeck and R. Renner, "Free randomness can be amplified," Nature Physics **8**, 450–454 (2012).

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters **67**, 661–663 (1991).

[16] J. Barrett, L. Hardy, and A. Kent, "No signalling and quantum key distribution," Physical Review Letters **95**, 010503 (2005).

[17] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Physical Review Letters **98**, 230501 (2007).

[18] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," New Journal of Physics **11**, 045021 (2009).

[19] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," Physical Review Letters **113**, 140501 (2014).

[20] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," Nature communications **9**, 459 (2018).

[21] G. de la Torre, M. J. Hoban, C. Dhara, G. Prettico, and A. Acín, "Maximally nonlocal theories cannot be maximally random," Physical Review Letters **114**, 160502 (2015).

[22] A. Acín, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," Physical Review Letters **108**, 100402 (2012).

[23] C. Dhara, G. Prettico, and A. Acín, "Maximal quantum randomness in Bell tests," Physical Review A **88**, 052116 (2013).

[24] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, "Optimal randomness certification from one entangled bit," Physical Review A **93**, 040102 (2016).

[25] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, "Quantum randomness extraction for various levels of characterization of the devices," Journal of Physics A: Mathematical and Theoretical **47**, 424028 (2014).

[26] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, "Device-independent certification of two bits of randomness from one entangled bit and gisin's elegant bell inequality," Phys. Rev. A **97**, 012314 (2018).

[27] P. J. Brown, S. Ragy, and R. Colbeck, "A framework for quantum-secure device-independent randomness expansion," IEEE Transactions on Information Theory **66**, 2964–2987 (2020).

[28] E. Woodhead, J. Kaniewski, B. Bourdoncle, A. Salavrakos, J. Bowles, A. Acín, and R. Augusiak, "Maximal randomness from partially entangled states," Physical Review Research **2**, 042028 (2020).

[29] C. Bamps and S. Pironio, "Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing," Physical Review A **91**, 052111 (2015).

[30] R. Bhavsar, S. Ragy, and R. Colbeck, "Improved device-independent randomness expansion rates from tight bounds on the two sided randomness using CHSH tests," (2021), arXiv:2103.07504 [quant-ph].

[31] P. Brown, H. Fawzi, and O. Fawzi, "Device-independent lower bounds on the conditional von Neumann entropy," (2021), arXiv:2106.13692 [quant-ph].

[32] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Physical Review A **40**, 4277–4281 (1989).

[33] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, 2003).

[34] B. Cirel'son, "Quantum generalizations of Bell's inequality," Letters in Mathematical Physics **4**, 93–100 (1980).

[35] S. Popescu and D. Rohrlich, "Which states violate Bell's inequality maximally?" Physics Letters A **169**, 411–414 (1992).

[36] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, "Device-independent state estimation based on Bell's inequalities," Physical Review A **80**, 062327 (2009).

[37] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," e-print arXiv:1607.01796 (2016).

[38] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order term," IEEE Transactions on Information Theory **65**, 7596–7612 (2019).

[39] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, "Device-independent randomness expansion against quantum side information," Nature Physics **17**, 448–451 (2021).

[40] L. Wooltorton, P. Brown, and R. Colbeck, Supplemental Material containing proofs of the propositions and including additional references [51–54].

[41] C. A. Miller and Y. Shi, "Randomness in nonlocal games between mistrustful players," Quantum information & computation **17**, 595–610 (2017).

[42] H. Fu and C. A. Miller, "Local randomness: Examples and application," Physical Review A **97**, 032324 (2018).

[43] T. Metger, O. Fawzi, D. Sutter, and R. Renner, "Generalised entropy accumulation," (2022), arXiv:2203.04989 [quant-ph].

[44] E. Woodhead, B. Bourdoncle, and A. Acín, "Randomness versus nonlocality in the Mermin-Bell experiment with three parties," Quantum **2**, 82 (2018).

[45] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, "Entropy bounds for multiparty device-independent cryptography," PRX Quantum **2**, 010308 (2021).

[46] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, "Self-testing quantum systems of arbitrary local dimension with minimal number of measurements," npj Quantum Information **7**, 151 (2021).

[47] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, "Bell-type inequalities to detect true n-body nonseparability," Physical Review Letters **88**, 170405 (2002).

[48] M. Masini, S. Pironio, and E. Woodhead, "Simple and practical DIQKD security analysis via BB84-type uncertainty relations and pauli correlation constraints," (2021), arXiv:2107.08894 [quant-ph].

[49] M. Mckague, "Self-testing graph states," in *Revised Selected Papers of the 6th Conference on Theory of Quantum Computation, Communication, and Cryptography - Volume 6745*, TQC 2011 (Springer-Verlag, Berlin, Heidelberg, 2011) p. 104–120.

[50] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, "Robust self-testing of the three-qubit W state," Physical Review A **90**, 042339 (2014).

[51] C. Jordan, "Essai sur la géométrie à n dimensions," Bulletin de la S. M. F. **3**, 103–174 (1875).

[52] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, "Geometry of the set of quantum correlations," Physical Review A **97**, 022104 (2018).

[53] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, "Certifying the building blocks of quantum computers from Bell's theorem," Physical Review Letters **121**, 180505 (2018).

[54] X. Valcarce, J. Zivy, N. Sangouard, and P. Sekatski, "Self-testing two-qubit maximally entangled states from generalized Clauser-Horne-Shimony-Holt tests," Physical Review Research **4**, 013049 (2022).

Appendix A: Proof of Propositions 1 and 2

The goal of this section is to prove Propositions 1 and 2, which are restated below:

Proposition 1 (I_δ-family of self-tests). *Let $0 < \delta \leq \pi/6$, and define the family of Bell expressions parameterized by δ,*

$$I_\delta = \langle A_0 B_0 \rangle + \frac{1}{\sin\delta}\Big(\langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle\Big) - \frac{1}{\cos 2\delta}\langle A_1 B_1 \rangle. \tag{A1}$$

Then we have the following:

(i) The local bound is given by $I_\delta^{\mathrm{L}} = -1 + \frac{2}{\sin\delta} + \frac{1}{\cos 2\delta}$.

(ii) The quantum bound is given by $I_\delta^{\mathrm{Q}} = \frac{2\cos^3\delta}{\cos 2\delta \sin\delta}$.

(iii) Up to local isometries there is a unique strategy that achieves $I_\delta = I_\delta^{\mathrm{Q}}$:

$$\begin{aligned} \rho_{Q_A Q_B} = |\psi\rangle\langle\psi| \text{ where } |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ A_0 = \sigma_Z, \quad B_0 = \sigma_X, \\ A_1 = -\sin\delta\,\sigma_Z + \cos\delta\,\sigma_X, \\ B_1 = \cos\delta\,\sigma_Z - \sin\delta\,\sigma_X. \end{aligned} \tag{A2}$$

Proposition 2 (J_γ-family of self-tests). *Let $0 \leq \gamma \leq \pi/12$, and define the family of Bell expressions parameterized by γ,*

$$J_\gamma = \langle A_0 B_0 \rangle + \left(4\cos^2\left(\gamma + \frac{\pi}{6}\right) - 1\right)\Big(\langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle\Big). \tag{A3}$$

Then we have the following:

(i) The local bound is given by $J_\gamma^{\mathrm{L}} = 12\cos^2\left(\gamma + \frac{\pi}{6}\right) - 4$.

(ii) The quantum bound is given by $J_\gamma^{\mathrm{Q}} = 8\cos^3\left(\gamma + \frac{\pi}{6}\right)$.

(iii) Up to local isometries there is a unique strategy that achieves $J_\gamma = J_\gamma^{\mathrm{Q}}$:

$$\begin{aligned}
\rho_{Q_A Q_B} = |\psi\rangle\langle\psi| \ \textit{where}\ |\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
A_0 = \sigma_Z, \quad B_0 &= \sin 3\gamma\, \sigma_Z + \cos 3\gamma\, \sigma_X,\\
A_1 = \cos\left(\frac{2\pi}{3} - 2\gamma\right)\sigma_Z &+ \sin\left(\frac{2\pi}{3} - 2\gamma\right)\sigma_X,\\
B_1 = \cos\left(\frac{\pi}{6} + \gamma\right)\sigma_Z &- \sin\left(\frac{\pi}{6} + \gamma\right)\sigma_X.
\end{aligned} \tag{A4}$$

We follow the same method for both cases. For part (i), the local bound can be found by setting the observables A_x, B_y to ± 1, corresponding to an extremal or deterministic strategy. Since these are the vertices of the local polytope, one such combination will be the optimal local strategy.

For the quantum bound in part (ii), a sum-of-squares (SOS) decomposition is found for the Bell expression offset by its claimed maximum quantum value, exploiting the symmetry of the Bell expression under relabelling of A and B [29]. The existence of an SOS decomposition proves the maximum quantum value claimed, and is detailed in Appendices A 1 and A 2.

For the self-test in part (iii) we use the resulting SOS decomposition in combination with Jordan's lemma [51]. This simplifies the analysis to qubits, and we derive a system of non-linear equations satisfied by any state and measurements that achieve the maximum quantum value. The resulting system is then analytically solved, and we show the only state and measurements for which these equations are satisfied is given by the target strategy (Eqs. (A2) and (A4)) up to local unitaries. This process is detailed in Appendices A 3 to A 5, and completes the proof of Propositions 1 and 2. We remark that our self-tests define hyperplanes tangential to the corresponding strategy on the boundary of the quantum set [52].

For completeness, in Appendix A 6, we show from Jordan's lemma that the private randomness of any strategy that saturates the quantum bounds in Propositions 1 and 2 is equal to that of the target strategy.

1. Self-testing and sum-of-squares decompositions

We consider only the exact self-testing statement in this work, and leave proof of the robust statement for future work. We begin by defining self-testing.

Definition 1 (Self-test)**.** Let the observables A_x, B_y and pure state $|\psi\rangle_{Q_A Q_B}$ be the target two-qubit strategy, and let S be a Bell operator. The inequality $\langle S \rangle \leq I^{\mathrm{Q}}$ *self-tests* the target state and measurements if for all physical quantum strategies $(\tilde{\rho}_{\tilde{Q}_A \tilde{Q}_B}, \tilde{A}_x, \tilde{B}_y)$ that satisfy $\langle \tilde{S} \rangle = I^{\mathrm{Q}}$, there exists a local isometry $V : \mathcal{H}_{\tilde{Q}_A} \otimes \mathcal{H}_{\tilde{Q}_B} \otimes \mathcal{H}_E \to \mathcal{H}_{Q_A} \otimes \mathcal{H}_{Q_B} \otimes \mathcal{H}_{\mathrm{Junk}}$, $V = V_A \otimes V_B \otimes \mathbb{I}_E$, and ancillary state $|\xi\rangle_{\mathrm{Junk}}$ such that, for the purification $|\Psi\rangle_{\tilde{Q}_A \tilde{Q}_B E}$ of $\tilde{\rho}_{\tilde{Q}_A \tilde{Q}_B}$,

$$V\Big[(\tilde{A}_x \otimes \tilde{B}_y \otimes \mathbb{I}_E)|\Psi\rangle_{\tilde{Q}_A \tilde{Q}_B E}\Big] = (A_x \otimes B_y)|\psi\rangle_{Q_A Q_B} \otimes |\xi\rangle_{\mathrm{Junk}}. \tag{A5}$$

Throughout this appendix, we refer to the physical state and measurements we are trying to self-test as the "reference", denoted with a tilde. The strategies in Eqs. (A2) and (A4) are then the "target" state and measurements; which target strategy we refer to will be clear from the context.

For a Bell operator S that defines the quantum Bell inequality $\langle S\rangle \leq I^{\mathrm{Q}}$, the operator $\bar{S} := I^{\mathrm{Q}}\mathbb{I} - S$, satisfies $\langle\phi|\bar{S}|\phi\rangle \geq 0$ for all quantum states $|\phi\rangle$, i.e., $\bar{S} \succeq 0$. If there exists a set of operators P_i that are polynomials of A_x, B_y and satisfy

$$\bar{S} = \sum_i P_i^\dagger P_i, \tag{A6}$$

then we have found a sum-of-squares (SOS) decomposition of the operator $\bar{S}$: positivity of $\bar{S}$ follows directly from the fact that $K^\dagger K \succeq 0$ for any operator K.

SOS decompositions can be used to enforce algebraic constraints on any state and measurements that satisfy $\langle S\rangle = I^{\mathrm{Q}}$, since this implies

$$\langle\bar{S}\rangle = \sum_i \langle\psi|P_i^\dagger P_i|\psi\rangle = 0\,. \tag{A7}$$

This can only hold if $P_i|\psi\rangle = 0$ for all i. Relations of this form are used to prove the self-testing statement in Definition 1.

2. SOS decomposition for the inequalities in Propositions 1 and 2

Finding an SOS decomposition can be recast as a semidefinite program (SDP) [29]. We start by considering a vector $\boldsymbol{R} = [R_0, ..., R_k, ...]^{\mathrm{T}}$ whose components are linear combinations of A_0, A_1, B_0 and B_1. We consider the case where each polynomial P_i is linear, writing $P_i = \sum_k q_i^k R_k$ for some coefficients $\{q_i^k\}_k$. Then

$$\begin{aligned}\bar{S} &= \sum_i P_i^\dagger P_i \\ &= \sum_{kj} R_k^\dagger \left(\sum_i \left(q_i^k\right)^* q_i^j\right) R_j \\ &= \sum_{kj} R_k^\dagger M_{kj} R_j = \boldsymbol{R}^\dagger M \boldsymbol{R}\,,\end{aligned} \tag{A8}$$

where M is the Gram matrix of the set of vectors $\{\boldsymbol{q}^k\}$. Since M is a Gram matrix, it is positive semidefinite by construction. We can hence use semidefinite programming to find an $M \succeq 0$ that satisfies Eq. (A8), and then find the polynomials P_i via the matrix square root:

$$\bar{S} = \boldsymbol{R}^\dagger M \boldsymbol{R} = \left(\sqrt{M}\boldsymbol{R}\right)^\dagger \left(\sqrt{M}\boldsymbol{R}\right). \tag{A9}$$

Since each entry of the vector $\sqrt{M}\boldsymbol{R}$ takes the form $[\sqrt{M}\boldsymbol{R}]_i = \sum_k [\sqrt{M}]_{ik} R_k$, we find that $P_i = [\sqrt{M}\boldsymbol{R}]_i$ provides the set of polynomials that satisfies Eq. (A8).

For the Bell operator $\bar{S}_\delta = I_\delta^{\mathrm{Q}}\mathbb{I} - I_\delta$, where

$$I_\delta = A_0 B_0 + \frac{1}{\sin\delta}\left(A_0 B_1 + \ A_1 B_0\right) - \frac{1}{\cos 2\delta} A_1 B_1, \tag{A10}$$

the SOS decomposition is given by the following lemma.

Lemma 1 (I_δ-family SOS decomposition)**.** *Let* $\boldsymbol{R} = [R_0, R_1, R_2, R_3]^T$*, where*

$$R_0 = \frac{1}{\sqrt{2}}(B_1 - A_1), \tag{A11}$$

$$R_1 = \frac{1}{\sqrt{2}}(B_0 - A_0), \tag{A12}$$

$$R_2 = \frac{1}{\sqrt{2}}(B_1 + A_1), \tag{A13}$$

$$R_3 = \frac{1}{\sqrt{2}}(B_0 + A_0). \tag{A14}$$

For every $\delta \in (0, \pi/6]$, the Bell expressions $\bar{S}_\delta$ can be written as a SOS decomposition $\bar{S}_\delta = \boldsymbol{R}^\dagger M_\delta \boldsymbol{R}$ where

$$M_\delta = \begin{bmatrix} (\alpha - 1/2)\zeta & \beta & 0 & 0 \\ \beta & \alpha + 1/2 & 0 & 0 \\ 0 & 0 & (\alpha + 1/2)\zeta & -\beta \\ 0 & 0 & -\beta & \alpha - 1/2 \end{bmatrix}, \tag{A15}$$

for $\alpha = 1/(2\tan\delta)$, $\beta = 1/(2\sin\delta)$ and $\zeta = 1/\cos 2\delta$.

The maximum quantum value of I_δ is $I_\delta^{\mathrm{Q}} = \frac{2\cos^3\delta}{\cos 2\delta \sin\delta}$.

Proof. The claim $\bar{S}_\delta = \boldsymbol{R}^\dagger M_\delta \boldsymbol{R}$ can be verified by direct calculation. Since $\bar{S}_\delta \succeq 0$ we have $\langle I_\delta \rangle \leq I_\delta^{\mathrm{Q}}$, but the quantum strategy given in (A2) shows that this bound is achievable. □

Four polynomials $P_i(\delta)$ emerge from this decomposition:

$$P_0(\delta) = k_+\big[R_0 + (\sin\delta + \cos\delta)R_1\big], \tag{A16}$$
$$P_1(\delta) = (\sin\delta + \cos\delta)P_0(\delta), \tag{A17}$$
$$P_2(\delta) = k_-\big[R_2 + (\sin\delta - \cos\delta)R_3\big], \tag{A18}$$
$$P_3(\delta) = (\sin\delta - \cos\delta)P_2(\delta), \tag{A19}$$

where

$$k_\pm = \frac{1}{\sqrt{2\sin\delta\,(\cos\delta \pm \sin\delta)(2 \pm \sin(2\delta))}}. \tag{A20}$$

Similarly, the shifted Bell operator for the J_γ family is given by $\bar{S}'_\gamma = J_\gamma^{\mathrm{Q}}\mathbb{I} - J_\gamma$, where

$$J_\gamma = A_0B_0 + (4\cos^2(\gamma + \pi/6) - 1)\Big(A_0B_1 + A_1B_0 - A_1B_1\Big), \tag{A21}$$

and we have the following SOS decomposition:

Lemma 2 (J_γ-family SOS decomposition)**.** *Let $\boldsymbol{R}$ be as defined in Lemma 1. For every $\gamma \in [0, \pi/12]$, the Bell expressions $\bar{S}'_\gamma$ can be written as a SOS decomposition $\bar{S}'_\gamma = \boldsymbol{R}^\dagger M'_\gamma \boldsymbol{R}$ where*

$$M'_\gamma = \begin{bmatrix} 1/2 + \mu(4\mu^2 - 2\mu - 1) & 2\mu^2 - 1/2 & 0 & 0 \\ 2\mu^2 - 1/2 & \mu + 1/2 & 0 & 0 \\ 0 & 0 & -1/2 + \mu(4\mu^2 + 2\mu - 1) & 1/2 - 2\mu^2 \\ 0 & 0 & 1/2 - 2\mu^2 & \mu - 1/2 \end{bmatrix}, \tag{A22}$$

where $\mu = \cos(\gamma + \pi/6)$.

The maximum quantum value of J_γ is $J_\gamma^{\mathrm{Q}} = 8\mu^3$.

This can be proven in exactly the same way as Lemma 1 and gives rise to the polynomials

$$P'_0(\gamma) = c_+\big[(2\mu - 1)R_0 + R_1\big], \tag{A23}$$
$$P'_1(\gamma) = \frac{P'_0(\gamma)}{2\mu - 1}, \tag{A24}$$
$$P'_2(\gamma) = c_-\big[(2\mu + 1)R_2 - R_3\big], \tag{A25}$$
$$P'_3(\gamma) = -\frac{P'_2(\gamma)}{2\mu + 1}, \tag{A26}$$

where

$$c_\pm = \frac{4\mu^2 - 1}{2\sqrt{4\mu^3 \mp 2\mu^2 \pm 1}}. \tag{A27}$$

Lemmas 1 and 2 establish the quantum bounds in Propositions 1 and 2, and give us the tools needed to prove the self-testing claims, following a reduction to qubits detailed in the next section.

3. Applying Jordan's lemma

We can use the polynomials derived above for both families of inequalities to impose algebraic constraints on the state and measurements that satisfy $\langle \bar{S} \rangle = 0$. We employ Jordan's lemma [51], a unique simplification that can be made in the 2-input 2-output scenario [18, 30]. The lemma states that for two observables A_0 and A_1 on a Hilbert space $\mathcal{H}$, each with eigenvalues ± 1, there exists a basis transformation such that both are simultaneously block diagonal with block size no greater than two. The Hilbert space decomposes into this block diagonal structure, and, by dilating where necessary, we can take each block to be a qubit system. There then exists a block diagonal density operator that reproduces the statistics of the original system. This can be summarised as follows.

Lemma 3 (Jordan's lemma)**.** *Let A_0 and A_1 be two binary observables on a Hilbert space $\mathcal{H}_A$. Then there exists a basis in which A_0 and A_1 are block diagonal with block dimensions at most 2. Moreover, for every state and set of measurements on $\mathcal{H}_{\tilde{Q}_A} \otimes \mathcal{H}_{\tilde{Q}_B}$ that generates a post-measurement state ρ_{ABE}, there exists another state and set of measurements, given by a convex combinations of two-qubit systems, that generates the same post-measurement state.*

For self-testing literature that also utilises Jordan's lemma, see e.g. [36, 53, 54].

It is known that a full reduction to a convex combination of two-qubit strategies with measurements in the XZ-plane is sufficient for evaluating the global entropy [18, 30]. By employing Jordan's lemma to systems $\tilde{Q}_A$ and $\tilde{Q}_B$, the resulting parameterization of a single two-qubit strategy is given by 7 parameters: 3 for the state, which can be taken to be diagonal in the Bell basis, and 4 for the measurements, one defining each angle in the XZ-plane. Let

$$\begin{aligned}
|\Phi_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
|\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
|\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned} \tag{A28}$$

The two-qubit state is given by

$$\rho = \sum_{\alpha=0}^{3} \lambda_\alpha |\Phi_\alpha\rangle\langle\Phi_\alpha|, \tag{A29}$$

where $\lambda_\alpha \geq 0$ and $\sum_\alpha \lambda_\alpha = 1$. The measurements are given by

$$\begin{aligned}
A_x &= \cos a_x \, \sigma_Z + \sin a_x \, \sigma_X, \\
B_y &= \cos b_y \, \sigma_Z + \sin b_y \, \sigma_X,
\end{aligned} \tag{A30}$$

where $-\pi < a_x, b_y \leq \pi$, $x, y \in \{0, 1\}$. See [18, 30] for details of this reduction.

Our methodology will be to show that the only two-qubit strategy that satisfies the relations imposed by the SOS polynomials is the target strategy up to local unitaries, hence the extraction map can be written in terms of unitaries that rotate each Jordan block to the target.

4. Proof of the self-testing claim for the I_δ-family

We now prove the self-testing claim in Proposition 1, i.e., that the family of inequalities in Eq. (A1) self-tests the state and measurements in Eq. (A2).

Theorem 1 (Self-testing the I_δ-family)**.** *The family of Bell expressions in Eq. (A1) provides a self-test for the two-qubit state and family of measurements in Eq. (A2) according to Definition 1. [Equivalently, up to local isometries, the only state and measurements that satisfy $I_\delta = I_\delta^{\mathrm{Q}}$ are those of Eq. (A2).]*

Proof. The previous section implies that it is sufficient to consider two qubit states that are diagonal in the Bell basis as in (A29) and measurements of the form (A30). Consider the expectation value of the operator $\bar{S}_\delta$ for a two qubit

state ρ and measurements A_x, B_y that saturate the inequality in Eq. (A1):

$$\begin{aligned}\langle \bar{S}_\delta \rangle &= \sum_i \langle P_i^\dagger(\delta) P_i(\delta) \rangle \\ &= \sum_i \mathrm{Tr}[\rho P_i^\dagger(\delta) P_i(\delta)] \\ &= \sum_i \sum_\alpha \lambda_\alpha \| P_i(\delta) |\Phi_\alpha\rangle \|^2 = 0. \end{aligned} \tag{A31}$$

Since $\lambda_\alpha \geq 0,\ \| P_i(\delta)|\Phi_\alpha\rangle\|^2 \geq 0$, we have

$$\lambda_\alpha \| P_i(\delta)|\Phi_\alpha\rangle\|^2 = 0 \ \forall i \ \forall \alpha. \tag{A32}$$

Without loss of generality, suppose $\lambda_0 \neq 0$ (if $\lambda_0 = 0$, then for some α' with $\lambda_{\alpha'} \neq 0$, there is a local unitary U such that $U \otimes \mathbb{I}|\Phi_{\alpha'}\rangle = |\Phi_0\rangle$, so cases where $\lambda_0 = 0$ are equivalent to the case $\lambda_0 \neq 0$ up to local unitaries). Note that $(U \otimes U^{\mathrm{T}})|\Phi_0\rangle = |\Phi_0\rangle$ for all single qubit unitaries U, where U^{T} is the transpose of U in the $\{|0\rangle, |1\rangle\}$ basis. It follows that we can take $a_0 = 0$, i.e., $A_0 = \sigma_Z$.

By (A32), we have that $P_i(\delta)|\Phi_0\rangle = 0$ for $i = 0, 2$ (the cases $i = 1, 3$ are identical by linear dependence). Using the form of the measurements (cf. (A30)), we arrive at the system of nonlinear equations

$$(\sin\delta + \cos\delta)\sin b_0 + (\sin b_1 - \sin a_1) = 0, \tag{A33}$$
$$(\sin\delta - \cos\delta)\sin b_0 + (\sin b_1 + \sin a_1) = 0, \tag{A34}$$
$$(\sin\delta + \cos\delta)(\cos b_0 - 1) + (\cos b_1 - \cos a_1) = 0, \tag{A35}$$
$$(\sin\delta - \cos\delta)(\cos b_0 + 1) + (\cos b_1 + \cos a_1) = 0. \tag{A36}$$

Subtracting Eq. (A34) from Eq. (A33), and Eq. (A36) from Eq. (A35) gives

$$\sin a_1 = \sin b_0 \cos\delta, \tag{A37}$$
$$\cos a_1 = \cos b_0 \cos\delta - \sin\delta\,. \tag{A38}$$

Then using $\sin^2 a_1 + \cos^2 a_1 = 1$ we recover

$$\begin{aligned} 1 &= \sin^2 b_0 \cos^2\delta + (\cos b_0 \cos\delta - \sin\delta)^2 \\ &= 1 - \sin 2\delta\ \cos b_0, \end{aligned} \tag{A39}$$

and hence we have $\cos b_0 = 0$. Since $-\pi < b_0 \leq \pi$ we have $b_0 = \pm\pi/2$, i.e., $B_0 = \pm\sigma_X$. Noting that $\sigma_Z \otimes \sigma_Z$ has no effect on $|\Psi_0\rangle$ and that $\sigma_Z\sigma_X\sigma_Z = -\sigma_X$, we can take $b_0 = \pi/2$, i.e., $B_0 = \sigma_X$ without loss of generality. Then, $\sin b_0 = 1$.

Using these in (A33)–(A36) we find $\sin b_1 = -\sin\delta$ and $\cos b_1 = \cos\delta$, hence $b_1 = -\delta$. Similarly, $\sin a_1 = \cos\delta$ and $\cos a_1 = -\sin\delta$ so we have $A_1 = -\sin\delta\,\sigma_Z + \cos\delta\,\sigma_X$ and $B_1 = \cos\delta\,\sigma_Z - \sin\delta\,\sigma_X$, recovering the observables in Eq. (A2). We have therefore proved the self-testing of the measurements.

For the state, consider $\| P_i(\delta)|\Phi_\alpha\rangle\|^2$ for $i = 0, 2$ and $\alpha = 1, 2, 3$. By direct calculation, using the observables we found above, we find all of these to be $\cos^2\delta$. Hence, by (A32), we must have $\lambda_1 = \lambda_2 = \lambda_3 = 0$ and thus $\lambda_0 = 1$.

Finally we derive the extraction map from Definition 1. According to Jordan's lemma, both Hilbert spaces decomposes block-diagonally with 2×2 blocks. This is equivalent to identifying $\mathcal{H}_{\tilde{Q}_A} = \mathcal{H}_{F_A} \otimes \mathcal{H}_{Q_A}$ where F_A is a system that flags the 2×2 Jordan block, and Q_A is a qubit system (similarly for $\mathcal{H}_{\tilde{Q}_B}$). With purifying system E, the purified state hence takes the form

$$|\Psi\rangle_{\tilde{Q}_A\tilde{Q}_B E} = \sum_{ij} \sqrt{p_{ij}} |ij\rangle_{F_A F_B} \otimes |\varphi_{ij}\rangle_{Q_A Q_B} \otimes |ij\rangle_E, \tag{A40}$$

where $\rho_{\tilde{Q}_A\tilde{Q}_B} = \mathrm{Tr}_E\left[|\Psi\rangle\langle\Psi|_{\tilde{Q}_A\tilde{Q}_B E}\right] = \sum_{ij} p_{ij} |ij\rangle\langle ij|_{F_A F_B} \otimes |\varphi_{ij}\rangle\langle\varphi_{ij}|_{Q_A Q_B}$ is the state shared by the devices. Similarly, the measurements admit the decomposition

$$\tilde{A}_x \otimes \tilde{B}_y = \sum_{ij} |ij\rangle\langle ij|_{F_A F_B} \otimes A_x^i \otimes B_y^j. \tag{A41}$$

Above we established that, up to local unitaries, the only two qubit strategy that can achieve $\langle \tilde{S}_\delta \rangle = I_\delta^{\mathrm{Q}}$ is the target in Eq. (A2). Therefore, for every measurement pair $A_x^i \otimes B_y^j$ and state $|\varphi_{ij}\rangle$ there exist local unitaries $U_A^i : \mathcal{H}_{Q_A} \to \mathcal{H}_{Q_A}$

and $U_B^j : \mathcal{H}_{Q_B} \to \mathcal{H}_{Q_B}$ such that $U_A^i A_x^i (U_A^i)^\dagger = A_x$, $U_B^j B_y^j (U_B^j)^\dagger = B_y$, and $(U_A^i \otimes U_B^j)|\varphi_{ij}\rangle = |\Phi_0\rangle$. Thus, if we define the unitary

$$V = \sum_{ij} |ij\rangle\langle ij|_{F_A F_B} \otimes U_A^i \otimes U_B^j \otimes \mathbb{I}_E \,, \tag{A42}$$

then we have the extraction

$$V(\tilde{A}_x \otimes \tilde{B}_y \otimes \mathbb{I}_E)V^\dagger V|\Psi\rangle_{\tilde{Q}_A \tilde{Q}_B E} = (A_x \otimes B_y)|\Phi_0\rangle_{Q_A Q_B} \otimes \left(\sum_{ij} \sqrt{p_{ij}} |ij\rangle_{F_A F_B} \otimes |ij\rangle_E \right). \tag{A43}$$

This is of the form in Definition 1, and completes the self-testing proof. □

5. Proof of the self-testing claim for the J_γ-family

We follow an identical methodology to the previous section to prove the self-testing claim in Proposition 2.

Theorem 2 (Self-testing the J_γ-family)**.** *The family of Bell expressions in Eq. (A3) provides a self-test for the family of two qubit states and measurements in Eq. (A4) according to Definition 1. [Equivalently, up to local isometries, the only state and measurements that satisfy $J_\gamma = J_\gamma^{\mathrm{Q}}$ are those of Eq. (A4).]*

Proof. As in the proof of Theorem 1 we can use local unitaries to ensure that $\lambda_0 \neq 0$ and $a_0 = 0$. $P_0'(\gamma)|\Phi_0\rangle = 0$ and $P_2'(\gamma)|\Phi_0\rangle = 0$ then give

$$(2\mu - 1)(\sin b_1 - \sin a_1) + \sin b_0 = 0, \tag{A44}$$
$$(2\mu + 1)(\sin b_1 + \sin a_1) - \sin b_0 = 0, \tag{A45}$$
$$(2\mu - 1)(\cos b_1 - \cos a_1) + \cos b_0 - 1 = 0, \tag{A46}$$
$$(2\mu + 1)(\cos b_1 + \cos a_1) - \cos b_0 - 1 = 0, \tag{A47}$$

where $\mu = \cos(\gamma + \pi/6)$. Eliminating $\sin b_0$ from the first two and $\cos b_0$ from the second two gives

$$\sin a_1 = -2\mu \sin b_1 \tag{A48}$$
$$\cos a_1 = 1 - 2\mu \cos b_1 \,. \tag{A49}$$

Using $\sin^2 a_1 + \cos^2 a_1 = 1$ then gives $\cos b_1 = \mu = \cos(\gamma + \pi/6)$ and $\sin b_1 = \pm \sin(\gamma + \pi/6)$, corresponding to $B_1 = \cos(\gamma + \pi/6)\,\sigma_Z \pm \sin(\gamma + \pi/6)\,\sigma_X$. We can take the case with the minus sign without loss of generality by using the local unitary σ_Z if needed.

Eqs. (A48) and (A49) then give $\sin a_1 = \sin(2(\gamma + \pi/6))$ and $\cos a_1 = -\cos(2(\gamma + \pi/6))$.

Then (A45) gives

$$\sin b_0 = -\left(4\sin^3(\gamma + \pi/6) - 3\sin(\gamma + \pi/6)\right) = \sin(3(\gamma + \pi/6)) \,,$$

and (A47) gives

$$\cos b_0 = -\cos(3(\gamma + \pi/6)) \,.$$

We hence have

$$\begin{aligned} A_0 &= \sigma_Z \\ A_1 &= -\cos(2(\gamma + \pi/6))\,\sigma_Z + \sin(2(\gamma + \pi/6))\,\sigma_X \\ B_0 &= -\cos(3(\gamma + \pi/6))\,\sigma_Z + \sin(3(\gamma + \pi/6))\,\sigma_X \\ B_1 &= \cos(\gamma + \pi/6)\,\sigma_Z - \sin(\gamma + \pi/6)\,\sigma_X, \end{aligned}$$

which is equivalent to the measurement strategy in Eq. (A4).

The remainder of the argument is identical to that in the proof of Theorem 1. □

6. Evaluating the conditional entropy

By Jordan's lemma, there is no loss in generality if we assume the devices behave according to a convex combination of two-qubit strategies. As proved in the previous sections, the only two-qubit strategy that can saturate Eq. (A1) is that in Eq. (A2) (likewise the only two-qubit strategy that can saturate Eq. (A3) is that in Eq. (A4)), up to local unitaries. Therefore, according to Definition 1, there exists an isometry V from the reference system to the target two-qubit system. For completeness, we now show that the conditional entropy $H(AB|X=0,Y=0,E)$ when the devices maximally saturate one of the self-testing inequalities is equal to entropy of the target strategy unconditioned on Eve. We show this for the I_δ-family, and the proof for the J_γ-family is identical.

Theorem 3 (Entropy of self-tested strategies)**.** *For any physical system achieving $I_\delta = I_\delta^{\mathrm{Q}}$, its conditional entropy $H(AB|X=0,Y=0,E)_{\rho_{ABE}}$ evaluated for the post-measurement state ρ_{ABE} is given by the entropy of the target strategy unconditioned on E, i.e.,*

$$H(AB|X=0,Y=0,E)_{\rho_{ABE}} = H(AB|X=0,Y=0)_{\rho_{AB}} = H(\{\mathrm{p}(ab|00)\}), \tag{A50}$$

where $\mathrm{p}(ab|00)$ *is the distribution of the target two qubit strategy.*

Proof. The proof comes directly from the fact that the observation $I_\delta = I_\delta^{\mathrm{Q}}$ implies the post measurement state is uncorrelated with E, and the density operator ρ_E can be factored out as a tensor product, i.e. $\rho_{ABE} = \rho_{AB} \otimes \rho_E$. The post measurement state for measurements $X = Y = 0$ is proportional to

$$\rho_{ABE} = \sum_{ab} |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B \otimes \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B}\Big[(\tilde{M}_{a|0}\otimes\tilde{N}_{b|0}\otimes\mathbb{I}_E)|\Psi\rangle\langle\Psi|_{\tilde{Q}_A\tilde{Q}_BE}\Big], \tag{A51}$$

where $\tilde{M}_{a|x}, \tilde{N}_{b|y}$ are projectors for the observables $\tilde{A}_x = \tilde{M}_{0|x} - \tilde{M}_{1|x}$, $\tilde{B}_y = \tilde{N}_{0|y} - \tilde{N}_{1|y}$. From Theorem 1, the observation $I_\delta = I_\delta^Q$ implies the existence of the local isometry V satisfying

$$V\Big[(\tilde{A}_x\otimes\tilde{B}_y\otimes\mathbb{I}_E)|\Psi\rangle_{\tilde{Q}_A\tilde{Q}_BE}\Big] = (A_x\otimes B_y)|\psi\rangle_{Q_AQ_B}\otimes|\xi\rangle_{\mathrm{Junk}}, \tag{A52}$$

in accordance with Definition 1. Since the isometery acts as identity on E, we can decompose the junk system as $\mathcal{H}_{\mathrm{Junk}} = \mathcal{H}_J \otimes \mathcal{H}_E$. Using the fact that $V^\dagger V = \mathbb{I}$, we have the following series of equalities for the partial trace term:

$$\begin{aligned}
\mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B}\Big[(\tilde{M}_{a|0}\otimes\tilde{N}_{b|0}\otimes\mathbb{I}_E)|\Psi\rangle\langle\Psi|_{\tilde{Q}_A\tilde{Q}_BE}\Big] &= \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B}\Big[V^\dagger V(\tilde{M}_{a|0}\otimes\tilde{N}_{b|0}\otimes\mathbb{I}_E)V^\dagger V|\Psi\rangle\langle\Psi|V^\dagger V\Big]\\
&= \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B}\Big[V^\dagger\Big((M_{a|0}\otimes N_{b|0})|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|\Big)V\Big]\\
&= \mathrm{Tr}_{Q_AQ_BJ}\Big[(M_{a|0}\otimes N_{b|0})|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|\Big]\\
&= \mathrm{p}(ab|00)\mathrm{Tr}_J\big[|\xi\rangle\langle\xi|\big],
\end{aligned} \tag{A53}$$

where $\mathrm{p}(ab|xy) = \langle\psi|M_{a|x}\otimes N_{b|y}|\psi\rangle$ is the distribution generated by the target strategy. Consequently, the post-measurement state takes the form

$$\rho_{ABE} = \left(\sum_{ab}\mathrm{p}(ab|00)|a\rangle\langle a|\otimes|b\rangle\langle b|\right)\otimes\rho_E, \tag{A54}$$

where $\rho_E = \mathrm{Tr}_J\big[|\xi\rangle\langle\xi|_{JE}\big]$, and we find

$$r = \inf_{\substack{\rho_{Q_AQ_BE},\\ \{M_{a|x}\}_a,\{N_{b|y}\}_b\\ I_\delta = I_\delta^{\mathrm{Q}}}} H(AB|X=0,Y=0,E)_{\rho_{ABE}} = H(AB|X=0,Y=0)_{\rho_{AB}} = H(\{\mathrm{p}(ab|00)\})\,. \tag{A55}$$

This concludes the proof. □

As a corollary of Theorem 3, $r = 2$ when the I_δ inequalities are used, since $\mathrm{p}(ab|00) = \mathrm{p}_\delta(ab|00) = 1/4$ for the self-tested strategies in Eq. (A2). When the J_γ-family of self-tests are used, $r = 1 + H_{\mathrm{bin}}\Big[\frac{1}{2}(1+\sin 3\gamma)\Big]$, where $H_{\mathrm{bin}}(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy.

Appendix B: Proof of Proposition 3

In the main text, we made the following proposition regarding the I_δ and J_γ-family of self-tests described in the previous section:

Proposition 3 (Maximum randomness versus CHSH value). *The maximum randomness for strategies achieving a CHSH value in the range $s \in (2, 3\sqrt{3}/2]$ is 2 bits, and is generated by the family of strategies in Eq. (A2). For the range $s \in [3\sqrt{3}/2, 2\sqrt{2}]$, the maximum is given by*

$$1 + H_{\text{bin}}\Big[\frac{1}{2} + \frac{s}{2} - \frac{3}{\sqrt{2}}\cos\Big(\frac{1}{3}\arccos\Big[-\frac{s}{2\sqrt{2}}\Big]\Big)\Big], \tag{B1}$$

where $H_{\text{bin}}[\cdot]$ is the binary entropy, and is generated by the family of strategies in Eq. (A4).

This statement is trivial for CHSH scores in the range $(2, 3\sqrt{3}/2]$ since each member of the I_δ-family generates $r = 2$, the global maximum for this scenario. Moreover, the curve provided by the J_γ-family will always be a lower bound on the true maximum, since these are achievable randomness rates certified by the self-tests detailed in Appendix A 5. In this section we will prove that the J_γ-family give the maximum global randomness achievable by any strategy with the corresponding CHSH value.

Let $\mathcal{Q}$ denote the set of quantum distributions, and $\mathcal{C}(P)$ denote the CHSH value of a distribution P. Moreover, let $H(AB|X=0,Y=0,E)_P$ be the conditional von Neumann entropy of the outputs A, B for inputs $X = 0, Y = 0$ given observed distribution P, minimized over all quantum strategies that could give rise to P, i.e.,

$$H(AB|X=0,Y=0,E)_P := \inf_{\substack{\rho_{Q_A Q_B E},\\ \{M_{a|x}\}_a, \{N_{b|y}\}_b \\ \text{compatible with } P}} H(AB|X=0,Y=0,E)_{\rho_{ABE}}. \tag{B2}$$

Similarly, let $H(AB|X=0,Y=0)_P$ be the Shannon entropy of the distribution on A, B for inputs $X = 0, Y = 0$. Then the curve $R : [3\sqrt{3}/2, 2\sqrt{2}] \to [0, 2],\ s \mapsto R(s)$ we want to find is defined by the optimization

$$\begin{aligned} R(s) = \max_P\ & H(AB|X=0,Y=0,E)_P \\ \text{s.t.}\ \ & \mathcal{C}(P) = s, \\ & P \in \mathcal{Q}. \end{aligned} \tag{B3}$$

Our proof of Proposition 3 proceeds by defining a sequence of upper bounds on $\text{Graph}[R(s)] = \{(s, r) \mid r = R(s)\}$, before establishing that the final upper bound is achieved by our J_γ-family of self-tests.

Our first bound follows from strong subadditivity of the von Neumann entropy (that the entropy $H(AB|X=0,Y=0,E)$ cannot decrease if E is discarded) and is $R(s) \le \bar{R}(s)$, where

$$\begin{aligned} \bar{R}(s) = \max_P\ & H(AB|X=0,Y=0)_P \\ \text{s.t.}\ \ & \mathcal{C}(P) = s, \\ & P \in \mathcal{Q}. \end{aligned} \tag{B4}$$

First we prove the following two lemmas:

Lemma 4 (Monotonicity of $\bar{R}(s)$)**.** *The function $\bar{R}(s)$ is strictly decreasing on its domain.*

Proof. First note that $\bar{R}(3\sqrt{3}/2) > \bar{R}(s)\ \forall s \in (3\sqrt{3}/2, 2\sqrt{2}]$. This is because the largest CHSH value achievable when $\text{p}(ab|00) = 1/4$ is $3\sqrt{3}/2$, (see Corollary 1[1]). Because it is an entropy, the objective function $H(AB|X=0,Y=0)_P$ is concave in P, therefore the optimization (B4) defining $\bar{R}(s)$ is convex. It follows that $\bar{R}(s)$ is concave in s. To see

[1] Monotonicity of $\bar{R}(s)$ is not needed to establish Corollary 1.

this, let $\lambda \in [0,1]$ and $s_1, s_2 \in (3\sqrt{3}/2, 2\sqrt{2}]$, then

$$\begin{aligned}
\bar{R}[\lambda s_1 + (1-\lambda)s_2] &= \max_P \; H(AB|X=0,Y=0)_P \\
&\quad \text{s.t.} \;\; \mathcal{C}(P) = \lambda s_1 + (1-\lambda)s_2, \\
&\quad\quad\;\; P \in \mathcal{Q}, \\
&\geq \max_{P_1,P_2} \; H(AB|X=0,Y=0)_{\lambda P_1 + (1-\lambda)P_2} \\
&\quad \text{s.t.} \;\; \mathcal{C}(P_1) = s_1, \; \mathcal{C}(P_2) = s_2, \\
&\quad\quad\;\; P_1, P_2 \in \mathcal{Q}, \\
&\geq \max_{P_1,P_2} \; \lambda H(AB|X=0,Y=0)_{P_1} + (1-\lambda) H(AB|X=0,Y=0)_{P_2} \\
&\quad \text{s.t.} \;\; \mathcal{C}(P_1) = s_1, \; \mathcal{C}(P_2) = s_2, \\
&\quad\quad\;\; P_1, P_2 \in \mathcal{Q}, \\
&= \lambda \bar{R}(s_1) + (1-\lambda)\bar{R}(s_2),
\end{aligned} \tag{B5}$$

where we used the concavity of the Shannon entropy to obtain the inequality. Since $\bar{R}(s)$ is initially decreasing, and is a concave function, it must be monotonically decreasing. □

Lemma 5 (Inverse function of $\bar{R}(s)$)**.** *Suppose $r = \bar{R}(s)$. The function $\bar{R}(s)$ has the following inverse, denoted $\bar{R}^{-1}$, that satisfies $s = \bar{R}^{-1}(r)$, given by*

$$\begin{aligned}
\bar{R}^{-1}(r) = \max \; & \mathcal{C}(P) \\
\text{s.t.} \;\; & H(AB|X=0,Y=0)_P = r, \\
& P \in \mathcal{Q}.
\end{aligned} \tag{B6}$$

Proof. We prove Lemma 5 by showing $\bar{R}^{-1}(\bar{R}(s)) = s$, and $\bar{R}(\bar{R}^{-1}(r)) = r$, and using Lemma 4. First consider $\bar{R}^{-1}(\bar{R}(s)) = s$,

$$\begin{aligned}
\bar{R}^{-1}(\bar{R}(s)) = \max \; & \mathcal{C}(P) \\
\text{s.t.} \;\; & H(AB|X=0,Y=0)_P = \bar{R}(s), \\
& P \in \mathcal{Q}.
\end{aligned} \tag{B7}$$

The constraint $H(AB|X=0,Y=0)_P = \bar{R}(s)$ implies the achievable CHSH values for the distribution P must lie to the left of s, i.e., $\mathcal{C}(P) \leq s$, since the curve $\bar{R}(s)$ is decreasing (cf. Lemma (4)). We therefore have that $\bar{R}^{-1}(\bar{R}(s)) = \max_{\{P \in \mathcal{Q} \text{ s.t. } \mathcal{C}(P) \leq s\}} \mathcal{C}(P) = s$. For the other direction $\bar{R}(\bar{R}^{-1}(r))$, the same reasoning holds. The constraint $\mathcal{C}(P) = \bar{R}^{-1}(r)$ implies that $H(AB|X=0,Y=0)_P \leq r$ since any distribution that achieves a CHSH value of $\bar{R}^{-1}(r)$ can generate no more than r bits of randomness. Hence $\bar{R}(\bar{R}^{-1}(r)) = r$. This completes the proof. □

From the above lemma, we can solve for upper bounds on the points $(s, R(s)) \in \text{Graph}[R(s)]$ using the inverse function, i.e., $(s, \bar{R}(s)) = (\bar{R}^{-1}(r), r)$ where $\bar{R}(s) = r$. What remains is to compute $\bar{R}^{-1}(r)$ (or at least an upper bound, which will correspond to an upper bound on $R(s)$ due to the monotonicity argument). To do so we use the following two lemmas to formulate the constraints $H(AB|X=0,Y=0)_P = r$ as linear functions of the distribution P, defining a new upper bound:

Lemma 6. *Let $\mathcal{E}$ be the local channel that flips both output bits with probability $1/2$, i.e., $\mathcal{E} : \{p(ab|xy)\} \to \left\{\frac{1}{2}p(ab|xy) + \frac{1}{2}p(\bar{a}\bar{b}|xy)\right\}$ where $\bar{a}$ ($\bar{b}$) is the bit-wise complement of a (b), i.e., $\bar{a} = a \oplus 1$. The entropy after applying $\mathcal{E}$ is non-decreasing. Further, the CHSH value is invariant under $\mathcal{E}$.*

Proof. The first claim comes from the data processing inequality, that states that the entropy is non-decreasing under post-processing, i.e., $H(AB|X=0,Y=0)_P \leq H(AB|X=0,Y=0)_{\mathcal{E}(P)}$. The second claim comes from the fact that the correlators $\langle A_x B_y \rangle$ are invariant under $\mathcal{E}$. □

Notice that when Alice applies the post-processing map $\mathcal{E}$ to her devices, the probabilities are symmetrized, i.e., $\text{p}(aa|00) = \epsilon$, $\text{p}(a\bar{a}|00) = 1/2 - \epsilon$, $0 \leq \epsilon \leq 1/2$. In this case, we find $H(AB|X=0,Y=0)_{\mathcal{E}(P)} = 1 + H_{\text{bin}}(2\epsilon)$. As a

consequence of Lemma 6, we can define the following upper bound on $\bar{R}(s)$:

$$\begin{aligned}\bar{R}(s) \leq \bar{\bar{R}}(s) = \max\ & H(AB|X=0,Y=0)_{\mathcal{E}(P)} \\ \text{s.t.}\ & \mathcal{C}(\mathcal{E}(P)) = s, \\ & P \in \mathcal{Q} \\ = \max\ & H(AB|X=0,Y=0)_P \\ \text{s.t.}\ & \mathcal{C}(P) = s, \\ & \mathrm{p}(00|00) = \mathrm{p}(11|00), \\ & \mathrm{p}(01|00) = \mathrm{p}(10|00), \\ & P \in \mathcal{Q}, \end{aligned} \tag{B8}$$

where the second equality comes from the fact that optimizing the entropy over $\mathcal{E}(P), P \in \mathcal{Q}$ is equal to optimizing the entropy over symmetrized distributions in $\mathcal{Q}$ (following the convexity of $\mathcal{Q}$), and $\mathcal{C}(\mathcal{E}(P)) = \mathcal{C}(P)$. We can then define an inverse using Lemma 5, just as was done for $\bar{R}(s)$; we remark that Lemma 5 applies here, since Lemmas 4 and 5 will hold when $\mathcal{Q}$ is replaced by any convex subset of $\mathcal{Q}$, e.g., the set of symmetrized quantum distributions. This inverse is given by

$$\begin{aligned}\bar{\bar{R}}^{-1}(r) = \max\ & \mathcal{C}(P) \\ \text{s.t.}\ & H(AB|X=0,Y=0)_P = r, \\ & \mathrm{p}(00|00) = \mathrm{p}(11|00), \\ & \mathrm{p}(01|00) = \mathrm{p}(10|00), \\ & P \in \mathcal{Q}. \end{aligned} \tag{B9}$$

Lemma 7. *The optimization in Eq. (B9) has the following upper bound:*

$$\begin{aligned}\bar{\bar{R}}^{-1}(r) \leq \max\ & \mathcal{C}(P) \\ \text{s.t.}\ & \langle A_0 B_0 \rangle = 4\epsilon_r - 1, \\ & P \in \mathcal{Q}, \end{aligned} \tag{B10}$$

where ϵ_r satisfies $r = 1 + H_{\mathrm{bin}}(2\epsilon_r)$.

Proof. Firstly, consider symmetrized distributions, i.e., $\mathrm{p}(aa|00) = \epsilon$, $\mathrm{p}(a\bar{a}|00) = 1/2 - \epsilon$, $H(AB|X=0,Y=0)_P = 1 + H_{\mathrm{bin}}(2\epsilon)$. One can notice that for $\epsilon \in [1/4, 1/2]$ there is a one to one mapping between $H(AB|X=0,Y=0)_P$ and ϵ. Moreover, the range of ϵ we are interested in is given by $\epsilon \in [1/4, (2+\sqrt{2})/8]$, since $\epsilon = 1/4$ corresponds to the $\delta = \pi/6$ strategy ($r = 2$), and $\epsilon = (2+\sqrt{2})/8$ corresponds to the optimal CHSH strategy ($r \approx 1.6$). Hence for every choice of r, there exists a unique ϵ_r that satisfies $r = H(AB|X=0,Y=0)_P = 1 + H_{\mathrm{bin}}(2\epsilon_r)$ for $r \in [2, 1.6...]$. We can therefore write the constraint $r = H(AB|X=0,Y=0)_P$ in terms of linear functions of P:

$$\begin{aligned}\bar{\bar{R}}^{-1}(r) = \max\ & \mathcal{C}(P) \\ \text{s.t.}\ & \mathrm{p}(00|00) = \epsilon_r, \\ & \mathrm{p}(01|00) = \mathrm{p}(10|00) = \frac{1}{2} - \epsilon_r, \\ & P \in \mathcal{Q}, \end{aligned} \tag{B11}$$

where ϵ_r satisfies $r = 1 + H_{\mathrm{bin}}(2\epsilon_r)$. We can now relax this by considering the two party correlators, $\langle A_x B_y \rangle$; we replace the stronger constraints on the probabilities $\mathrm{p}(ab|00)$ with a single weaker constraint on the $X=0, Y=0$ correlator, and arrive at the desired upper bound. □

In the next two lemmas, we rewrite the upper bound in Eq. (B10) using an SOS decomposition. Let $C = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$ be the CHSH operator, and consider the following optimization:

$$\begin{aligned}\tilde{R}^{-1}(r) = \min_{t,z,S}\ & t \\ \text{s.t.}\ & t\mathbb{I} - C = S + z\Big(A_0B_0 - (4\epsilon_r - 1)\mathbb{I}\Big), \end{aligned} \tag{B12}$$

where S is an SOS decomposition for the operator expression $t\mathbb{I} - z\Big(A_0B_0 - (4\epsilon_r - 1)\mathbb{I}\Big) - C$. One can notice that for any feasible point (t, z, S), and any distribution P that satisfies $\langle A_0B_0\rangle = 4\epsilon_r - 1$, we get an upper bound on the CHSH value, $t \geq \langle C\rangle = \mathcal{C}(P)$. Hence $\tilde{R}^{-1}(r)$ gives an upper bound on the CHSH value across all distributions that satisfy $\langle A_0B_0\rangle = 4\epsilon_r - 1$, i.e., an upper bound on Eq. (B10). An SOS decomposition is given in the following lemma:

Lemma 8. *Let $\boldsymbol{R}$ be as defined in (1). The operator expression $t\mathbb{I} - z\Big(A_0B_0 - (4\epsilon_r - 1)\mathbb{I}\Big) - C$ admits the SOS decomposition*

$$M = \begin{bmatrix} m_2 - 1/2 & 1/2 & 0 & 0 \\ 1/2 & m_1 + (z+1)/2 & 0 & 0 \\ 0 & 0 & m_2 + 1/2 & -1/2 \\ 0 & 0 & -1/2 & m_1 - (z+1)/2 \end{bmatrix}, \tag{B13}$$

for any m_1, m_2 satisfying $2(m_1 + m_2) = t + z(4\epsilon_r - 1)$.

This was derived using the symmetry arguments as was done for self-testing, and one can verify for any m_1, m_2 that satisfy the equality condition $\boldsymbol{R}^\dagger M \boldsymbol{R} = t\mathbb{I} - z\Big(A_0B_0 - (4\epsilon_r - 1)\mathbb{I}\Big) - C$.

Lemma 9. *The upper bound in Eq. (B12) is equivalent to the the following optimization problem:*

$$\begin{aligned} \tilde{R}^{-1}(r) = \max_{\mu} \quad & \sqrt{(2-4\epsilon_r)^2 + (2-4\epsilon_r)\mu} + \sqrt{(4\epsilon_r)^2 - 4\epsilon_r\mu} + \mu \\ & 4\epsilon_r - 2 \leq \mu \leq 4\epsilon_r. \end{aligned} \tag{B14}$$

Moreover, the optimal value is given by

$$\tilde{R}^{-1}(r) = 6\cos(2\theta) - 4\cos^3(2\theta), \tag{B15}$$

for the optimal argument

$$\mu^* = 4\cos(2\theta)\sin^2(2\theta), \tag{B16}$$

where $\theta = \frac{1}{6}\arccos(1 - 4\epsilon_r)$.

Proof. By inserting the SOS decomposition from Lemma 8, we can rewrite the optimization in the following way:

$$\begin{aligned} \tilde{R}^{-1}(r) = \min_{t,z,m_1,m_2} \quad & t \\ \text{s.t.} \quad & \begin{bmatrix} m_2 - 1/2 & 1/2 \\ 1/2 & m_1 + (z+1)/2 \end{bmatrix} \succeq 0, \\ & \begin{bmatrix} m_2 + 1/2 & -1/2 \\ -1/2 & m_1 - (z+1)/2 \end{bmatrix} \succeq 0, \\ & 2(m_1 + m_2) = t + z(4\epsilon_r - 1) \\ = \min_{X_1, X_2} \quad & (2 - 4\epsilon_r)\mathrm{Tr}[X_1] + 4\epsilon_r \mathrm{Tr}[X_2] \\ \text{s.t.} \quad & \mathrm{Tr}[X_1|0\rangle\langle 1|] = 1/2, \\ & \mathrm{Tr}[X_2|0\rangle\langle 1|] = -1/2, \\ & \mathrm{Tr}[X_1|0\rangle\langle 0|] - \mathrm{Tr}[X_2|0\rangle\langle 0|] = -1, \\ & X_1 \succeq 0, \ X_2 \succeq 0, \end{aligned} \tag{B17}$$

where $\{|i\rangle\}$ is the standard computational basis. We remark that the particular form of the SOS decomposition used is not unique, and strictly speaking we therefore find and upper bound on $\tilde{R}^{-1}(s)$ when inserting this into the constraint. For ease of notation we redefine $\tilde{R}^{-1}(s)$ above and acknowledge this is an upper bound on Eq. (B12).

This SDP has the following dual:

$$\begin{aligned}
&\max_{\lambda,\nu,\mu} \ \lambda+\nu+\mu \\
&\text{s.t.} \quad \begin{bmatrix} 2-4\epsilon_r & -\lambda \\ -\lambda & 2-4\epsilon_r+\mu \end{bmatrix} \succeq 0, \\
&\qquad \begin{bmatrix} 4\epsilon_r & -\nu \\ -\nu & 4\epsilon-\mu \end{bmatrix} \succeq 0, \\
=&\max_{\lambda,\nu,\mu} \ \lambda+\nu+\mu \\
&\qquad 4\epsilon_r-2 \le \mu \le 4\epsilon_r, \\
&\qquad \lambda^2 \le (4\epsilon_r-2)^2-(4\epsilon_r-2)\mu, \\
&\qquad \nu^2 \le 4\epsilon_r(4\epsilon_r-\mu), \\
=&\max_{\mu} \ \sqrt{(4\epsilon_r-2)^2-(4\epsilon_r-2)\mu}+\sqrt{(4\epsilon_r)^2-4\epsilon_r\mu}+\mu \\
&\qquad 4\epsilon_r-2 \le \mu \le 4\epsilon_r,
\end{aligned} \tag{B18}$$

where the last equality comes from the fact that the objective is maximized when λ and ν saturate their respective upper bounds. The first claim then follows from strong duality. To see this, consider the primal problem in Eq. (B17); the point $(t, z, m_1, m_2) = (4, 0, 1, 1)$ satisfies $2(m_1+m_2) = t+z(4\epsilon_r-1)$, and the eigenvalues of the two matrices are given by $1 \pm 1/\sqrt{2} > 0$. This point is strictly feasible, i.e., Slater's condition holds.

For the second claim, consider the final optimization (B18) over μ. For algebraic convenience, let us use the shifted variable $m = \mu - 4\epsilon_r + 1$, with $-1 \le m \le 1$. Let $f(m)$ be the objective function in terms of m, i.e., $f(m) = m + 4\epsilon_r - 1 + \sqrt{2(1+m)(1-2\epsilon_r)} + 2\sqrt{\epsilon_r(1-m)}$. Then $f'(m) = 0$ gives

$$1 - \frac{\epsilon_r}{\sqrt{\epsilon_r(1-m)}} = \frac{1-2\epsilon_r}{\sqrt{2(1+m)(1-2\epsilon_r}}.$$

After some rearrangement we obtain

$$\frac{(m+4\epsilon_r-1)(4m^3-3m+4\epsilon_r-1)}{1-m^2} = 0.$$

The solutions are hence $m = 1-4\epsilon_r$ or m needs to be a solution of the cubic $4m^3-3m+4\epsilon_r-1=0$. Using the formula for the roots of a cubic we find the roots to be

$$m_k = \cos\left(\frac{1}{3}\arccos(1-4\epsilon_r) - \frac{2\pi k}{3}\right) \quad \text{where} \quad k = 0, 1, 2.$$

Considering the four stationary points and the two endpoints of the range of m we find that the maximum occurs for $m = m^* = \cos\left(\frac{1}{3}\arccos(1-4\epsilon_r)\right)$, which corresponds to $\mu = \mu^* = m^* + 4\epsilon_r - 1$. If we define $\theta = \frac{1}{6}\arccos(1-4\epsilon_r)$ so that $m^* = \cos(2\theta)$, $1-4\epsilon_r = \cos(6\theta)$ and $2\epsilon_r = \sin^2(3\theta)$, we find $\mu^* = \cos(2\theta) - \cos(6\theta)$. The maximum value of the objective function is

$$\begin{aligned}
f(m^*) &= \cos(2\theta) - \cos(6\theta) + \sqrt{2\cos^2(3\theta)(1+\cos(2\theta))} + \sqrt{2\sin^2(3\theta)(1-\cos(2\theta))} \\
&= \cos(2\theta) - \cos(6\theta) + 2\cos(\theta)\cos(3\theta) + 2\sin(\theta)\sin(3\theta) \\
&= 3\cos(2\theta) - \cos(6\theta) = 6\cos(2\theta) - 4\cos^3(2\theta)\,,
\end{aligned}$$

where we have used that for $\epsilon_r \in [1/4, 1/2]$, $\theta \in [\pi/12, \pi/6]$ so that $\cos(\theta)$, $\sin(\theta)$, $\cos(3\theta)$ and $\sin(3\theta)$ are all positive. □

Corollary 1. *The maximum CHSH score achievable by any quantum strategy with $p(ab|00) = 1/4$ for all a and b is $3\sqrt{3}/2$.*

Proof. When $\epsilon_r = 1/4$, $\tilde{R}^{-1}(r) = 3\sqrt{3}/2$, i.e., $3\sqrt{3}/2$ is an upper bound on the maximum achievable CHSH value when $\mathrm{p}(ab|00) = 1/4$. We know this upper bound is achievable for the $\delta = \pi/6$ self-test in Eq. (A1), hence this must be the true maximum. □

Our final theorem shows the optimality of the constructions.

Theorem 4 (Maximal global randomness versus CHSH value)**.** *The maximum global randomness, $R(s)$, for quantum strategies that achieve a particular CHSH value s is given by*

$$R(s) = \begin{cases} 2, & s \in (2, 3\sqrt{3}/2] \\ 1 + H_{\text{bin}}\left[\frac{1}{2} + \frac{s}{2} - \frac{3}{\sqrt{2}} \cos\left(\frac{1}{3}\arccos\left[-\frac{s}{2\sqrt{2}}\right]\right)\right], & s \in [3\sqrt{3}/2, 2\sqrt{2}], \end{cases} \tag{B19}$$

where $H_{\text{bin}}(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy. Moreover, the inequalities in Eq. (A1) and Eq. (A3) self-test the quantum state and measurements that achieve this maximum.

Proof. The case of $R(s) = 2$ for $s \in (2, 3\sqrt{3}/2]$ is trivially an upper bound on the maximum, and is shown to be achievable by the self-tests in Eq. (A1). For the case $s \in [3\sqrt{3}/2, 2\sqrt{2}]$, we use the sequence of upper bounds and inverse functions defined in this section. Consider the points $(s, r) \in \text{Graph}[R(s)]$. We have the following:

$$\begin{aligned} (s, r) &= (s, R(s)) \\ &\leq (s, \bar{R}(s)) \\ &\leq (s, \bar{\bar{R}}(s)) \\ &= (\bar{\bar{R}}^{-1}(r), r) \\ &\leq (\tilde{R}^{-1}(r), r), \end{aligned} \tag{B20}$$

where $\leq$ denotes component-wise inequality. Hence we can find an upper bound on $\text{Graph}[R(s)]$ using Lemma 9, i.e.

$$s \leq \tilde{R}^{-1}(r) = 6\cos 2\theta - 4\cos^3 2\theta, \;\; \theta = \frac{1}{6}\arccos[1 - 4\epsilon_r], \;\; r = 1 + H_{\text{bin}}(2\epsilon_r). \tag{B21}$$

We define this upper bound on $\text{Graph}[R(s)]$ as

$$\text{Graph}[\tilde{R}^{-1}(r)] = \left\{(s, r) \mid s = \tilde{R}^{-1}(r)\right\}. \tag{B22}$$

We now show it is achievable. From the self-tests in Eq. (A3), we find a tight lower bound on the conditional von Neumann entropy parameterized by $\gamma \in [0, \pi/12]$,

$$\begin{aligned} r(\gamma) &= \inf_{\substack{\rho_{Q_A Q_B E}, \\ \{M_{a|x}\}_a, \{N_{b|y}\}_b \\ \text{Compatible with: } \langle S_\gamma \rangle = I_\gamma^{\text{Q}}}} H(AB|X=0, Y=0, E)_{\rho_{ABE}} \\ &= H(AB|X=0, Y=0)_{P_\gamma} \\ &= 1 + H_{\text{bin}}\left[\frac{1}{2}(1 + \sin 3\gamma)\right], \end{aligned} \tag{B23}$$

where P_γ is the distribution generated by Eq. (A4). We find the associated CHSH value is given by

$$s(\gamma) = \mathcal{C}(P_\gamma) = \sin 3\gamma + 3\cos\left(\gamma + \frac{\pi}{6}\right). \tag{B24}$$

Since this is achievable, we have derived a parametric lower bound on $\text{Graph}[R(s)] = \{(s, r) \mid r = R(s)\}$:

$$\text{Graph}_\Gamma = \left\{(s(\gamma), r(\gamma)) \mid \gamma \in [0, \pi/12]\right\}. \tag{B25}$$

Analysing the $X = 0, Y = 0$ block of P_γ, we find $\epsilon_r = \frac{1}{4}(1 + \sin 3\gamma)$. Inverting this, we find $\gamma = \frac{1}{3}\arcsin[4\epsilon_r - 1]$, and inserting into Eq. (B24), we express s in terms of ϵ_r, and hence r. Calling this function $R_\Gamma^{-1}(r)$:

$$\begin{aligned} R_\Gamma^{-1}(r) \equiv s(\gamma) &= 4\epsilon_r - 1 + 3\cos\left(\frac{1}{3}\arcsin[4\epsilon_r - 1] + \frac{\pi}{6}\right) \\ &= -\cos 6\theta + 3\cos 2\theta = 6\cos 2\theta - 4\cos^3 2\theta, \end{aligned} \tag{B26}$$

where we used the identities $\arcsin(x) = -\arcsin(-x)$ and $\arcsin(x) = \pi/2 - \arccos(x)$. This implies

$$\text{Graph}_\Gamma = \text{Graph}[R_\Gamma^{-1}(r)] = \left\{(s, r) \mid s = R_\Gamma^{-1}(r)\right\}. \tag{B27}$$

One can immediately see that $R_\Gamma^{-1}(r) = \tilde{R}^{-1}(r)$, from which it follows $\mathrm{Graph}[\tilde{R}^{-1}(r)] = \mathrm{Graph}[R_\Gamma^{-1}(r)]$, i.e., the upper and lower bounds coincide, and $\mathrm{Graph}[R(s)] = \mathrm{Graph}[\tilde{R}^{-1}(r)] = \mathrm{Graph}[R_\Gamma^{-1}(r)]$. This shows that the family of inequalities in Eq. (A3) self-test the maximum.

From this, we can derive an explicit expression for $R(s)$, $s \in [3\sqrt{3}/2, 2\sqrt{2}]$. We begin by changing variables $\hat{\theta} = 2\theta = \frac{1}{3}\arccos[1 - 4\epsilon_r]$. We wish to express s in terms of $\hat{\theta}$, and hence ϵ_r, which amounts to solving the cubic

$$4\cos^3\hat{\theta} - 6\cos\hat{\theta} + s = 0. \tag{B28}$$

Employing another change of variables, $\cos\hat{\theta} = \sqrt{2}\cos\phi$:

$$4\cos^3\phi - 3\cos\phi = \cos 3\phi = -\frac{s}{2\sqrt{2}}, \tag{B29}$$

which has solutions

$$\phi_k = \frac{1}{3}\arccos\Big[-\frac{s}{2\sqrt{2}}\Big] + \frac{2\pi k}{3},\ k = 0, 1, 2. \tag{B30}$$

Notice for $\theta \in [\pi/12, \pi/8]$, we require $\sqrt{2}\cos\phi \in [\sqrt{3}/2, 1/\sqrt{2}]$, which for $s \in [3\sqrt{3}/2, 2\sqrt{2}]$ is only satisfied when $k = 0$. We therefore find that $\cos\hat{\theta} = \sqrt{2}\cos\Big(\frac{1}{3}\arccos\Big[-\frac{s}{2\sqrt{2}}\Big]\Big)$. We can now solve for ϵ_r, setting $\phi \equiv \phi_0$:

$$\begin{aligned}
\epsilon_r &= \frac{1}{4}(1 - \cos 3\hat{\theta}) \\
&= \frac{1}{4}(1 - 4\cos^3\hat{\theta} + 3\cos\hat{\theta}) \\
&= \frac{1}{4}\Big(1 - \sqrt{2}(1 - 4\cos^3\phi + 3\cos\phi - 4\cos^3\phi)\Big) \\
&= \frac{1}{4}\Big(1 - \sqrt{2} + 2\sqrt{2}\sin^2\Big(\frac{3\phi}{2}\Big) - 4\sqrt{2}\cos^3\phi\Big) \\
&= \frac{1}{4}\Big(1 + s - 3\sqrt{2}\cos\Big[\frac{1}{3}\arccos\Big(-\frac{s}{2\sqrt{2}}\Big)\Big]\Big),
\end{aligned} \tag{B31}$$

where for the second equality we used the identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, for third we used $1 - 4\cos^3\theta + 3\cos\theta = 2\sin^2\Big(\frac{3\theta}{2}\Big)$, $\sin^2\theta = \frac{1}{2}(1 - \cos 2\theta)$, and for the final we used the triple angle formula again. The claim then follows using the fact that $R(s) = 1 + H_{\mathrm{bin}}(2\epsilon_r)$. □