Self-testing Quantum States via Non-maximal Bell Violation

Ashutosh Rai,1,2 Matej Pivoluska,2,3 Souradeep Sasmal,4 Manik Banik,5 Sibasish Ghosh,6 and Martin Plesch2,3

1School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea
2Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia
3Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic
4Light and Matter Physics, Raman Research Institute, Bengaluru 560080, India
5School of Physics, IISER Thiruvananthapuram, Thiruvananthapuram, Kerala 695551, India
6Optics & Quantum Information Group, The Institute of Mathematical Sciences, HBNI, C.I.T. Campus, Taramani, Chennai 600113, India

Self-testing protocols enable certification of quantum devices without demanding full knowledge about their inner workings. A typical approach in designing such protocols is based on observing nonlocal correlations which exhibit maximum violation in a Bell test. We show that in Bell experiment known as Hardy’s test of nonlocality not only the maximally nonlocal correlation self-tests a quantum state, rather a non-maximal nonlocal behavior can serve the same purpose. We, in fact, completely characterize all such behaviors leading to self-test of every pure two qubit entangled state except the maximally entangled ones. Apart from originating a novel self-testing protocol, our method provides a powerful tool towards characterizing the complex boundary of the set of quantum correlations.

Introduction.—Learning quantum properties of an unknown physical system is ubiquitous for designing and testing devices based on the laws of quantum mechanics. Complete information about the physical state [1, 2] and process [3, 4] of such a device can be obtained through tomography which requires considerable resources for implementation. On the other hand, some particular properties of a quantum system, like certification of quantum entanglement or incompatibility of measurements, can be learnt with less resources by constructing suitable witness operators [5–9]. The aforesaid methods still might not be optimal or available for certain scenarios [10–12]. Interestingly, however, some physical systems can be certified by employing comparatively far less resources through device-independent tests where a device is treated simply as a black box [13–15]. Then only from the input-output statistics termed as correlation or behavior of the box one can find the quantum state of the device. Such a certification is referred to as a self-test as it enables a user to verify the device without knowing details of its inner-workings [16–28].

Bell inequalities naturally fit into the device-independent paradigm for certification of quantum systems since their derivations, based on the assumptions of local-realism [29], are independent of a quantum description of the physical state of the system or measurements applied to it [30–35]. Therefore, various kind of Bell inequalities play a central role in the construction of self-testing protocols [16–28]. In a Bell test only some special type of input-output statistics can self-test a quantum state; the one which can be realized (up to local isometry) by a unique quantum state and measurements [28]. Further, within the (convex) set of all quantum behaviors in a given Bell experiment those leading to self-testing protocols must necessarily be extremal points on the quantum boundary [26–28]. Then, the fact that any linear Bell inequality is maximized at some extremal point of the quantum set leads to a natural intuition that self-testing occurs on achieving maximal violation [18–28].

In our work, we present a different approach for self-testing quantum states. By considering a Bell experiment called Hardy’s test of nonlocality [32] we show that self-test of a quantum state is possible also with a non-maximal violation. Such self-tests can be achieved for a two-parametric set of pure qubit states, which cover the whole spectrum from almost-not-entangled to almost-fully-entangled states. This result is interesting per se, as it allows self-testing of a broad spectrum of states through a single Bell test. On top of that, it has two important corollaries. First, the presented method using the concave cover approach is very general and can also be applied to other types of Bell tests. Second, as the behaviors which lead to self-testing are extremal points of the set of all quantum correlations, our result forms a stepping stone in the way of characterizing this set [36–38] and provides an important tool for future work in this area; one such step is realized, as we find that a part of the boundary of the quantum set is determined from Hardy’s nonlocal correlations.

Hardy’s Test.—The nonlocality test proposed by Hardy [32] relates to a Bell experiment with two space-like separated parties, Alice and Bob, who share parts of a composite physical system. Alice randomly chooses to perform one of measurements $x \in \{A_0, A_1\}$ and Bob randomly chooses to perform one of measurements $y \in \{B_0, B_1\}$ on their respective parts. Outcomes of all the measurements are binary, denoted $a \in \{\pm 1\}$ for Alice and $b \in \{\pm 1\}$ for Bob. Result of the experiment is termed a correlation or a behavior and recorded
as a vector of probabilities: \( \mathcal{R} = \{ p(a, b|x, y) : x \in \{A_0, A_1 \}, y \in \{B_0, B_1 \}, \text{and } a, b \in \{\pm 1\} \} \). A behavior is termed local, if it can be expressed in factorized form, i.e., \( p(a, b|x, y) = \int_{\lambda \in \Lambda} d\lambda \ p(\lambda) \zeta(x, \lambda) \zeta(b, y, \lambda) \), where \( p(\lambda) \) is a probability distribution over a set of local-hidden-variables \( \Lambda \), and \( \zeta(x, \lambda), \zeta(b, y, \lambda) \) are local response functions of Alice and Bob respectively, which without loss of any generality can be considered as deterministic \[39\]. Any behavior that cannot have a local-hidden-variable model is called nonlocal. Hardy showed that if the four conditions

\[
\begin{align*}
 p_{\text{Hardy}}(+1, +1 | A_0, B_0) > 0, \\
p_{\text{Hardy}}(+1, -1 | A_0, B_1) = 0, \\
p_{\text{Hardy}}(-1, +1 | A_1, B_0) = 0, \\
p_{\text{Hardy}}(+1, +1 | A_1, B_1) = 0,
\end{align*}
\]

are satisfied, then the resulting behavior is necessarily nonlocal. The probability \( p_{\text{Hardy}} \) in Eq. (1a) quantifies the amount of nonlocality and it attains the maximum value \( p_{\text{max}}^{\text{Hardy}} = (-11 + 5\sqrt{5})/2 \) in quantum mechanics \[26\]; the maximum is achieved with projective measurements on a pure two qubit state \[26, 40\].

All two qubit states showing Hardy’s nonlocality.—In a two qubit state space \( C^2 \otimes C^2 \), Hardy’s nonlocal behaviors can result only from projective measurements on pure entangled states \[41\]. Without loss of generality, let us consider projective measurements of the following form

\[
\begin{align*}
 A_0 &= |0\rangle\langle 0|-|1\rangle\langle 1|, & A_1 &= |u_0\rangle\langle u_0|-|u_1\rangle\langle u_1|; \\
 B_0 &= |0\rangle\langle 0|-|1\rangle\langle 1|, & B_1 &= |v_0\rangle\langle v_0|-|v_1\rangle\langle v_1|;
\end{align*}
\]

where,

\[
\begin{align*}
 |u_0\rangle &= C_\alpha|0\rangle + e^{i\phi}S_\alpha|1\rangle, & |u_1\rangle &= -S_\alpha|0\rangle + e^{i\phi}C_\alpha|1\rangle, \\
 |v_0\rangle &= C_\beta|0\rangle + e^{i\phi}S_\beta|1\rangle, & |v_1\rangle &= -S_\beta|0\rangle + e^{i\phi}C_\beta|1\rangle,
\end{align*}
\]

with \( C_\alpha := \cos(z/2), \ S_\alpha := \sin(z/2) \) and \( \alpha, \beta \in [0, \pi] \) and \( \phi, \xi \in [0, 2\pi] \). Then, any pure two qubit state \( |\psi\rangle \) satisfying constraints of Eqs. (ib-1d) must be orthogonal to \( |0\rangle \otimes |v_1\rangle, \ |u_1\rangle \otimes |0\rangle, \) and \( |u_0\rangle \otimes |v_0\rangle, \) and therefore it must be of the form

\[
|\psi\rangle = T_a|u_0v_0\rangle + T_b|u_1v_0\rangle + |u_1v_1\rangle, \quad T_z := \tan \frac{z}{2}.
\]

The set of sixteen probabilities derived from the two qubit state in Eq. (3) and measurements given by Eq. (2) can be expressed in an array as follows

\[
\begin{array}{c|cccc}
 & (+, +) & (+, -) & (-, +) & (-, -) \\
 A_0B_0 & (1-r)(1-s) & (1-r)s & (1-r)s & (1-r)(1-s) \\
 A_0B_1 & (1-r)s & 0 & (1-r)s & (1-r)s \\
 A_1B_0 & (1-r)(1-s) & (1-r)s & 0 & (1-r)s \\
 A_1B_1 & 0 & 1-s & (1-r)s & (1-r)s \\
\end{array}
\]

where \( r := 1 - S_\alpha^2 S_\beta^2 \) and \( s := r^{-1} C_\alpha^2 \). Observe that \( 0 \leq r, s \leq 1 \) for any choice of \( \alpha, \beta \in [0, \pi] \). Additionally, a behavior \( \mathcal{R}_{\text{Hardy}} \) is nonlocal if and only if \( (r, s) \in (0, 1) \times (0, 1) \). The value of \( \alpha \) and \( \beta \) for a given value of \( r \) and \( s \) can be obtained from

\[
\alpha = 2\sin^{-1} \sqrt{1-r}, \quad \beta = 2\sin^{-1} \sqrt{(1-r)/(1-r_s)}.
\]

The two qubit Hardy state in Eq. (3) when expressed in the standard basis, and in terms of the parameters \( r \) and \( s \), takes the following form

\[
|\psi(r,s)\rangle = -e^{i\phi} \sqrt{(1-r)(1-s)} \langle 00| - e^{i\xi} \sqrt{(1-r)^2 s} \langle 10|,
\]

\[
- e^{i\phi} \sqrt{(1-r)(1-s)} \langle 10| + e^{i(\xi+\phi)} \sqrt{(1-r)^2 s} \langle 11|
\]
which states that for any concave real function $f$ where

$$x = (+1) \Pi_{\pm |x} + (-1) \Pi_{\pm |i} \quad \text{where} \ x \in \{A_0, A_1\},$$

$$y = (+1) \Pi_{\pm |y} + (-1) \Pi_{\pm |y} \quad \text{where} \ y \in \{B_0, B_1\}.$$ 

These observables can be written in a Jordan canonical form derived in Ref. [45] (also see [44, 46]), which states that: for any set of four projection operators $\{\Pi_{\pm |M_0}, \Pi_{\pm |M_0}, \Pi_{\pm |M_0}, \Pi_{\pm |M_0}\}$ acting on a Hilbert space $\mathcal{H}$ and satisfying conditions $\Pi_{\pm |M_0} + \Pi_{\pm |M_0} = I$ and $\Pi_{\pm |M_0} + \Pi_{\pm |M_0} = I$, there is an orthonormal basis of $\mathcal{H}$ in which all the four operators are simultaneously block diagonal with maximum block size $2 \times 2$. The orthonormal basis induces a direct sum decomposition $\mathcal{H} = \bigoplus_k \mathcal{H}^k$ where dimension of each component subspace $\mathcal{H}^k$ is at most two. Then, the four projection operators can be decomposed as $\Pi_{\pm |M_0} = \bigoplus_k \Pi_{\pm |M_0}$ and each component $\Pi_{\pm |M_0}$ acts (non-identity) only on subspace $\mathcal{H}^k$. The projector on subspace $\mathcal{H}^k$ can be written as $\Pi^k = \Pi_{\pm |M_0} + \Pi_{\pm |M_0} = \Pi_{\pm |M_0} + \Pi_{\pm |M_0}$.

On applying the stated result to the observables $A_0, A_1$ ($B_0, B_1$) and state space $\mathcal{H}_A$ ($\mathcal{H}_B$) of Alice (Bob) gives

$$p(a, b | x, y) = \sum_{ij} \mu_{ij} \Tr(\rho_{ij} \Pi_{|a, b|} \otimes \Pi_{|x, y|}) = \sum_{ij} \mu_{ij} p_{ij}(a, b | x, y),$$

where $\mu_{ij} = \Tr(\rho_{ij} \Pi_{|a, b|} \otimes \Pi_{|x, y|})$ and satisfies $\sum_{ij} \mu_{ij} = 1$ and $\mu_{ij} \geq 0$, and $p_{ij} = (\Pi_{|a, b|} \otimes \Pi_{|x, y|})/\mu_{ij}$ is trace one positive operator on component subspace $\mathcal{H}_A^k \otimes \mathcal{H}_B^l$.

Let us define from the probabilities in Eq. (4) a function $\Omega(r, s) = \sum_{a,b,x,y} c_{abxy} p(a, b | x, y) + c_0$ where $c_{abxy}$ and $c_0$ are some real coefficients. Then on applying Eq. (7) to each probability term in $\Omega(r, s)$ we get

$$\Omega(r, s) = \sum_{ij} \mu_{ij} \Omega(r_{ij}, s_{ij}),$$

where $r_{ij} = p_{ij}(-1, -1 | A_0, B_0)$ and $s_{ij} = p_{ij}(-1, -1 | A_1, B_0)$. From Eq. (7) one can find that $r = \sum_{ij} \mu_{ij} r_{ij}$ and $s = \sum_{ij} \mu_{ij} s_{ij}$. Furthermore, whenever the black-box statistics satisfies the zero constraints of Hardy’s test, then the same is true in every $\mathcal{H}_A^k \otimes \mathcal{H}_B^l$ subspace. Now we like to state and prove the following Lemma.

**Lemma 1.** Let $E(r, s) : (0, 1) \times (0, 1) \to \mathbb{R}$ be a concave envelope of $\Omega(r, s)$, and suppose $\Omega(r, s) = \Omega(r, s) \circ \Omega(r, s)$ for $(r, s) \in \mathcal{R}$. Then for all $(r, s) \in \mathcal{R}$, and for all $(i, j)$, $r_{ij} = r$ and $s_{ij} = s$, provided $\Omega(r, s)$ is a nonlinear function of $r$ and $s$ over the region $\mathcal{R}$.

**Proof.** A concave envelope $E(r, s)$ of a function $\Omega(r, s)$ over the domain $(0, 1) \times (0, 1)$ is defined as the lowest-valued concave function that overestimates or equals $\Omega(r, s)$ in its domain. Now consider Jensen’s inequality which states that for any concave real function $f(x)$:

$$f(x) \leq f(\mathbb{E}[x])$$

where $\mathbb{E}[x]$ denotes the expected value of $x$. This inequality is known as Jensen’s inequality.

**Figure 1:** The light (blue) shaded region $\Omega^*(r, s)$ is concave. The dark (blue) region is $\mathcal{R}^*(r, s)$ where the concave cover $E^*(r, s) = \Omega^*(r, s)$. The dark (blue) dot shows point $(r, s) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ where $\Omega^*(r, s)$ is maximized.
The function $\Omega^\ast(r,s)$ is a nonlinear function and it is concave in a part of its domain. Further, for the considered function, thereexist a concave cover $\mathcal{E}^\ast(r,s)$, and a region $\mathcal{R}^\ast \subset (0,1) \times (0,1)$ where $\mathcal{E}^\ast(r,s) = \Omega^\ast(r,s)$. We constructed the cover function numerically, and then find the region $\mathcal{R}^\ast$ as shown in Fig. 1 (see Appendix (A.) for the method). From the considered example and application of Lemma 1, we conclude that if probability distribution of the black-box is such that $(r,s) \in \mathcal{R}^\ast$ then in every subspace $H_A^i \otimes H_B^j$, $r_{ij} = r$ and $s_{ij} = s$. We now ask whether such a property can hold for all $(r,s) \in (0,1) \times (0,1)$. In other words, is it possible to vary over the possible choice of functions $\Omega(r,s)$ such that union of all the resulting regions covers the full parameter space $(0,1) \times (0,1)$? Such a property will free the black box parameters $r$ and $s$ from any restrictions and lead to an interesting extension of Lemma 1. We find answer to the question in affirmative through the following lemma.

**Lemma 2.** If the black-box statistics in the Bell-experiment is of the form $\mathcal{S}_{\text{total}}(r,s)$ as in Eq. (4), then for all $(r,s) \in (0,1) \times (0,1)$ in every $H_A^i \otimes H_B^j$ subspace, $r_{ij} = r$ and $s_{ij} = s$.

*Proof.* First we recall that Lemma 1 is applicable to any function $\Omega(r,s)$ defined as some linear combination of all the probabilities in Eq (4) plus a constant term. We find that, a proof of Lemma 2 follows on considering simply a single parameter family of functions

$$\Omega_v(r,s) = \Omega^\ast(r,s) + \nu p(+|A_0) + (1-\nu) p(-|A_0) - 1/2,$$

where $0 \leq \nu \leq 1$, $p(+|A_0) = p(+,+|A_0B_0) + p(+,-|A_0B_0)$, and $p(-|A_0) = 1 - p(+|A_0)$. Note that at $\nu = 1/2$, $\Omega_{1/2}(r,s) \equiv \Omega^\ast(r,s)$ and $\mathcal{R}_{1/2} \equiv \mathcal{R}^\ast$. For the family of functions $\Omega_v(r,s)$ on considering $\nu \in \{d/N : d \in \{1,2,...,N-1\}\}$, we find that for a sufficiently large value of $N$, $\cup_v \mathcal{R}_v$ is shown when for $N = 10$, i.e., when the parameter $\nu$ takes values from the set $\{0.1, 0.2,..., 0.9\}$. Note that the region where $r_{ij} = r$ and $s_{ij} = s$, in all $H_A^i \otimes H_B^j$ subspace, is expanded. A more detailed exposition of the proof which follows on increasing the value of $N$ is provided in the Appendix (B).

Finally, in the following we prove the main result of the paper by using Lemma 2.

**Theorem.** In a black-box Bell experiment, if a behavior $\mathcal{S}_{\text{total}}(r,s)$ of the form given in Eq. (4) is observed, then the state of unknown system $\rho_{AB}$ is equivalent up to local isometries to $|\zeta\rangle^{AB} \otimes |\psi(r,s)\rangle^{A'B'}$ where $|\psi(r,s)\rangle_{\text{total}}$ is the pure two qubit Hardy state given by the Eq. (6) and $|\zeta\rangle^{AB}$ is some arbitrary bipartite state.

*Proof.* Consider a purification $|\chi\rangle^{ABP}$ of the unknown state $\rho_{AB}$, in brief we denote such a purification simply as $|\chi\rangle^{AB}$ since the desired local isometry is not required to act on the purification space [28]. Also observables $A_0, A_1, B_0, B_1$ can be considered in a $2 \times 2$ block diagonal form [28]. Then, there is a basis in which the observables are in the following block diagonal form

$$\begin{align*}
\Pi^+_+|A_0 &= |2i\rangle\langle 2i|, \\
\Pi^+_+|A_1 &= |u_{2i}\rangle\langle u_{2i}|, \\
\Pi^-_+|B_0 &= |2j\rangle\langle 2j|, \\
\Pi^-_+|B_1 &= |v_{2j}\rangle\langle v_{2j}|,
\end{align*}$$

where,

$$\begin{align*}
|u_{2i}\rangle &= C_{\alpha_i}|2i\rangle + e^{i\phi}S_{\alpha_i}|2i+1\rangle, \\
|u_{2i+1}\rangle &= -S_{\alpha_i}|2i\rangle + e^{i\phi}C_{\alpha_i}|2i+1\rangle, \\
|v_{2j}\rangle &= C_{\beta_j}|2j\rangle + e^{i\phi}S_{\beta_j}|2j+1\rangle, \\
|v_{2j+1}\rangle &= -S_{\beta_j}|2j\rangle + e^{i\phi}C_{\beta_j}|2j+1\rangle,
\end{align*}$$

with $i, j \in \{0,1,2,...\}$, $\alpha_i, \beta_j \in [0,\pi]$ and $\phi, \xi \in [0,2\pi)$. Note that, without loss of generality, the phases $\xi$ and $\phi$ can be considered independent of indices $i$ and $j$ in every $H_A^i \otimes H_B^j$ subspace since this can be achieved by choosing a suitable measurement basis and rotating the state by local unitaries such that the probabilities $p_{ij}(a,b|x,y)$ remain invariant. Also note that in the subspace $H_A^i \otimes H_B^j$ parameters $r_{ij}$ and $s_{ij}$ are given by $r_{ij} = 1 - S_{\alpha_i}^2C_{\beta_j}^2$, $s_{ij} = r_{ij}^{-1}C_{\alpha_i}^2$. Now suppose $\mathcal{S}_{\text{total}}(r,s)$ is observed in the black-box experiment, then Lemma 2 implies that in each subspace $H_A^i \otimes H_B^j, r_{ij} = r$ and $s_{ij} = s$.
and \( s_{ij} = s \) and, therefore, \( \mathcal{T}_{\text{Hardy}}(r_{ij}, s_{ij}) = \mathcal{T}_{\text{Hardy}}(r, s) \).

This can be true if and only if in \( \mathcal{H}_A \otimes \mathcal{H}_B \) subspace, \( \rho_{ij} = |\psi_{\text{Hardy}}\rangle_i \langle \psi_{\text{Hardy}}|_j \), where

\[
|\psi_{\text{Hardy}}\rangle_{ij} = -\sqrt{\frac{(1-r)(1-s)}{1-rs}}|2i, 2j\rangle - e^{i\theta_0}\sqrt{\frac{(1-r)(1-s)}{1-rs}}|2i, 2j+1\rangle
- e^{i\theta_1}\sqrt{\frac{(1-r)(1-s)}{1-rs}}|2i+1, 2j\rangle + e^{i\theta_2}\sqrt{\frac{(1-r)(1-s)}{1-rs}}|2i+1, 2j+1\rangle, \tag{15}
\]

Hence, the unknown state \( |\chi\rangle^{AB} \) can only be a direct sum of the form \( |\chi\rangle^{AB} = \bigoplus_{ij} \sqrt{\mu_{ij}} |\psi_{\text{Hardy}}\rangle_{ij} \). Finally, we can give local isometries \( \Phi^A \) and \( \Phi^B \) such that

\[
(\Phi^A \otimes \Phi^B)|\chi\rangle^{AB}|00\rangle^{A'B'} = |\xi\rangle^{AB} \otimes |\psi(r, s)\rangle^{A'B'}. \tag{46}
\]

where components of the \( |00\rangle^{A'B'} \) are local ancilla qubits appended to the unknown state \( |\chi\rangle^{AB} \), and after application of the local isometry \( \Phi^A \otimes \Phi^B \) we want to get the target state \( |\psi_{(r, s)}\rangle^{A'B'} \) along with some arbitrary bipartite state \( |\xi\rangle^{AB} \). The isometry map \( \Phi^A = \Phi^B = \Phi \) with \( \Phi |2k, 0\rangle^{XX} \rightarrow |2k, 0\rangle^{XX} \) and \( \Phi |2k + 1, 0\rangle^{XX} \rightarrow |2k, 1\rangle^{XX} \), where \( XX' \in \{ AA', BB' \} \), has the desired property. This concludes our proof.

The Theorem implies that any behavior in the form of Eq. (4) are extremal points of the set of quantum behaviors and hence it determines a part of the quantum boundary. Further, one can check that all the behaviors that are Hardy nonlocal but not in the form given by Eq. (4) are in the interior of the quantum set and they must arise on measuring mixed entangled states in higher than two qubit dimensions.

**Discussion and conclusion.**—Hardy’s test of nonlocality, viewed differently, is a form of tailored Bell inequality [47, 48]. However, in distinction to, for instance, tilted-Clauser-Horne-Shimony-Holt inequality [47], Hardy’s test places certain constraints on some outcome probabilities; note that in a Bell test such constraints can take variety of forms. Importance of tailored Bell inequalities is starkly revealed through various protocols for self-testing, randomness generation, quantum key distribution, etc., wherever the knowledge of the geometry of the quantum set of correlations plays a crucial role [36]. In this sense tailoring by constraining outcome probabilities can possibly play an important role, as we have demonstrated in this work through the Hardy’s test. The fact that our approach can have broader applications can be seen by noticing the three key features in the derivation of our results: (i) due to the constraints on probabilities a Hardy nonlocal state in a two qubit space is pure and unique for an arbitrarily fixed measurement [41, 43], (ii) existence of a simple Jordan canonical form for two dichotomic observables for each party [44–46], and (iii) possibility of finding a concave cover to an arbitrary linear combination of outcome probabilities and application of Jensen’s inequality. Note that, there can be tailored Bell tests other than Hardy’s where the three properties may hold. In general, these three features may be found in any Bell scenario with \( n \)-parties, two measurements per party, and two outcomes to every measurement.

To summarize, in this work, we have presented a method for self-testing quantum states by using the concave cover of a linear combination of observed outcome probabilities. We showcased the applicability of this approach on Hardy’s test of nonlocality, leading to a two-parametric set of characterizable states with a broad spectrum of entanglement properties. This technique allows a full (up to local isometries) specification of the source state, even without maximal violation in Hardy’s test. Our results show many potential development paths as the method introduced in this work can be possibly applied to different kind of Bell tests, allowing better specification of source states in a device-independent fashion. At the same time, it provides a very powerful tool for characterizing the boundary of the quantum set of correlations.

**Acknowledgements.**—AR is primarily supported by the National Research Foundation of Korea (NRF-2021R1A2C2006309), an Institute of Information and Communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (Grant No. 2019-0-00831) and the University IT Research Center (ITRC) Program (IITP-2021-2018-0-01402). AR, M. Pivoluska, and M. Plesch acknowledge funding and support from VEGA Project No. 2/0136/19. M. Pivoluska, and M. Plesch additionally acknowledge GAMU project MUNI/G/1596/2019. MB acknowledges support through the research grant of INSPIRE Faculty fellowship from the Department of Science and Technology, Government of India.

AR thankfully acknowledge fruitful discussions with Prof. Joonwoo Bae, Prof. Guruprasad Kar, and Dr. Ramij Rahaman at different stages of this work.
APPENDICES

Appendix (A): Computation of Concave cover for functions $\Omega(r,s)$

Let us describe our method for computing the concave covers to the class of functions $\Omega(r,s)$ introduced in Lemma-1 of the main text. Consider the first concrete example to which application of the Lemma-1 gives interesting insight,

$$\Omega^*(r,s) = \frac{r (1-r) s (1-s)}{1-rs}.$$  \hfill (16)

The three dimensional plot of $\Omega^*(r,s)$ is shown in Fig.(3a) which indicates that the function can be concave in some parts of its domain. On computing the two eigenvalues of Hessian matrix of $\Omega^*(r,s)$ we find that there a region of domain where both the eigenvalues are negative, therefore, the function is concave in this region; this region is shown in Fig.(3b).

![Figure 3: Region of concavity for the function $\Omega^*(r,s)$](image)

Next, we constructed a concave cover $E^*(r,s)$ of the function $\Omega^*(r,s)$. Recall that by definition a concave cover of the function $\Omega^*(r,s)$ is the lowest-valued concave function that overestimates or equals $\Omega^*(r,s)$ in its domain. We numerically computed the concave cover by applying the ConvexHullMesh function provided in MATHEMATICA. The concave cover $E^*(r,s)$ is shown in Fig.(4a) and the part of domain $R^*$ where $E^*(r,s) = \Omega^*(r,s)$ is shown as a shaded region in Fig.(4b). Figure one of the main text is obtained by superposing Fig.(3b) and Fig.(4b).

By a similar procedure one can construct the concave cover $E(r,s)$ to any function $\Omega(r,s)$, and then the corresponding region $R$ where $E(r,s) = \Omega(r,s)$.

Appendix (B): Details of the proof for Lemma-2 in the main text

Let us now consider the following single parameter family of functions, of the two variables $r$ and $s$, introduced in the construction of the proof of Lemma-2 in the main text

$$\Omega_v(r,s) = \Omega^*(r,s) + v |A_0| + (1-v) p(-1 | A_0|) - 1/2,$$

$$= \Omega^*(r,s) + v (s-rs) + (1-v) (1-s+rs) - 1/2,$$ \hfill (17)
(a) Concave cover $E^*(r,s)$ of function $\Omega^*(r,s)$

(b) Shaded (Blue) region shows $\mathcal{R}^*$ where $E^*(r,s) = \Omega^*(r,s)$

**Figure 4**: Construction of concave cover $E^*(r,s)$ and region $\mathcal{R}^*$

where the parameter $\nu \in (0,1)$ and variables $(r, s) \in (0,1) \times (0,1)$. Firstly, we constructed finite subset of functions from the family in Eq. (17) containing $N-1$ members: $S_N = \{\Omega_\nu(r,s) : \nu \in \{d/N : d \in \{1, 2, ..., N-1\}\}\}$. Let us denote the $k$-th member of $S_N$ by $S_N(k)$ where $k \in \{1, 2, ..., N-1\}$.

(a) $\mathcal{R}_{\nu}^* (\nu = 1/4)$

(b) $\mathcal{R}_{\nu}^* (\nu = 1/2)$

(c) $\mathcal{R}_{\nu}^* (\nu = 3/4)$

(d) $\cup_{\nu} \mathcal{R}_{\nu}^*$

**Figure 5**: Plots of regions $\mathcal{R}_{\nu}^*$ and $\cup_{\nu} \mathcal{R}_{\nu}^*$ for $\nu \in \{1/4, 1/2, 3/4\}$ and $N = 4$.

(a) $N = 2$

(b) $N = 5$

(c) $N = 10$

(d) $N = 100$

**Figure 6**: Plots of region $\cup_{\nu} \mathcal{R}_{\nu}^*$ for different values of $N$.

Secondly, we numerically constructed concave envelope functions of $S_N(k)$ for all values of $k$ by ConvexHullMesh
function in MATHEMATICA, then the region of domain where value of a concave envelope function coincide with the value of $S_R(k)$ was found as $R_V$. Finally, for fixed values of $N$ the region $\cup \mathcal{R}_V$ was constructed. For example, the Fig. (5) shows these region for $N = 4$. By the above procedure, for a sufficiently large value of $N$ we find that \( \cup \mathcal{R}_V = (0, 1) \times (0, 1) \). As an illustration see Fig. (6) where the region $\cup \mathcal{R}_V$ is plotted when $N$ take values 2, 5, 10, and 100.

[1] In Quantum State Estimation, edited by M. Paris and J. Rehacek, Lect. Notes Phys. Vol. 649 (Springer, Heidelberg, 2004).
[2] D. Gross, Yi-Kai Liu, S. T. Flammia, S. Becker, and J. Eisert; Quantum State Tomography via Compressed Sensing, Phys. Rev. Lett. 105, 150401 (2010).
[3] J. L. O’Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, Quantum Process Tomography of a Controlled-NOT Gate, Phys. Rev. Lett. 93, 080502 (2004).
[4] M. Mohseni, A. T. Rezakhani, and D. A. Lidar, Quantum-process tomography: Resource analysis of different strategies, Phys. Rev. A 77, 032322 (2008).
[5] O. Gühne and G. Tóth; Entanglement Detection, Phys. Rep. 474, 1 (2009).
[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. 81, 865 (2009).
[7] C. Carmeli, T. Heinosaari, and A. Toigo, Quantum Incompatibility Witnesses, Phys. Rev. Lett. 122, 170402 (2019).
[8] J. Bae, D. Chruscinski and B.C. Hiesmayr; Mirrored entanglement witnesses, NPJ Quantum Inf. 6, 15 (2020).
[9] J. Bavaresco, N.H. Valencia, C. Klöckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, M. Huber; Measurements in two bases are sufficient for certifying high-dimensional entanglement, Nature Phys. 14, 1032–1037 (2018).
[10] B. Reichhardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature 496, 456 (2013).
[11] U. Vazirani and T. Vidick; Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 113, 140501 (2014).
[12] C. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, Journal of the ACM. 63, 33 (2016).
[13] V. Scarani; The device-independent outlook on quantum physics (lecture notes on the power of Bell’s theorem), Acta Physica Slovaca 62, 347, (2012) arXiv:1303.3081 [quant-ph].
[14] S. Pironio, V. Scarani, and T. Vidick; Focus on device-independent quantum information, New J. Phys. 18, 100202 (2016).
[15] A. Acín and M. Navascués, Black box quantum mechanics, in Quantum [Un]Speakables II, edited by R. Bertlmann and A. Zeilinger (Springer, Berlin, 2017), pp. 307–319.
[16] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. 4, 273 (2004) [arXiv:quant-ph/0307205].
[17] M. McGague, T.H. Yang and V. Scarani, Robust self-testing of the singlet, J. Phys. A: Math. Theor. 45, 455304 (2012).
[18] T. H. Yang and M. Navascues, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A 87, 050102(R) (2013).
[19] 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, Phys. Rev. A 91, 052111 (2015).
[20] Y. Wang, X. Wu and V. Scarani; All the self-testings of the singlet for two binary measurements, New J. Phys. 18, 025021 (2016).
[21] A. Coladangelo, K.T. Goh and V. Scarani; All pure bipartite entangled states can be self-tested, Nat. Commun. 8, 15485 (2017).
[22] T. Coopmans, J. Kaniewski, and C. Schaffner, Robust self-testing of two-qubit states, Phys. Rev. A 99, 052123 (2019).
[23] J. Kaniewski, Weak form of self-testing, Phys. Rev. Research 2, 033420 (2020).
[24] S. Ishizaka, Geometrical self-testing of partially entangled two-qubit states, New J. Phys. 22, 023022 (2020).
[25] F. Baccari, R. Augusiak, I. Supic, and A. Acín; Device-Independent Certification of Genuinely Entangled Subspaces, Phys. Rev. Lett. 125, 260507 (2020).
[26] R. Rabelo, L. Y. Zhi, and V. Scarani; Device-Independent Bounds for Hardy’s Experiment, Phys. Rev. Lett. 109, 180401 (2012).
[27] A. Rai, M. Pivoluska, M. Plesch, S. Sasmal, M. Banik, and S. Ghosh; Device-independent bounds from Cabello’s nonlocality argument, Phys. Rev. A 103, 062219 (2021).
[28] I. Supic and J. Bowles; Self-testing of quantum systems: a review, Quantum 4, 337 (2020).
[29] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. A 47, 777 (1935).
[30] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics 1, 195 (1964); J. S. Bell, On the problem of hidden variables in quantum mechanics, Rev. Mod. Phys. 38, 447 (1966).
[31] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. 23, 880 (1969).
[32] Lucien Hardy, Nonlocality for two particles without inequalities for almost all entangled states, Phys. Rev. Lett. 71, 1605 (1993).
[33] M.J.W. Hall, Relaxed Bell inequalities and Kochen-Specker theorems, Phys. Rev. A 84, 022102 (2011).
[34] V. Scarani, Bell Nonlocality, Oxford University Press, London, (2019).
[35] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. 86, 419 (2014).
[36] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vertesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, Geometry of the set of quantum correlations, Phys. Rev. A 97, 022104 (2018).
[37] S. Ishizaka, Necessary and sufficient criterion for extremal quantum correlations in the simplest Bell scenario, Phys. Rev. A 97, 050102(R) (2018).
[38] A. Rai, C. Duarte, S. Brito, and R. Chaves, Geometry of the quantum set on no-signaling faces, Phys. Rev. A 99, 032106 (2019).
[39] A. Fine; Hidden Variables, Joint Probability, and the Bell Inequalities, Phys. Rev. Lett. 48, 291 (1982).
[40] K. P. Seshadreesan and S. Ghosh, Constancy of maximal nonlocal probability in Hardy’s nonlocality test for bipartite quantum systems, J. Phys. A: Math. Theor. 44, 315305 (2011).
[41] G. Kar, Hardy’s nonlocality for mixed states, Phys. Lett. A 228, 119 (1997).
[42] S. Goldstein, Nonlocality without inequalities for almost all entangled states for two particles, Phys. Rev. Lett. 72, 1951 (1994).
[43] T.F. Jordan, Testing Einstein-Podolsky-Rosen assumptions without inequalities with two photons or particles with spin 1/2, Phys. Rev. A 50, 62 (1994).
[44] Lluís Masanes, Asymptotic Violation of Bell Inequalities and Distillability, Phys. Rev. Lett. 97, 050503 (2006).
[45] Lluís Masanes, Extremal quantum correlations for N parties with two dichotomic observables per site, arXiv:quant-ph/0512100v1 (2005).
[46] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. 11, 045021 (2009).
[47] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, Phys. Rev. Lett. 108, 100402 (2012).
[48] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Bell Inequalities Tailored to Maximally Entangled States, Phys. Rev. Lett. 119, 040402 (2017).