Title	Beyond Gisin's theorem and its applications : violation of local realism by two-party Einstein-Podolsky-Rosen steering
Author(s)	Chen, Jing-Ling; Su, Hong-Yi; Xu, Zhen-Peng; Wu, Yu-Chun; Wu, Chunfeng; Ye, Xiang-Jun; ukowski, Marek; Kwek, Leong Chuan
Citation	Chen, J.-L., Su, H.-Y., Xu, Z.-P., Wu, Y.-C., Wu, C., Ye, X.-J., et al. (2015). Beyond Gisin's theorem and its applications : violation of local realism by two-party Einstein-Podolsky-Rosen steering. Scientific Reports, 5, 11624-.
Date	2015
URL	http://hdl.handle.net/10220/38338
Rights	This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

SCIENTIFIC REP♀RTS

Beyond Gisin's Theorem and its Applications: Violation of Local Realism by Two-Party Einstein-Podolsky-Rosen Steering

Jing-Ling Chen[1,2], Hong-Yi Su[1], Zhen-Peng Xu[1], Yu-Chun Wu[3,4], Chunfeng Wu[5], Xiang-Jun Ye[1], Marek Żukowski[6,7] & L. C. Kwek[2,8,9]

We demonstrate here that for a given mixed multi-qubit state if there are at least two observers for whom mutual Einstein-Podolsky-Rosen steering is possible, i.e. each observer is able to steer the other qubits into two different pure states by spontaneous collapses due to von Neumann type measurements on his/her qubit, then nonexistence of local realistic models is fully equivalent to quantum entanglement (this is not so without this condition). This result leads to an enhanced version of Gisin's theorem (originally: all pure entangled states violate local realism). Local realism is violated by all mixed states with the above steering property. The new class of states allows one e.g. to perform three party secret sharing with just pairs of entangled qubits, instead of three qubit entanglements (which are currently available with low fidelity). This significantly increases the feasibility of having high performance versions of such protocols. Finally, we discuss some possible applications.

Quantum mechanical correlations do not admit local realistic models. This pivotal result concerns the foundations of quantum mechanics (QM) and has many applications in quantum information theory. The states exhibiting quantum correlations can be grouped using the following hierarchy[1]: those that are entangled, those that allow for Einstein-Podolsky-Rosen (EPR) "steering", and those that violate local realism (LR)[2].

According to Erwin Schrödinger[3], quantum entanglement is "the characteristic trait of quantum mechanics" distinguishing it from any classical theory. This feature of quantum states is a highly useful resource in many fascinating applications of quantum information, such as teleportation[4,5], dense coding, communication protocols, and computation[6,7]. Moreover, states that violate local realism have gained ubiquitous applications in different quantum information tasks, such as quantum key distribution[8], communication complexity[9], quantum information processing and random number generation[10].

[1]Theoretical Physics Division, Chern Institute of Mathematics, Nankai University, Tianjin 300071, People's Republic of China. [2]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543. [3]Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, People's Republic of China. [4]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, Anhui, China. [5]Pillar of Engineering Product Development, Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372. [6]Institute of Theoretical Physics and Astrophysics, University of Gdańsk, PL-80-952 Gdańsk, Poland. [7]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, 230026 Hefei, China. [8]National Institute of Education,1 Nanyang Walk, Singapore 637616. [9]Institute of Advanced Studies, Nanyang Technological University, 60 Nanyang View, Singapore 639673. Correspondence and requests for materials should be addressed to J.L.C. (email: chenjl@nankai.edu.cn) or L.C.K. (email: cqtklc@nus.edu.sg)

In Schrödinger's reply to the EPR paper[11], he made a fine distinction between entangled states and states shared between two parties that are amenable for steering, i.e. in which the action of one party can affect the reduced state of the other party through the an appropriate choice of measurements. Also, in contrast to quantum entanglement which has received widespread interest due to its usefulness as a resource for tasks in quantum information processing, there have been relatively fewer developments in the notion of "steerable" states. In 2007, Wiseman *et al.*[1] revisited the issue and reformulate the idea of "steerable" state from a quantum information perspective. Since then, several interesting studies on EPR steering have appeared both in theory[12,13] and in experiments[14–18]. Recently, some of us have demonstrated an all-versus-nothing proof of EPR steering[19].

Quantum steering in a bipartite scenario essentially describes the ability of one party, say Alice, to prepare the other party's (Bob's) systems in different ensembles of quantum states by measuring her own particle (under more than two different settings). Naturally, Alice has no control over the actual result of her actions, but she is able to control over the set of projected states on Bob's side with her measurement for a given setting. If Bob does not trust Alice, Alice's manipulation of her system appears as a black box described by some local hidden variable (LHV) theory. This could imply a local hidden state (LHS) description of her actions: that is that she just simply sends some states to Bob according to some probability distribution. Quantum steering means that such a description is impossible and that Alice must use quantum measurements on her system to prepare states on Bob's side.

As pointed by Wiseman *et al.*[1], there is a hierarchical structure. For a given state, quantum steering is strictly implied by the violation of local realism. Simply put, steering excludes the possibility of local "hidden" state models of correlations, in which a quantum mechanical model is applied to only one of the systems, while the other one is described using a local hidden variable model. LHS model allows for a full LHV model for both (all) systems. Of course separable (mixed) states can be thought of as probabilistic distributions of hidden states for each party, and thus states with steering are a proper subset of entangled states, endowed with an additional potentially useful property.

The close connection between quantum entanglement and violation of local realism[20] can be traced back to Gisin's work, Ref. 21, in which he presented a theorem stating that any pure entangled state of two qubits violates a Bell-like inequality. The result was generalized in Refs. 22,23. Gisin's theorem for three qubits was shown numerically by Chen *et al.*[24] and analytically by Choudhary *et al.*[25]. In 2012, Yu *et al.*[26] provided a complete proof of Gisin's theorem for all entangled pure states. Within the hierarchical picture of the states exhibiting quantum correlations, Gisin's theorem says that violation of local realism and quantum entanglement are equivalent for all *pure* states.

Gisin's theorem applies only to pure states. The aim of this paper is to develop an "enhanced" version of Gisin's theorem that can apply also to some class of mixed states. We shall show that some form of EPR steering allows the Gisin's theorem to be applicable to a wider range of entangled states than just pure ones. As pure entangled states always allow steering, we have a direct broadening of the realm of validity of Gisin's theorem. Our result also provides a rigorous criterion for marking the borders between quantum entanglement, EPR steering and violation of local realism. This is a nontrivial problem since it is not easy to reduce a superset to a subset by imposing extra constraints.

Our result serves as a contribution to recent studies of general nonlocal theories which satisfy the non-signaling principle[27,28] (or its extensions[29]), asking the question under what conditions an entangled state does not violate local realism[30]. Other links are with studies of the role of quantum contextuality in violation of local realism like e.g. Ref. 31. In Methods, we prove two theorems regarding the EPR steerability. We also note that the original Gisin's theorem is a special case of Theorem 1. We note that our criterion for steerability of quantum states is useful in some applications. We then describe how our criterion for steerability of quantum states could be applied to the Third Man cryptographic protocol and we show how Theorem 2 can serve as a valuable resource in a quantum certificate authorization protocol.

Results

Enhanced Gisin's theorem. Gisin's original work starts with two qubits in a pure state. In the spirit of this, let us also start with the two-qubit case, for which we have the following theorem:

Theorem 1 *For a two-qubit entangled state, ϱ, shared between Alice and Bob, the state violates local realism if any party can steer the other party into two different pure states by performing on her/his qubit some orthogonal projective measurements $\left\{\mathcal{P}^0_{\vec{n}}, \mathcal{P}^1_{\vec{n}}\right\}$, where $\mathcal{P}^0_{\vec{n}} = |+\vec{n}\rangle\langle+\vec{n}|$, $\mathcal{P}^1_{\vec{n}} = |-\vec{n}\rangle\langle-\vec{n}|$ are projectors along the $\vec{n}$-direction.*

Note that in the theorem, the word "different" refers to the fact that the reduced states of one party (after the other performs the measurements) are different.

Proof. Take the spectral decomposition of two-qubit density matrix: $\varrho = \sum_{i=1}^4 \nu_i |\Psi_i\rangle\langle\Psi_i|$, the positive ν_i add up to one. For $|\Psi_i\rangle$, if Alice performs the orthogonal projective measurements on on her qubit given by $\left\{\mathcal{P}^0_{\vec{n}}, \mathcal{P}^1_{\vec{n}}\right\}$ along the $\vec{n}$-direction and is able in this way to steer Bob's qubit into two different states $|\chi_1\rangle$ and $|\chi_2\rangle$, then the state $|\Psi_i\rangle$ must be in the form

$$|\Psi_i\rangle = F_i |+\vec{n}\rangle |\chi_1\rangle + \sqrt{1 - F_i^2} e^{i\tau_i} |-\vec{n}\rangle |\chi_2\rangle, \tag{1}$$

with real F_i satisfying $0 < F_i < 1$. However, in the formula we have only two mutually orthogonal vectors $|+\overrightarrow{n}\rangle|\chi_1\rangle, |-\overrightarrow{n}\rangle|\chi_2\rangle$). This means that we can have only the two independent $|\Psi_i\rangle$ with the same steer$_i$ng property. Hence, the rank of ϱ is at most 2:

$$\varrho = \nu_1|\Psi_1\rangle\langle\Psi_1| + \nu_2|\Psi_2\rangle\langle\Psi_2|. \tag{2}$$

If also Bob with measurements on his qubit can steer Alice's qubit into two different pure states, this additionally constrains the form of the two pure states to

$$|\Psi_1\rangle = \cos\frac{\zeta}{2}|00\rangle + \sin\frac{\zeta}{2}e^{i\tau}|11\rangle, \tag{3}$$

$$|\Psi_2\rangle = \sin\frac{\zeta}{2}|00\rangle - \cos\frac{\zeta}{2}e^{i\tau}|11\rangle. \tag{4}$$

For a derivation see Methods

A mixture of the such states, with $\nu_1 \neq \nu_2$, always violates the Clauser-Horne-Shimony-Holt (CHSH) inequality. In quantum mechanics the correlation function is computed using $Q_{ij} = Q_{\overrightarrow{n}_{A_i}\overrightarrow{m}_{B_j}} = \text{tr}\left(\varrho\overrightarrow{\sigma}_{\overrightarrow{n}_{A_i}} \otimes \overrightarrow{\sigma}_{\overrightarrow{m}_{B_j}}\right)$, where $\overrightarrow{\sigma}_{\overrightarrow{n}_{A_i}} = \overrightarrow{n}_{A_i} \cdot \overrightarrow{\sigma}$, and $\overrightarrow{\sigma}$; is the Pauli matrix vector, whereas $\overrightarrow{n}_{A_i}$ is the i-th measuring direction of Alice. We shall use the spherical coordinates, so that $\overrightarrow{n}_{A_i} = (\sin\theta_{A_i}\cos\phi_{A_i}, \sin\theta_{A_i}\sin\phi_{A_i}, \cos\theta_{A_i})$; similarly for Bob. The local realistic CHSH constraint is that $\mathcal{I}_{\text{CHSH}} = \frac{1}{2}(Q_{11} + Q_{12} + Q_{21} - Q_{22}) \leq 1$. By putting $\phi_{A_1} = \phi_{B_1} = \phi_{B_2} = \theta_{A_1} = 0$, $\theta_{A_2} = \pi/2$, $\theta_{B_2} = -\theta_{B_1}$, $\phi_{A_2} = \tau$, we get $\mathcal{I}_{\text{CHSH}}^{\max} = \sqrt{1 + \mathcal{C}^2}$, where $\mathcal{C} = |V|\sin\zeta|$ is the degree of entanglement, and $V = \nu_1 - \nu_2$. Except at $\zeta = 0, \pi$ or $V = 0$, $\mathcal{C}$ is always non-vanishing, and the CHSH inequality is violated.

Note that other criterions for steerability, e.g., the steerable weight proposed in Ref. 32 as a measure to effectively quantify the EPR steering, could also be used to prove the theorem; however, developing a stricter steering criterion is beyond our aim of the present paper. Note also that, the original Gisin's theorem is a special case of Theorem 1. For example, take $\nu_1 = 1$. The state $|\Psi_1\rangle$, for $\zeta \neq 0$ or π, is a two-qubit pure state in its Schmidt decomposition, and its steerable weight equals 1. Moreover, when $\nu_1 = \nu_2 = 1/2$ (i.e., $V = 0$), the state becomes a separable state, that has a vanishing degree of entanglement and does not violate any Bell inequality.

For the general case of N qubits, we have the following theorem:

Theorem 2 *For an N-qubit entangled state shared by N observers $\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_N$, the state violates local realism if there exists at least two observers, each with the ability to steer the remaining $N-1$ qubits into two different pure states by performing on her/his qubit some orthogonal projective measurements.*

Note that as in **Theorem 1**, "different" refers to the fact that the reduced states of the remaining $N-1$ parties (after one observer, say $\mathcal{O}_k$, performs his measurements) are different.

Without any loss of generality, we assume that the first two observers have the ability to steer the remaining $N-1$ qubits. As such, the state ϱ is either (a) an arbitrary N-qubit entangled pure state or (b) a rank-2 density matrix as in (2) with

$$|\Psi_1\rangle = \cos\frac{\zeta}{2}|0_10_2\rangle \otimes |\chi_1\rangle + \sin\frac{\zeta}{2}e^{i\tau}|1_11_2\rangle \otimes |\chi_2\rangle, \tag{5}$$

$$|\Psi_2\rangle = \sin\frac{\zeta}{2}|0_10_2\rangle \otimes |\chi_1\rangle - \cos\frac{\zeta}{2}e^{i\tau}|1_11_2\rangle \otimes |\chi_2\rangle, \tag{6}$$

states for $\mathcal{O}_3, \cdots, \mathcal{O}_N$, and the relative phase τ can always be taken as zero.

The violation of local realism for Case (a) has been shown analytically in[25,26] with the use a generalized Hardy (see e.g. inequality[33–35]). To prove Case (b), it is convenient to consider first $N = 3$, before moving to $N \geq 4$. (See Methods for the rigorous proof).

Application 1: The Third Man cryptography. We have extended the class of states for which Gisin's Theorem holds. But are these new states endowed with properties that can be put to use in quantum information tasks, do they form a kind of new resource? Below we shall show that in specific cases they can reduce the number of entangled particles needed to perform a task. In our example for three partners this is The Third Man cryptography[36,37] or equivalently secret sharing[38]. The example is extendible to more partners.

Imagine that Charlie is sending the states of Theorem 1 to Alice and Bob. He randomly chooses whether to send $|\Psi_1\rangle$ or $|\Psi_2\rangle$, with probabilities ν_1 and ν_2, which are different but quite similar. To simplify the example, assume that both pure states are maximally entangled, that is $\zeta = \pi/2$. Alice and Bob are asked to perform randomly chosen measurements using local bases $\overrightarrow{x}$ and $\overrightarrow{y}$, and also in some auxiliary

bases in the *xy* planes, usually needed in the Ekert91 protocol[8]. But the trouble is that while one of the pure states gives perfectly correlated results when both measured in $\overrightarrow{x}$ direction, and anti-correlated results for measurements in directions $\overrightarrow{y}$, the other one gives perfect anti-correlations for $\overrightarrow{x}$ measurements and perfect correlations for $\overrightarrow{y}$'s (it is irrelevant for the argument for which of the states this is so). Thus only if Charlie sends them information about which state he sent in the given run, they can unscramble the key, out of their measurements in the identical local bases. Thus Charlie holds a key to their key. Without additional information provided by him Alice and Bob cannot form a usable key. This is the Third Man cryptography.

Of course, if Charlie sends information on the states to just Alice, she can transform her string of data into one which is a copy of the string of Bob, and she can also build a working key (this is a secret sharing version of the same protocol). Of course, all this is done under the standard Ekert91 protocol, Alice and Bob exchange information on measurements bases without revealing the results, etc. Note, that for high, say ν_1, with classical error correction methods Alice and Bob could be able to extract a key, but it will be short, with respect to the numbers of runs (copies of the state sent by Charlie). Only with the help of Charlie it can be of maximal possible length (half of the numbers of runs, if the protocol runs perfectly).

Previous versions of such protocol, see[36,37] or[38], required three qubit entangled GHZ states. The reader may quickly judge how difficult the step is from two-particle entanglement distribution to three-particle entanglement distribution by consulting the review[7]. Also the fidelity of photonic three-particle entangled states is currently still typically below 90%, while in the two-particle case it can be now well over 99%. Low fidelity leads to errors in the key distribution. Thus the scheme with steerable states has a clear advantage over the the original one with GHZ states.

There is one more advantage. By making measurements in the $\overrightarrow{z}$ directions, which are always perfectly correlated, Alice and Bob can check whether the mixed state received by them from Charlie (ϱ, that is the state before he reveals in which runs were $|\Psi_1\rangle$ or $|\Psi_2\rangle$) is indeed entangled (as it violates the CHSH inequality). Thus they can have an independent quality check of Charlie's distribution methods. This is impossible under GHZ stated based protocols.

Note that the protocol settings for Alice and Bob are $\overrightarrow{x}$ and $\overrightarrow{y}$. With settings in $\overrightarrow{x}$ and $\overrightarrow{y}$ Alice and Bob cannot violate the CHSH inequality with ϱ for which ν_1 and ν_2 are close. Using the Horodecki criterion for violations of the CHSH inequality[39], $\sum_{i,j=\overrightarrow{x},\overrightarrow{y}} Q_{ij}^2 > 1$, given here in the form derived in[40], one can easily establish that the threshold difference is $|\nu_1 - \nu_2| = 1/\sqrt{2}$. The correlations in these directions are very weak, thus they are indeed unable to extract a key with such measurements, and the Ekert91 protocol. Without Charlie's help they are helpless. Of course, the presented scheme can be modified in many ways.

Application 2: The quantum certificate authorization protocol.

The state ϱ we discussed in **Theorem 2** can serve as a valuable resource in quantum cryptography[41]. A good example is an application to quantum certificate authorization involving three parties, say, Alice, Bob and Charlie, against a lurking eavesdropper, Eve. Suppose Alice needs to send some private information to Bob through internet, and yet she is not sure if the receiving party is Bob. So Alice goes to the certificate authority, Charlie, who is trusted by Alice and capable of certifying Bob's identity. With Charlie's help, Alice is then able to share secret keys with Bob at a distance.

There are two goals to be achieved here. Specifically, Alice's private information (i) should be received by the true Bob (and not someone else who claims to be Bob) and (ii) should not be intercepted by Eve. This task can be classically realized through digital signatures and public-private keys. Given ϱ, we see that we are able to present a quantum analogue of this protocol (see also[42,43]). As shown in Fig. 1, upon Alice's request for identification of Bob, Charlie produces an ensemble of three-qubit states ϱ's and distributes the first qubit to Alice, the second qubit to Bob, and keeps the third qubit. Alice and Bob measure their qubits randomly along one of two directions: $\overrightarrow{z}$ or $\overrightarrow{x}$ (i.e., projections to $|0\rangle\langle0|$, $|1\rangle\langle1|$ or $|+\rangle\langle+|$, $|-\rangle\langle-|$); similarly Charlie also measures his qubit randomly by a projection to $|\chi_1\rangle\langle\chi_1|$ or $|\chi_2\rangle\langle\chi_2|$. Such a joint measurement can be repeated for, say, N times, where N is large enough. If the state shared by Alice and Bob is reliable, they should get the same results (cf. Eqs. (4) in the main text) for any measurement along $\overrightarrow{z}$.

In order to detect a possible Eve, Charlie randomly picks m runs from N as a subset and requests Alice and Bob to broadcast through a public channel their directions and results for these m runs. With their data at hand Charlie starts to do analysis in three steps: (i) keep joint measuring results for which Alice and Bob measured along the same direction, i.e., $\overrightarrow{z}_A \otimes \overrightarrow{z}_B$ and $\overrightarrow{x}_A \otimes \overrightarrow{x}_B$, and discard those for $\overrightarrow{x}_A \otimes \overrightarrow{z}_B$ and $\overrightarrow{z}_A \otimes \overrightarrow{x}_B$; (ii) keep joint measuring results for which Charlie measured along $|\chi_1\rangle (|\chi_2\rangle)$ when Alice and Bob obtained both "0" ("1") along $\overrightarrow{z}$; (iii) verify (a) whether Alice (Bob) can steer Bob (Alice) and Charlie into two pure states when measuring along $\overrightarrow{z}$, and (b) whether $V \sin \zeta \neq 0$.

Here (a) can be verified by examining whether Charlie's probability of obtaining $|\chi_1\rangle (|\chi_2\rangle)$ is always unity when Alice and Bob obtained both "0" ("1") along $\overrightarrow{z}$. For (b), the three-qubit state ϱ is entangled iff $V \sin \zeta \neq 0$. To realize the quantum certificate authorization protocol, Charlie can produce ϱ with nonorthogonal $|\chi_1\rangle$ and $|\chi_2\rangle$. The coincidence probability that Alice and Bob get the same result can be
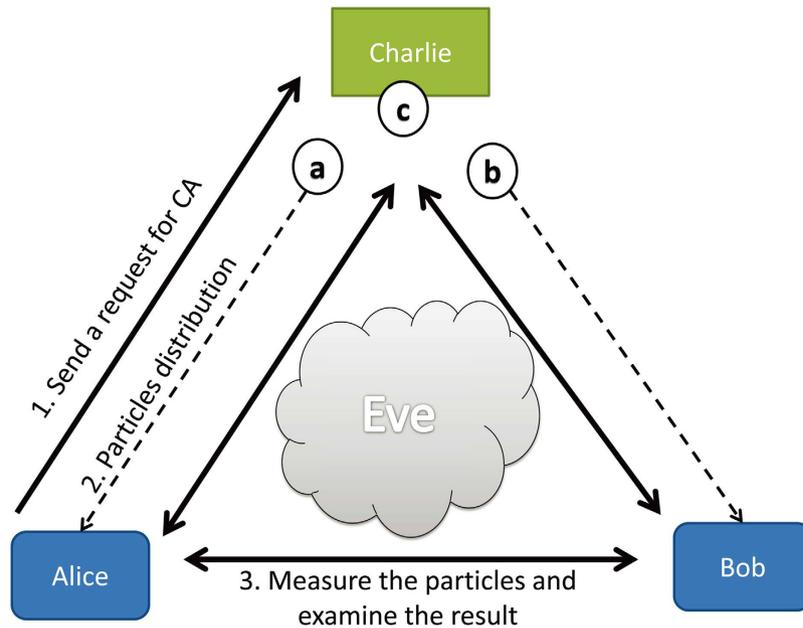
Figure 1. (Color online) The illustration of quantum certificate authorization protocol. Upon Alice's request for identification of Bob, Charlie produces a three-qubit state ϱ and then distributes the first qubit (represented as a ball labeled by "a", similarly for the others) to Alice , the second qubit "b" to Bob, and keeps the third qubit "c". To ensure the security, Charlie randomly measures his qubit along $|\chi_1\rangle$ or $|\chi_2\rangle$, Alice and Bob randomly measure their qubits along $\vec{z}$ or $\vec{x}$. Such a measurement can be repeated for large enough times. Finally Charlie performs a random inspection to see whether Alice and Bob are able to share secret keys at the quantum level that defy Eve's eavesdrop.

obtained as $\frac{1}{2}(1 + V \cos \phi \sin \zeta)$ when Alice and Bob measure along $\vec{x}$. To check whether ϱ is entangled is equivalent to check whether the coincidence probability is not equal to 1/2. In other words, result (a) ensures that both Alice and Bob can steer the remaining parties into two pure states; and if (a) is true, result (b) certifies that the state ϱ is entangled. Hence, if both (a) and (b) are fulfilled, then according to **Theorem 2** the state ϱ violates local realism, and the protocol is secure. Note that the secret keys are obtained from the unbroadcast part of results when Alice and Bob measure along $\vec{z}$.

Discussion

Our result sheds new light on the relation between entanglement of mixed states, and LHV models for correlations. It pinpoints a precisely defined class of states, which is strictly larger than all pure entangled states, and which has the property that just by the fact that a state belongs to the class, one knows that it violates local realism. The property is as follows: for an N-qubit state, there exist a pair of observers such that each of them singlehandedly can steer the remaining $N-1$ qubits of the other observers into two different pure states. Our results are for qubit systems. A generalization to more complicated ones is still an open question, and under investigation. Mixed states covered by the enhanced Gisin theorem, due to their specific properties, may allow new quantum protocols which allow to reduce the complication of entangled states involved in them (as in our example, we need, e.g., two-particle entangled states to have secret sharing between three parties). Other protocols, such as quantum certificate authorization, are also possible.

Methods

Proof of Eqs. (3) and (4). Without loss of generality, if Alice measures her qubit in the z-direction and if she steers Bob's qubit into two different pure states, then for the states (2) we have

$$|\Psi_1\rangle = \cos \frac{\zeta}{2}|00\rangle + \sin \frac{\zeta}{2}(\cos \beta e^{i\tau_1}|10\rangle + \sin \beta e^{i\tau_2}|11\rangle),$$

$$|\Psi_2\rangle = \sin \frac{\zeta}{2}|00\rangle - \cos \frac{\zeta}{2}(\cos \beta e^{i\tau_1}|10\rangle + \sin \beta e^{i\tau_2}|11\rangle).$$

However, if Bob measures his qubit along some specific direction, also Alice should be getting one of two steered states. We can denote Bob's projectors by $\{|\xi\rangle\langle\xi|, |\xi'\rangle\langle\xi'|\}$. The respective qubit basis states can be put as

$$|\xi\rangle = a|0\rangle + b|1\rangle, \quad |\xi'\rangle = b^*|0\rangle - a|1\rangle \tag{7}$$

with a real-valued, $b = \sqrt{1-a^2}e^{i\gamma}$. If the state of a qubit is pure, then the determinant of its density matrix is zero. If Bob measures his qubit of ϱ, given by (2), with the above projectors, the determinants of the steered states of Alice's qubit are

$$\mathrm{Det}\left[\rho_{|\xi\rangle}\right] = a^2\nu_1\nu_2\left|a\ \cos\ \beta + b\ \sin\ \beta e^{i(\tau_1-\tau_2)}\right|^2, \tag{8}$$

$$\mathrm{Det}\left[\rho_{|\xi'\rangle}\right] = |b|^2\nu_1\nu_2\left|b\ \cos\ \beta - a\ \sin\ \beta e^{i(\tau_1-\tau_2)}\right|^2. \tag{9}$$

We must find conditions for both of them to vanish. For the only interesting case of both ν_i greater than zero, we have to consider two situations. (i) Suppose $a=0$, then it is enough to have $|\cos\ \beta| = 0$. (ii) Suppose $a \neq 0$, then one has the conditions $|a\ \cos\ \beta + b\ \sin\ \beta e^{i(\tau_1-\tau_2)}| = 0$ and $|b|^2|b\ \cos\ \beta - a\ \sin\ \beta e^{i(\tau_1-\tau_2)}| = 0$. The only solution is $a=1$ (i.e., $|b| = 0$) and $|\cos\ \beta| = 0$. This directly leads to (3) and (4). For the general N qubits, one has a straight ahead extension of this reasoning leading to Eqs. (5) and (6).

Proof of Theorem 2 for $N=3$.   Take three observers Alice, Bob and Charlie. Assume that Alice and Bob have the ability to steer the remaining two qubits. Due to local unitary, one can always work with $|\chi_1\rangle_C = |0\rangle, |\chi_2\rangle_C = \cos\ \phi|0\rangle + \sin\ \phi|1\rangle$, and $\sin\ \frac{\zeta}{2}, \cos\ \frac{\zeta}{2}, \sin\phi, \cos\phi \geq 0$.

(i) Let us first consider the case where $\cos\phi \neq 0$. The three-qubit Hardy inequality is given by

$$\begin{aligned}\mathcal{I}_{\mathrm{Hardy}} = p(000|111) &- p(111|222) - p(000|112) \\ &- p(000|121) - p(000|211) \leq 0,\end{aligned} \tag{10}$$

where $p(abc|ijk)$ denotes the probability $p(A_i=a,\ B_j=b,\ C_k=c)$. Let the settings be $\theta_{A_1} = \theta_{B_1} = \theta_{C_1} = 0, \phi_{A_1} = \phi_{B_1} = \phi_{C_1} = 0, \theta_{C_2} = \pi, \phi_{C_2} = 0, \phi_{A_2} = \phi_{B_2} = \frac{\pi}{2}, \theta_{B_2} = \theta_{A_2}$, the quantum prediction then becomes

$$\begin{aligned}\mathcal{I}_{\mathrm{Hardy}}^{\mathrm{QM}} = \frac{\cos^4\frac{\theta_{A_2}}{2}}{2}\Bigg(&2V\ \sin\ \zeta\ \cos\ \phi\tan^2\frac{\theta_{A_2}}{2} \\ &- (1 + \cos^2\phi + V\ \cos\ \zeta\sin^2\phi)\Bigg).\end{aligned} \tag{11}$$

By taking

$$\tan^2\frac{\theta_{A_2}}{2} = \frac{(1 + \cos^2\ \phi + V\ \cos\ \zeta\ \sin^2\ \phi)}{V\ \sin\ \zeta\ \cos\ \phi}, \tag{12}$$

we finally have

$$\mathcal{I}_{\mathrm{Hardy}}^{\mathrm{QM}} = \frac{\cos^4\frac{\theta_{A_2}}{2}}{2}(1 + \cos^2\ \phi + V\ \cos\ \zeta\ \sin^2\ \phi) > 0. $$

(ii) If $\cos\phi = 0$, we employ the following Bell inequality:

$$\begin{aligned}\mathcal{I}_3 = \frac{1}{4}(Q_{111} &+ Q_{121} + Q_{211} + Q_{221} + Q_{110} \\ &+ Q_{120} + Q_{210} - 3Q_{220}) \leq 1,\end{aligned} \tag{13}$$

where Q_{ijk} are the qubit correlation functions defined in analogy to the two qubit ones (see above). The index 0 indicates that measurement performed on the corresponding qubit do not enter the function, and thus we have a two-qubit correlation function. By taking settings as $\phi_{A_1} = \phi_{B_1} = \phi_{C_1} = \phi_{A_2} = \phi_{B_2} = \phi_{C_2} = 0$, $\theta_{B_1} = \theta_{C_1} = \frac{\pi}{2}, \theta_{B_2} = \theta_{C_2} = \pi$, and $\theta_{A_2} = 0$, all correlation functions vanish except the following ones: $Q_{111} = V\ \sin\ \zeta\ \sin\ \theta_{A_1}, Q_{120} = -\cos\ \theta_{A_1}$, and $Q_{220} = -1$. The quantum prediction becomes

$$\mathcal{I}_3^{\mathrm{QM}} = 1 + \frac{\cos^2 \frac{\theta_{A_1}}{2}}{2} \left(V \sin \zeta \tan \frac{\theta_{A_1}}{2} - 1 \right).$$

Clearly, we have $\mathcal{I}_3^{\mathrm{QM}} > 1$ when $\tan \frac{\theta_{A_1}}{2} > \frac{1}{V \sin \zeta}$.

Proof of Theorem 2 for Cases $N \geq 4$. For $N \geq 4$, the states $|\chi_1\rangle$, $|\chi_2\rangle$ can be entangled. The proof can be split into two cases: (i) separable $|\chi_1\rangle$, $|\chi_2\rangle$, and (ii) at least one of them being entangled. To demonstrate violations of local realism, we employ an N-qubit Hardy inequality, together with some Bell inequalities devised by us particularly for the present paper.

The N-qubit Hardy inequality reads

$$\mathcal{I}_{\mathrm{Hardy}}^N = p(00\cdots0|11\cdots1) - p(11\cdots1|22\cdots2)$$
$$- \sum p(00\cdots0|\mathrm{Perm}[11\cdots12]) \leq 0 \qquad (14)$$

Here Perm[11 …12] is any permutation of indices between parties, and the summation is taken over all such permutations that are possible. We see that we have the following cases:

(i) One, or both, of $|\chi_1\rangle$, $|\chi_2\rangle$ is entangled. If $|\chi_1\rangle$ is entangled, one can use the following Bell inequality

$$p(0_1 0_2|1_1 1_2) \otimes \mathcal{I}_{\mathrm{Hardy}}^{N-2} \equiv p(0000\cdots0|1111\cdots1)$$
$$- p(0011\cdots1|1122\cdots2)$$
$$- \sum p(0000\cdots0|11\mathrm{Perm}[11\cdots12]) \leq 0 \qquad (15)$$

to detect violation of local realism. Here $\mathcal{I}_{\mathrm{Hardy}}^{N-2}$ is the $(N-2)$-qubit Hardy inequality for $\mathcal{O}_3$, $\mathcal{O}_4$, $\cdots$, $\mathcal{O}_N$. The validity of this inequality to test the violation of local realism of ϱ relies on the fact that when $\mathcal{O}_1$ and $\mathcal{O}_2$ measure their qubits respectively along the z-direction, these measurements are equivalent to a test for the violation of local realism of $|\chi_1\rangle$ using $\mathcal{I}_{\mathrm{Hardy}}^{N-2} \leq 0$. Also, if $|\chi_2\rangle$ is entangled, the violation of local realism is detected in similar manner.

(ii) None of the states $|\chi_1\rangle$, $|\chi_2\rangle$ is entangled. Up to LU, one can work with $|\chi_1\rangle = |0\ldots0\rangle$ and $|\chi_2\rangle = \otimes_{i=3}^N \left(f_i |0\rangle + g_i |1\rangle \right)$, where $f_i \geq 0$.

If the number of coefficients f_i that are equal to zero is $r \in \{0,1,\ldots\ldots,N-3\}$ (without loss of generality we have assumed that the first r coefficients are zero), then we use the following Bell inequality

$$p\left(0_1 0_2 \cdots 0_r | 1_1 1_2 \cdots 1_r\right) \otimes \mathcal{I}_{\mathrm{Hardy}}^{N-r} \leq 0 \qquad (16)$$

to test the violation of local realism. Let the settings be
$$\theta_{\mathcal{O}_j}^1 = \phi_{\mathcal{O}_j}^1 = 0, \quad \text{for } 1 \leq j \leq N,$$
$$\theta_{\mathcal{O}_j}^2 = \vartheta, \quad \phi_{\mathcal{O}_j}^2 = \frac{\pi}{2}, \quad \text{for } j = r+1, r+2,$$
$$\theta_{\mathcal{O}_j}^2 = \pi, \quad \phi_{\mathcal{O}_j}^2 = 0, \quad \text{for } r+3 \leq j \leq N,$$
then quantum mechanics demands

$$\mathcal{I}_{\mathrm{Hardy}}^{\mathrm{QM}} = \frac{\cos^4 \frac{\vartheta}{2}}{2^{r+1}} \left(2V \sin \zeta \left(\prod_{i=3+r}^N f_i \right) \tan^2 \frac{\vartheta}{2} - \left[1 + \left(\prod_{i=3+r}^N f_i \right)^2 + \left(1 - \left(\prod_{i=3+r}^N f_i \right)^2 \right) V \cos \zeta \right] \right).$$

Similar to Eq. (7) in the $N=3$ case in the main text and taking an appropriate value of ϑ, we always have $\mathcal{I}_{\mathrm{Hardy}}^{\mathrm{QM}} > 0$.

If all $f_i = 0$ (i.e., $r = N-2$), for an even N, the violation of local realism of the state ϱ is dictated by

$$\mathcal{I}^N = \frac{1}{2^{N-1}} \left(\sum_{i_1,i_2,\ldots,i_N=1}^2 Q_{i_1 i_2 \ldots i_N} \right) - Q_{22\ldots2} \leq 1, \qquad (17)$$

where correlation functions $Q_{i_1 i_2 \ldots i_N} = X_{1 i_1} X_{2 i_2} \cdots X_{N i_N}$, with $X_{k i_k} = \pm 1$, and i_k indicating settings for the k-th party. For $N=2$, the inequality (17) reduces to the CHSH inequality.

The classical bound is obtained as follows. The summation term in (17) is the binomial expansion of $\mathcal{Y} \equiv \frac{1}{2^{N-1}}(X_{11} + X_{12})(X_{21} + X_{22})\cdots(X_{N1} + X_{N2})$, which could take only three distinct values $\{-2, 0, 2\}$. The value of $Q_{22\ldots2}$ is closely related to $\mathcal{Y}$. Indeed, when $\mathcal{Y} = 2$, then $Q_{22\ldots2} = 1$ so that $\mathcal{I}^N = 1$; when $\mathcal{Y} = -2$, then $Q_{22\ldots2} = -1$ so that $\mathcal{I}^N = -1$; when $\mathcal{Y} = 0$, then $\mathcal{I}^N \leq 1$ since $Q_{22\ldots2}$ is no larger than 1. Hence, $\mathcal{I}^N \leq 1$ holds for any local theories.

In quantum mechanics, the correlation function is computed by $Q_{i_1 i_2 \ldots i_N} = \mathrm{tr}\left(\varrho \overrightarrow{\sigma}_{\overrightarrow{n}_{i_1}} \otimes \overrightarrow{\sigma}_{\overrightarrow{n}_{i_2}} \otimes \cdots \otimes \overrightarrow{\sigma}_{\overrightarrow{n}_{i_N}}\right)$, with $\overrightarrow{n}_{i_k} = \left(\sin\theta_{ki_k}\cos\phi_{ki_k},\ \sin\theta_{ki_k}\sin\phi_{ki_k},\ \cos\theta_{ki_k}\right)$. We explicitly have

$$Q_{i_1 i_2 \ldots i_N} = \cos\theta_{1i_1}\cos\theta_{2i_2}\cdots\cos\theta_{Ni_N}$$
$$+ V\sin\zeta\sin\theta_{1i_1}\sin\theta_{2i_2}\cdots\sin\theta_{Ni_N}$$
$$\times \cos\left(\phi_{1i_1} + \phi_{2i_2} + \cdots + \phi_{Ni_N}\right).$$

Taking the settings as $\phi_{1i_1} = \phi_{2i_2} = \cdots = \phi_{Ni_N} = 0$, $\theta_{N1} = \cdots = \theta_{21} = \pi - \theta_{11}$, $\theta_{N2} = \cdots = \theta_{22} = \pi - \theta_{12}$, and $\theta_{12} = \pi$, we get the quantum bound as

$$\mathcal{I}^N_{\mathrm{QM}} = \frac{1}{2^{N-1}}[2^{N-1} + V\sin\zeta\sin^N\theta_{11} - (1 - \cos\theta_{11})^N]$$
$$= 1 + \frac{V\sin\zeta\sin^N\theta_{11}}{2^{N-1}}\left(1 - \frac{\tan^N\frac{\theta_{11}}{2}}{V\sin\zeta}\right).$$

Clearly, we have $\mathcal{I}^N_{\mathrm{QM}} > 1$ when $\tan\frac{\theta_{11}}{2} < (V\sin\zeta)^{1/N}$.

For odd N, violation of local realism of the state ϱ is identified by

$$\mathcal{I}^N = \frac{1}{2^{N-1}}\left(\sum_{i_1,\ldots,i_{N-1}=1}^{2}\sum_{i_N=0}^{1} Q_{i_1 i_2 \ldots i_N}\right) - Q_{22\ldots20} \leq 1, \tag{18}$$

where $i_N = 0$ indicates that no measurement is performed on the N-th qubit. Quantum mechanically, we explicitly have

$$Q_{i_1 i_2 \ldots i_N} = V\cos\zeta\cos\theta_{1i_1}\cos\theta_{2i_2}\cdots\cos\theta_{Ni_N}$$
$$+ V\sin\zeta\sin\theta_{1i_1}\sin\theta_{2i_2}\cdots\sin\theta_{Ni_N}$$
$$\times \cos\left(\phi_{1i_1} + \phi_{2i_2} + \cdots + \phi_{Ni_N}\right),$$

and, $Q_{i_1 i_2 \ldots i_{N-1} 0} = \cos\theta_{1i_1}\cos\theta_{2i_2}\cdots\cos\theta_{Ni_N}$. By taking settings as $\phi_{1i_1} = \phi_{2i_2} = \cdots = \phi_{Ni_N} = 0$, $\theta_{ni_n} = \frac{\pi}{2}\times i_n$, $(n \neq 1)$, and $\theta_{12} = 0$, all correlation functions vanish except the following ones: $Q_{111\ldots11} = V\sin\zeta\sin\theta_{11}$, $Q_{122\ldots20} = -\cos\theta_{11}$, and $Q_{222\ldots20} = -1$. Hence, the quantum prediction of $\mathcal{I}^N$ in (18) is

$$\mathcal{I}^{\mathrm{QM}}_N = 1 + \frac{\cos^2\frac{\theta_{11}}{2}}{2^{N-2}}\left(V\sin\zeta\tan\frac{\theta_{11}}{2} - 1\right).$$

Clearly, we have $\mathcal{I}^{\mathrm{QM}}_N > 1$ when $\tan\frac{\theta_{11}}{2} > \frac{1}{V\sin\zeta}$, proving Theorem 2.

References
1. Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98,** 140402 (2007).
2. Bell, J. S. On the einstein podolsky rosen paradox. *Physics* (NY) **1,** 195–200 (1964).
3. Schrödinger, E. Discussion of probability relations between separated systems. *Proc. Cambridge Philos. Soc.* **31,** 555–563 (1935).
4. Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69,** 2881 (1992).
5. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895 (1993).
6. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000) pp. 20.
7. Pan, J.-W. *et al.* Multiphoton entanglement and interferometry. *Rev. Mod. Phys.* **84,** 777 (2012).
8. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661 (1991).
9. Brukner, Č., Żukowski, M., Pan, J.-W. & Zeilinger, A. Bell's Inequalities and Quantum Communication Complexity. *Phys. Rev. Lett.* **92,** 127901 (2004).
10. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* (London) **464,** 1021–1024 (2010).

11. Einstein, A., Podolsky, B. & Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47,** 777 (1935).
12. Oppenheim, J. & Wehner, S. The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics. *Science* **330,** 1072 (2010).
13. Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85,** 010301(R) (2012).
14. Saunders, D. J., Jones, S. J., Wiseman, H. M. & Pryde, G. J. Experimental EPR-steering using Bell-local states. *Nature Phys.* **6,** 845–849 (2010).
15. Smith, D. H. *et al.* Conclusive quantum steering with superconducting transition edge sensors. *Nature Commun.* **3,** 625 (2012).
16. Bennet, A. J. *et al.* Arbitrarily Loss-Tolerant Einstein-Podolsky-Rosen Steering Allowing a Demonstration over 1 km of Optical Fiber with No Detection Loophole. *Phys. Rev. X* **2,** 031003 (2012).
17. Wittmann, B. *et al.* Loophole-free quantum steering. *New J. Phys.* **14,** 053030 (2012).
18. Händchen, V. *et al.* Observation of one-way Einstein-Podolsky-Rosen steering. *Nature Photonics* **6,** 596 (2012).
19. Chen, J. L. *et al.* All-Versus-Nothing Proof of Einstein-Podolsky-Rosen Steering. *Sci. Rep.* **3,** 2143 (2013).
20. Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40,** 4277 (1989).
21. Gisin, N. Bell's inequality holds for all non-product states. *Phys. Lett. A* **154,** 201 (1991).
22. Popescu, S. & Rohrlich, D. Generic quantum nonlocality. *Phys. Lett. A* **166,** 293–297 (1992).
23. Gisin, N. & Peres, A. Maximal violation of Bell's inequality for arbitrarily large spin. *Phys. Lett. A* **162,** 15 (1992).
24. Chen, J. L., Wu, C. F., Kwek, L. C. & Oh, C. H. Gisin's Theorem for Three Qubits. *Phys. Rev. Lett.* **93,** 140407 (2004).
25. Choudhary, S. K., Ghosh, S., Kar, G. & Rahaman, R. Analytical proof of Gisin's theorem for three qubits. *Phys. Rev. A* **81,** 042107 (2010).
26. Yu, S., Chen, Q., Zhang, C., Lai, C. H. & Oh, C. H. All Entangled Pure States Violate a Single Bell's Inequality. *Phys. Rev. Lett.* **109,** 120402 (2012).
27. Popescu, S. & Rohrlich, D. Nonlocality as an axiom. *Found. Phys.* **24,** 379 (1994).
28. Masanes, Ll., Acín, A. & Gisin, N. General properties of nonsignaling theories. *Phys. Rev. A* **73,** 012112 (2006).
29. Fritz, T. *et al.* Local orthogonality as a multipartite principle for quantum correlations. *Nature Commun.* **4,** 2263 (2013).
30. Acín, A., Gisin, N. & Toner, B. Grothendieck's constant and local models for noisy entangled quantum states. *Phys. Rev. A* **73,** 062105 (2006).
31. Cabello, A. Proposal for Revealing Quantum Nonlocality via Local Contextuality. *Phys. Rev. Lett.* **104,** 220401 (2010).
32. Skrzypczyk, P., Navascués, M. & Cavalcanti, D. Quantifying Einstein-Podolsky-Rosen Steering. *Phys. Rev. Lett.* **112,** 180404 (2014).
33. Wu, X.-H. & Xie, R.-H. Proposal for Revealing Quantum Nonlocality via Local Contextuality. *Phys. Lett. A* **211,** 129 (1996).
34. Ghosh, S., Kar, G. & Sarkar, D. Hardy's nonlocality for entangled states of three spin-1/2 particles. *Phys. Lett. A* **243,** 249 (1998).
35. Cereceda, J. L. Hardy's nonlocality for generalized n-particle GHZ states. *Phys. Lett. A* **327,** 433 (2004).
36. Żukowski, M., Zeilinger, A., Horne, M. A. & Weinfurter, H. Quest for GHZ states. *Acta Phys. Pol. A* **93,** 187 (1998).
37. Chen, Y.-A. *et al.* Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography. *Phys. Rev. Lett.* **95,** 200502 (2005).
38. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59,** 1829 (1999).
39. Horodecki, R., Horodecki, P. & Horodecki, M. Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition. *Phys. Lett. A* **200,** 340 (1995).
40. Żukowski, M. & Brukner, Č. Bell's Theorem for General N-Qubit States. *Phys. Rev. Lett.* **88,** 210401 (2002).
41. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301 (2009).
42. Akshata Shenoy, H., Srikanth, R. & Srinivas, T. Counterfactual quantum certificate authorization. *Phys. Rev. A.* **89,** 052307 (2014).
43. Srinatha, N., Omkar, S., Srikanth, R., Banerjee, S. & Pathak, A. The quantum cryptographic switch. *Quantum Inf. Process* **13,** 59 (2014).

Acknowledgements

Author Contributions

J.L.C. initiated the idea. J.L.C., H.Y.S., Z.P.X., Y.C.W. and C.W. established the proof of the theorems. J.L.C., H.Y.S., C.W., M.Z. and L.C.K. wrote the main manuscript text. X.J.Y. prepared figure. All authors reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Chen, J.-L. *et al.* Beyond Gisin's Theorem and its Applications: Violation of Local Realism by Two-Party Einstein-Podolsky-Rosen Steering. *Sci. Rep.* **5**, 11624; doi: 10.1038/srep11624 (2015).