EPR-steering: closing the detection loophole with non-maximally entangled states and arbitrary low efficiency.

Giuseppe Vallone

Department of Information Engineering, University of Padova, via Gradenigo 6/B, I-35131, Padova

(ΩDated: May 2, 2014)

Quantum steering inequalities allow to demonstrate the presence of entanglement between two parties when one of the two measurement device is not trusted. In this paper we show that quantum steering can be demonstrated for arbitrary low detection efficiency by using two-qubit non-maximally entangled states. Our result can have important applications in one-sided device-independent quantum key distribution.

PACS numbers: 03.65.Ud

Introduction - Entanglement is the most peculiar feature of quantum mechanics and its detection represent an important task in quantum information. In order to detect entanglement between two parties (called Alice and Bob) it is possible to use the entanglement witness method [1–4], allowing to verify the presence of entanglement when both Alice and Bob devices are know and trusted (and they also known the dimension of the quantum state they share). They can measure an entanglement witness operator $W$ of the shared state. They can prove that the shared state is entangled. If their measuring outputs violate some Bell inequality [5–7] is equivalent to the detection of entanglement between Alice and Bob with untrusted devices. In this scenario, Alice and Bob don’t know how their measuring device work and they don’t know what is the state they share: however, if a particular combination of their measurement outputs violate some Bell inequality they can prove that the shared state is entangled. If the Bell inequality is violated no local hidden variable (LHV) model can explain the correlation. Formally, a LHV model is written as:

$$P(a, b|A_k, B_j) = \sum_\lambda p_\lambda A_k(\lambda) B_j(\lambda) \quad \text{(LHV model)} \quad (2)$$

In the rhs of equation (2) $\lambda$ is the hidden variable with probability $p_\lambda$ and $A_k(\lambda)$ and $B_j(\lambda)$ are the so called response function depending on $\lambda$ and taking values on the possible measurement outcomes. The possibility of revealing entanglement with untrusted measuring device has important consequences for the so called device-independent (DI) secure Quantum Key Distribution (QKD) [8–10]. Alice and Bob can establish a secret key even if the shared state and their measuring device where provided by an evestopper.

EPR-Steering inequalities lie in between Entanglement witness and Bell inequality: they allows to demonstrate entanglement when only one of the two measuring device is trusted [11]. Steering has attracted a lot of attention in the last years [12–15]. Let’s consider the case of trusted Bob’s device. If a steering inequality is violated, the shared stated cannot be written as a Local Hidden State (LHS) model:

$$P(a, b|A_k, B_j) = \sum_\lambda p_\lambda A_k(\lambda) \text{Tr}[\Pi^A_k \rho_B^\lambda] \quad \text{(LHS model)} \quad (3)$$

As noticed in [19], steering is also relevant for QKD: precisely, violating an EPR-steering inequality allow to demonstrate the security in one-sided DI secure QKD, in which Bob’s detection device is trusted while Alice’s apparatus is not.

In order to experimentally violate a Bell or steering inequality, it is crucial to close the so called loopholes: the locality [20] and freedom-of-choice [21] loopholes are not important in the framework of cryptography, because it is a necessary assumption of security that Alice’s and Bob’s laboratory have no information leakage. The most crucial loophole is the so called detection loophole: due to the low detection efficiency of typical two photon experiments, the inequality is calculated by using the additional assumption of fair sampling. Without fair sampling, at least 83% efficiency is required to violate the CHSH inequality [6] with maximally entangled state, while for a large class of two-party Bell inequalities the threshold detection efficiency can be lowered by using non maximally entangled state [22, 23].

In this paper we show that a steering inequality equivalent to the one introduced in [24, 25] and experimentally violated by using the fair-sampling assumption in [23] can be violated with arbitrary detection efficiency by us-
ing non-maximally entangled states (NMES). Note that in [15] a loophole-free steering was demonstrated by using an inequality requiring at least 33\% efficiency, while arbitrary loss tolerant inequality were proposed (and violated) in [16]: however, the latter inequalities require that Alice declare when she detect a photon (or equivalently when she can "steer" Bob's state) and cannot be applied when Alice's device is not allowed to give null result.

Rewriting the Steering inequality - Let's consider the particular case in which Bob subsystem is a qubit and the Alice measurement devices have two outputs, namely +1 and −1. Alice and Bob can respectively choose between \(n\) different measurements \(A_k\) and \(\sigma_{b_k}\), where \(\sigma_{b_k} \equiv \vec{b}_k \vec{\sigma}\), \(\vec{\sigma} = \{\sigma_1, \sigma_2, \sigma_3\}\) are the Pauli matrices and the \(\vec{b}_k\)'s are three-dimensional unit length vectors. We consider the situation in which the Alice measurement device cannot give null result: when Alice chooses a measurement the device is answering with +1 or −1. The inequality introduced in [24, 25] is written as

\[
S_n = \frac{1}{n} \sum_{k=1}^{n} \langle A_k \otimes \sigma_{b_k} \rangle \leq C_n, \quad (4)
\]

with \(S_n\) the steering parameter. If the correlation between Alice and Bob can be described by LHS model, the value of \(S_n\) is bounded by \(C_n = \frac{1}{2} \max(A_k) \lambda(\sum_k A_k \sigma_{b_k})\), where \(\lambda(O)\) is the maximum eigenvalues of the operator \(O\) and \(A_k = \pm 1\) (see [25]). The corresponding pure state eigenvectors can be used as \(\vec{\rho}_B\) in the LHS model to saturate the bound in (4).

Note that \(C_n\) depends on the choice of observables made by Bob. For low \(n\) values, if the \(\pm \vec{b}_k\) are chosen as the vertex of platonic solid, the square for \(n = 2\), the octahedron for \(n = 3\), the icosahedron for \(n = 6\) and the dodecahedron for \(n = 10\), the \(C_n\) values take the following values [25]:

\[
\begin{align*}
C_2 &= \frac{1}{\sqrt{2}}, & C_3 &= \frac{1}{\sqrt{3}}, & C_6 &= \frac{1 + \sqrt{5}}{6}, \\
C_{10} &= \frac{3 + \sqrt{5}}{10}, & & C_{n \to \infty} &= \frac{1}{2}.
\end{align*}
\]

With \(n = 4\) measurements it was shown in [25] that a bound of \(\frac{1}{\sqrt{3}}\) can be achieved if the \(\vec{b}_k\) are chosen as the vertex of a cube. However, it is possible to find a better choice of the measuring vectors: take \(\vec{b}_1 = (0, 0, 1)\), and choose the other three vector as \(\vec{b}_k = (\sin \beta_0 \cos \phi_k, \sin \beta_0 \sin \phi_k, \cos \beta_0)\) with \(\cos \beta_0 = \frac{\sqrt{6} - 1}{2}\) and \(\phi_2 = 0, \phi_3 = 2\pi/3, \phi_4 = 4\pi/3\). The same strategy can be applied with 5 measurements (with the same \(\beta_0\) and \(\phi_2 = 0\), \(\phi_3 = \pi/2\), \(\phi_4 = \pi\), \(\phi_5 = 3\pi/2\)). In figure [1] we show the directions of the measurements as the vertices of the solid figures. With these settings we obtain:

\[
C_4 = \frac{1 + \sqrt{13}}{8} < \frac{1}{\sqrt{3}}, \quad C_5 = \frac{1 + 2\sqrt{13}}{15}. \quad (6)
\]

Note than the \(C_n\) series is a decreasing series converging toward \(\frac{1}{2}\). For any choice of Bob observables, the inequality (4) can be violated by using a two qubit maximally entangled singlet state when Alice chooses the measurement \(A_k = \hat{a}_k \vec{\sigma}\) with \(\hat{a}_k = -\vec{b}_k\); in this case \(S_n = 1\).

From the inequality (4) we can derive a simpler inequality involving only one output on the Alice and Bob side. To do so it is sufficient to notice that the single qubit observables can be written as \(\sigma_{b_k} = 2\Pi_k^B - \mathbb{1}\) where \(\Pi_k^B\) is the projection operator on the +1 eigenstate of \(\sigma_{b_k}\). Since Alice apparatus always produces an output, we have \(P(1, b|A_k, B_j) - P(-1, b|A_k, B_j) = 2P(1, b|A_k, B_j) - 1\). Then the correlation term \(\langle A_k \sigma_{b_k} \rangle\) can be rewritten as \(4P(1, 1|A_k, \Pi_k^B) - 2P(1, 1|A_k) - 2P_B(1|\Pi_k^B) - 1\). Since only +1 outcomes are involved in both Alice and Bob side, we simplify the notation as \(\langle A_k \sigma_{b_k} \rangle = 4P(A_k, \Pi_k^B) - 2P(A_k) - 2P(\Pi_k^B) + 1\). The inequality (4) can be rewritten as

\[
S_n' = \frac{1}{n} \sum_{k=1}^{n} [2P(A_k, \Pi_k^B) - P(A_k) - P(\Pi_k^B)] \leq C'_n, \quad (7)
\]

with \(C'_n = \frac{C_{n-1}}{2}\). The relation between the previous inequality and (4) is the same that holds between the Clauser-Horne (CH) [7] and the CHSH [5] inequality: while in (4) correlations between two-output measurements are involved, the new inequality (7) involves only terms containing +1 outputs. Since the Bob measuring device is trusted his measurement can be described by a well characterized quantum observable and it is possible to consider only the events in which Bob obtains a non-null result (+1 or -1) [16]. Moreover, Alice apparatus can be simplified to have only the +1 output (in fact losses are equivalent to -1 output in the inequality (7)).

Let's now suppose that an honest Alice want to convince Bob about her ability to steer his state by us-
ing a two-qubit entangled state $\rho_{AB}$ with reduced states $\rho_A = \text{Tr}_B[\rho_{AB}]$ and $\rho_B = \text{Tr}_A[\rho_{AB}]$. Unfortunately Alice has an inefficient measuring device with $\eta$ efficiency. Alice use the projectors $\Pi_k^\rho$ as measurement. In this case $p(A_k, \Pi_k^\rho) = \eta \text{Tr}_B[\Pi_k^\rho \otimes \Pi_k^\rho \rho_{AB}]$, $p(A_k) = \eta \text{Tr}_A[\Pi_k^\rho \rho_A]$ and $p(\Pi_k^\rho) = \text{Tr}_B[\Pi_k^\rho \rho_B]$. Alice is able to demonstrate steering only if her efficiency satisfy $\eta > \eta_c^{(n)}$ with the critical efficiency given by

\[
\eta_c^{(n)} = \frac{C_n + \frac{1}{n} \sum_{k=1}^n \text{Tr}_B[\Pi_k^\rho \rho_B]}{\frac{1}{n} \sum_{k=1}^n (2 \text{Tr}_B[\Pi_k^\rho \rho_{AB}] - \text{Tr}_A[\rho_A])}
\]

(8)

\[
= \frac{C_n + \frac{1}{n} \sum_{k=1}^n (\tilde{b}_k \sigma)_{\rho_B}}{\frac{1}{n} \sum_{k=1}^n [\tilde{a}_k \sigma \otimes \tilde{b}_k \sigma]_{\rho_{AB}} + (\tilde{b}_k \sigma)_{\rho_B}},
\]

(9)

where $\rho_B$ is the reduced state on Bob side. By using maximally entangled state the best critical efficiency is given by

\[
\eta_c^{(n)} = C_n \quad \text{(for maximal entangled states)}
\]

(10)

In fact for maximally entangled state we have $\rho_B = \frac{1}{2} |01\rangle \langle 01| + \frac{1}{2} |10\rangle \langle 10|$ and we get $\langle \tilde{b}_k \sigma \rangle_{\rho_B} = 0 \forall \tilde{b}_k$. Moreover, by carefully choosing the $\tilde{a}_k$'s it is possible to obtain $\langle \tilde{a}_k \sigma \otimes \tilde{b}_k \sigma \rangle_{\rho_{AB}} = 1 \forall k$ and the best $\eta_c^{(n)}$ is equal to $C_n$.

Reducing $\eta_c$ with NMES - We now demonstrate that by using non-maximally entangled state the critical efficiency can be lowered. Let’s consider the following non-maximally entangled state:

\[
|\psi\rangle = \cos \frac{\theta}{2} |01\rangle - \sin \frac{\theta}{2} |10\rangle,
\]

(11)

and define the measuring projector as $\Pi_k^\rho = |a_k\rangle \langle a_k|$ and $\Pi_k^\rho = |b_k\rangle \langle b_k|$ with

\[
|a_k\rangle = \sin \frac{\alpha_k}{2} |0\rangle - e^{i\varphi_k} \cos \frac{\alpha_k}{2} |1\rangle,
\]

\[
|b_k\rangle = \cos \frac{\beta_k}{2} |0\rangle + e^{i\varphi_k} \sin \frac{\beta_k}{2} |1\rangle.
\]

(12)

with $0 \leq \varphi_k \leq 2\pi$, $0 \leq \varphi_k \leq 2\pi$ and $0 \leq \alpha_k \leq \pi$. The parameter $0 \leq \theta \leq \pi/2$ is an entanglement monotone [4] and can be related to the content of entanglement of the state $|\psi\rangle$. In equation (11) only the denominator depends on the $a_k$'s. It is maximized (and then $\eta_c$ is minimized) when the $a_k$'s are chosen such that:

\[
\tan \alpha_k = \sin \theta \tan \beta_k, \quad \varphi_k = \varphi_k.
\]

(13)

The efficiency $\eta_c$ is finally minimized by the following procedure: choose the $\tilde{b}_k$ such that the eigenvalues of the operator $\frac{1}{n} \sum_k \tilde{b}_k \sigma$ are precisely $\pm C_n$ and the $-C_n$ eigenvector is the state $|1\rangle$. By this choice we get $\frac{1}{n} \sum_{k=1}^n (\tilde{b}_k \sigma)_{\rho_B} = -C_n \cos \theta$. The remaining term $\frac{1}{n} \sum_{k=1}^n (\tilde{a}_k \sigma \otimes \tilde{b}_k \sigma)_{\rho_{AB}}$ in (9) can be calculated by means of [13]. For instance, the obtained values for $n = 2$ and $n = 3$ are $\eta_c^{(2)}(\theta) = \frac{1 - \cos \theta}{\sqrt{1 + \sin^2 \theta - \cos \theta}}$ and $\eta_c^{(3)}(\theta) = \frac{1 - \cos \theta}{\sqrt{1 + 2 \sin^2 \theta - \cos \theta}}$. In the $\eta \to \infty$ limit we should replace the sum $\frac{1}{\theta} \sum_{k=1}^n$ with the integral $\frac{1}{\pi \theta} \int_0^{\pi \theta} d \theta$ by considering an infinite number of $\tilde{b}_k$ vector with positive z component. In this case we obtained $\eta_c^{(\infty)} = 1/\theta + 1/\theta \sin \theta \arccos \theta$.

We report in figure 2 the values of the critical efficiencies $\eta_c^{(n)}$ as a function of $n$ for $n = 2, 3, 4, 5, 6$ and $\infty$ setting scenario. We notice that, for the maximally entangled state $\theta = \pi/2$, we get the expected result of $\eta_c^{(n)} = C_n$. We define $\bar{\eta}_c^{(n)}$ the limit of zero entanglement, namely $\bar{\eta}_c^{(n)} \equiv \lim_{\theta \to 0} \eta_c^{(n)}(\theta)$. It is worth noting that $\bar{\eta}_c^{(n)}$ is always lower than $\bar{\eta}_c^{(n)}$ and an arbitrary low value can be obtained by increasing the number $n$ of observables. In fact we have $\bar{\eta}_c^{(2)} = \frac{1}{2}$, $\bar{\eta}_c^{(3)} = \frac{1}{3}$, $\bar{\eta}_c^{(4)} \simeq 0.291$, $\bar{\eta}_c^{(5)} \simeq 0.268$, $\bar{\eta}_c^{(6)} \simeq 0.266$, $\bar{\eta}_c^{(\infty)} = 0$.

We can also calculate how the critical efficiency changes if the NMES is noisy. Here we consider a colored noise model, in which the shared state is given by

\[
\rho = (1 - \epsilon)|\psi\rangle \langle \psi| + \epsilon \rho_{\text{noise}}\]

\[
\rho_{\text{noise}} = \cos^2 \frac{\theta}{2} |01\rangle \langle 01| + \sin^2 \frac{\theta}{2} |10\rangle \langle 10|
\]

(14)

There are two main reasons to consider colored and not white (corresponding to $\rho_{\text{noise}} = \frac{1}{2} I$) noise: first of all, when the entangled state (11) is experimentally generated, for example by spontaneous parametric down conversion, the main source of imperfection comes from the difficulty of producing $|01\rangle$ and $|10\rangle$ perfectly indistinguishable: this introduces a decoherence precisely corresponding to our colored noise model. Moreover, the white noise will require higher efficiency since the advantage of using NMES comes from the "polarization" of single qubit reduced states $\rho_A$ and $\rho_B$, while white noise is completely "depolarized". On the other side, in the colored noise model, the reduced states $\rho_A$ and
most common noise present in actual experiments. For example, with 10% noise, the inequality can be violated by using 6 measurements and detection efficiency larger than 31.14%. Our result can have important application in quantum cryptography due to the recent connection between steering and cryptography [19]. This could be particular relevant for long distance quantum communication with high losses [26], in which the trusted device is located at distance with respect to the entanglement source while the untrusted device is placed close to the source to achieve the required efficiency needed to violate a steering inequality.

We thanks P. Villoresi for useful discussions. This work has been carried out within the Strategic Project QUINTET of the Department of Information Engineering, University of Padova and the Strategic-Research-Project QuantumFuture of the University of Padova.

[1] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A 223, 1 (1996).
[2] B. M. Terhal, Phys. Lett. A 271, 319 (2000).
[3] G. Tóth and O. Gühne, Physical Review Letters 94, 60501 (2005).
[4] R. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).
[5] J. S. Bell, Physics 1, 195 (1964).
[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
[7] J. F. Clauser and M. A. Horne, Phys. Rev. D 10, 526 (1974).
[8] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
[9] L. Masanes, S. Pironio, and A. Acín, Nat. Comm. 2, 238 (2011).
[10] M. Lucamarini, G. Vallone, I. Giannani, P. Mataloni, and G. Di Giuseppe, Physical Review A 86, 032325 (2012).
[11] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. 98, 140402 (2007).
[12] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A 76, 052116 (2007).
[13] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. 106, 130402 (2011).
[14] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, Nat. Comm. 3, 625 (2012).
[15] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, New Journal of Physics 14, 053030 (2012).
[16] A. J. Bennett, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, Phys. Rev. X 2, 031003 (2012).
[17] V. Händchen, T. Eberle, S. Steinlechner, A. Sambowski, T. Franz, R. F. Werner, and R. Schnabel, Nature Photonics 6, 598 (2012).
[18] J.-I. Chen, X.-J. Ye, C. Wu, H.-Y. Su, A. Cabello, L. C. Kwek, and C. H. Oh, arXiv:1204.1870.
[19] C. Branciard, E. C. Cavalcanti, S. P. Walborn,
[20] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. 81, 5039 (1998).

[21] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger, PNAS 107, 19708 (2010).

[22] P. H. Eberhard, Phys. Rev. A 47, R747 (1993).

[23] G. Vallone, G. Lima, E. S. Gómez, G. Cañas, J. A. Larsson, P. Mataloni, and A. Cabello, preprint (2011). arXiv:1106.2240.

[24] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A 80, 032112 (2009).

[25] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nature Physics 6, 845 (2010).

[26] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, New Journal of Physics 10, 033038 (2008).