MDI-EWs: demonstrating arbitrarily weak entanglement using untrusted measurement devices

Denis Rosset[1] * Cyril Branciard[2] † Yeong-Cherng Liang[1] ‡ Nicolas Gisin[1] §

[1] *Group of Applied Physics, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland*
[2] *School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia*

Abstract. We introduce in this talk Measurement-Device-Independent Entanglement Witnesses, which can be used to demonstrate entanglement in all entangled states using untrusted measurement devices. MDI-EWs provide a middle ground between conventional entanglement witnesses (which require well-characterized measurement devices) and the violation of Bell inequalities (which does not require calibrated measurement devices but which can only witness a strict subset of entangled states). We provide examples of MDI-EWs that are loss-tolerant and can be implemented with current technology. Moreover, the violation of an MDI-EW cannot be simulated using classical communication, however large, thus providing a signature of quantumness in a physical system.

Keywords: Entanglement, Quantum nonlocality, Quantum state certification, Quantum communication, Quantum tomography

The demonstration of the entangled nature of quantum states is a crucial question, because of the central role of entanglement in quantum information processing. Different methods are available to witness the presence of entanglement in a physical system, such as conventional entanglement witnesses, quantum tomography, Bell inequalities or device-independent witnesses.

There is an inherent trade-off in those methods: on one side, quantum tomography and conventional entanglement witnesses are in principle able to detect any amount of entanglement, but require well-calibrated measurement devices; indeed, systematic errors can lead to false positives on separable states [1]. On the other side, Bell inequalities and device-independent entanglement witnesses never lead to false positives, but the price to pay is that they only detect entanglement in a strict subset of entangled states and are quite sensitive to losses and inefficiencies of detection.

We define in this talk Measurement-Device-Independent Entanglement Witnesses [2] providing a different trade-off: MDI-EWs can witness entanglement in any entangled state, are insensitive to losses, and never lead to false positives.

1 MDI-EWs scenarios

The operation of MDI-EWs is based on the semiquantum games introduced by Buscemi in [3]. In the bipartite case, the two separated parties, Alice and Bob, receive quantum states τ_s (for Alice) and ω_t (for Bob) and must output values a and b respectively. The correlation between these values is characterized by the conditional probability distribution $P(a,b|\tau_s,\omega_t)$.

A MDI-EW is a linear combination of those probabilities:

$$I(P) = \sum_{stab} \tilde{\beta}_{stab} P(a,b|\tau_s,\omega_t), \tag{1}$$

such that $I(P) \geqslant 0$ holds when Alice and Bob only share classical resources such as shared randomness or classical communication. A violation $I(P) < 0$ guarantees that Alice and Bob share entanglement in a *Measurement-Device-Independent* (MDI) manner (altough not independently of the input states τ_s, ω_t and quantum theory). In particular, no assumption is made on the dimension of the quantum state shared by the parties.

Conventional entanglement witnesses require measurement devices to be well-characterized; this requirement is replaced in MDI-EWs by requiring input states to be produced precisely as prescribed in the protocol — a comparison of these requirements is given in Figure 1. This is a natural assumption when Alice and Bob want to verify entanglement in ρ_{AB}, and so select and prepare their input states themselves, trusting their own local state preparation devices. It can be argued that a state preparation device is easier to trust than a measurement device, because the latter is by definition open to its external environment and may receive physical systems outside its operating specifications [5].

2 Loss-tolerant MDI-EWs for any entangled state $\rho_{\mathbf{AB}}$

We consider now MDI-EWs that are loss-tolerant by construction. We make Alice's and Bob's outputs binary, with the convention that $a = 1$, $b = 1$ is a conclusive measurement and that $a = 0$, $b = 0$ is an inconclusive measurement or indicates the loss of part of the shared state. The inequality is then constructed using only conclusive events:

$$I(P) = \sum_{st} \beta_{st} P(1,1|\tau_s,\omega_t), \tag{2}$$

such that losses reducing uniformly $P(1,1|\tau_s,\omega_t)$ by a constant factor will not affect the sign of $I(P)$.

*denis.rosset@unige.ch
†c.branciard@physics.uq.edu.au
‡yeongcherng.liang@unige.ch
§nicolas.gisin@unige.ch

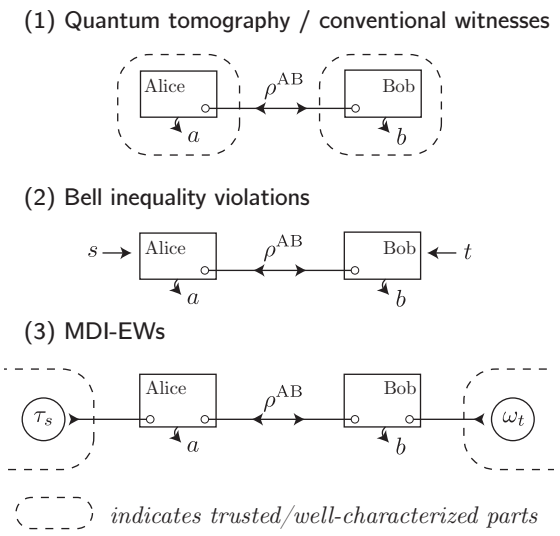

Figure 1: Different ways of witnessing entanglement in a quantum state ρ_{AB} and corresponding assumptions on the devices. (1) Quantum tomography/conventional entanglement witnesses require well-calibrated and trusted measurement devices. (2) Violating a Bell inequality is a signature of entanglement in ρ_{AB} regardless of the local operation of Alice and Bob measurement devices. (3) Measurement-device-independent entanglement witnesses rely on trusted local quantum state preparation devices without trusting the operation of Alice and Bob measurement devices.

We now construct an inequality able to witness entanglement in an arbitrary entangled state ρ_{AB} of dimension $d_A \times d_B$. For every entangled state ρ_{AB}, a conventional entanglement witness $\mathcal{W}$ can be constructed explicitly [6]. This $\mathcal{W}$ can be decomposed using real coefficients β_{st} on some local density matrices $\tau_s^\top$, $\omega_t^\top$:

$$\mathcal{W} = \sum_{st} \beta_{st} (\tau_s^\top \otimes \omega_t^\top), \tag{3}$$

and such β_{st} and transposed density matrices τ_s, ω_t define a MDI-EW as in (2) (see proof in [2]). This MDI-EW can be violated by Alice and Bob provided they perform the following joint measurements: Alice has to measure jointly the provided input state τ_s with ρ_{AB}; Bob does the same using ω_t. The measurement most favorable to a violation of (2) is a projection on the maximally entangled state $|\phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle$, with the outcome $a = 1$ corresponding to Alice projecting successfully on $|\phi_{d_1}\rangle$ and $b = 1$ corresponding to Bob projecting successfully on $|\phi_{d_2}\rangle$. The outcomes $a, b = 0$ indicate either an unsuccessful projection or the loss of the shared state. In the case of polarization-encoded qubits, such a partial Bell measurement can be realized using a beam-splitter and two detectors [4].

3 No-go theorem on simulation of MDI-EW correlations

We also showed in [7] a surprising feature of the quantum input scenarios used for our MDI-EWs: classical communication does not allow the parties to fake the presence of entanglement. Indeed, Alice and Bob receive quantum states τ_s, ω_t without knowing the classical indices s, t of those states. To communicate meaningfully, Alice and Bob have to measure their input states, and because the possible states are non-orthogonal, any measurement will also destroy information about the state.

This contrasts with Bell inequalities, where Alice and Bob know their inputs s, t and can simulate all correlations by simply communicating s and t — the same argument holds for device-independent approaches using classical inputs.

Thus, in quantum input scenarios, arbitrarily weak entanglement can always be distinguished from unlimited classical communication, reinforcing the point that *all* entangled states have an edge over classical resources in their information processing capabilities.

References

[1] *D. Rosset*, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin and Y.-C. Liang . Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses. In *Phys. Rev. A*, 86(6):062325, 2012.

[2] C. Branciard, *D. Rosset*, Y.-C. Liang and N. Gisin. Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States. In *Phys. Rev. Letters*, 110(6):060405, 2013.

[3] F. Buscemi. All Entangled Quantum States Are Nonlocal. In *Phys. Rev. Letters*, 108(20):200401, 2012.

[4] C.K. Hong, Z.Y. Ou and L. Mandel. Measurement of Subpicosecond Time Intervals between Two Photons by Interference. In *Phys. Rev. Letters*, 59(18):2044, 1987.

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. In *Nat. Photonics*, 4, 686, 2010.

[6] A.C. Doherty, P.A. Parrilo and F.M. Spedalieri. Detecting multipartite entanglement In *Phys. Rev. A*, 71(3):032333, 2005.

[7] *D. Rosset*, C. Branciard, Y.-C. Liang and N. Gisin. Entangled states cannot be classically simulated in generalized Bell experiments with quantum inputs. In *New Journal of Physics* **15**, 053025, 2013.