Quantum Information and Computation, Vol. 7, No. 1 (2007) 157–170

AN ANOMALY OF NON-LOCALITY

ANDRÉ ALLAN MÉTHOT, VALERIO SCARANI
Group of Applied Physics, Université de Genève
1211 Genève 4 Switzerland

Received February 7, 2006
Revised Auguest 8, 2006

Ever since the work of Bell, it has been known that entangled quantum states can produce non-local correlations between the outcomes of separate measurements. However, for almost forty years, it has been assumed that the most non-local states would be the maximally entangled ones. Surprisingly it is not the case: non-maximally entangled states are generally more non-local than maximally entangled states for all the measures of non-locality proposed to date: Bell inequalities, the Kullback-Leibler distance, entanglement simulation with communication or with non-local boxes, the detection loophole and efficiency of cryptography. In fact, one can even find simple examples in low dimensions, confirming that it is not an artefact of a specifically constructed Hilbert space or topology. This anomaly shows that entanglement and non-locality are not only different concepts, but also truly different resources. We review the present knowledge on this anomaly, point out that Hardy's theorem has the same feature, and discuss the perspectives opened by these discoveries.

Keywords: Entanglement, Non-locality, Simulation of entanglement

Communicated by: R Cleve

1. Introduction

The history of quantum non-locality is far from being continuous: it is indeed made of abrupt steps followed by periods of stagnation (which are however becoming shorter and shorter in the recent few years). The field was initiated in 1935 by Einstein, Podolsky and Rosen (EPR) who used entanglement in a cleverly constructed argument to attack the validity of quantum physics as a complete theory of Nature [1]. An entangled state was specified such that, when a position measurement is made on the first particle, the position of the second is known with perfect predictability and, conversely, when a momentum measurement is made on the first particle, the momentum of the second particle is known with arbitrary precision. Ruling out a *spukhafte Fernwirkung* (spooky action at a distance), EPR concluded that position and momentum must be elements of reality, i.e. must have values predetermined before the measurement. If translated into a mathematical formalism, local realism—the point of view put forth by EPR— translates into local hidden variable (LHV) models. It took the better part of three decades for Bell to come along and realize that if LHVs are indeed present, then the predictions of quantum theory cannot be correct [2]. Bell's result opens the possibility of discriminating experimentally between LHVs or quantum theory; still, not many people rushed on the test, and about 20 years had to elapse before the issue was settled (at least for the majority of the physicists) in favor of quantum theory [3]. Experiments have multiplied since, but we won't focus on them and come rather back to theory.

Letting apart the appearance of the Greenberger-Horne-Zeilinger argument involving more than two particles [4], we can safely say that until 1989 the studies on non-locality had focused on a single quantum state, namely the maximally entangled state of two spins one-half (qubits), which is in modern notations

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{1}$$

In 1991, Gisin asked whether any other bipartite entangled state could be non-local, and he found that *all* pure entangled bipartite states are in fact non-local [5]. Shortly later, Popescu and Rohrlich demonstrated that any pure entangled quantum state is non-local [6]. For mixed states, the situation is more complex; two milestones are [7, 8], but we won't discuss these issues here.

With the advent of quantum information, around 1995, the study of entanglement accelerated rapidly. One of the new ideas was to define a quantitative measure for entanglement. This problem is still unsolved in general. However, for pure bipartite quantum states (on which we focus from now on), the amount of entanglement is uniquely defined as

$$\mathcal{E}\left(|\psi_{AB}\rangle\right) = S(\rho_A) \tag{2}$$

where $S(\cdot)$ is von Neumann entropy and $\rho_A = \mathrm{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$ is the state of A obtained by partial trace [9]. Note that since $S(\rho_A) = S(\rho_B)$ for all bipartite pure states, the definition is not ambiguous. As a consequence, a maximally entangled state of two d-level systems is one which can be written (in a convenient basis) as

$$|\Psi_d\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle|k\rangle, \tag{3}$$

since it reaches up to $\mathcal{E}\left(|\Psi_d\rangle\right) = \log_2(d)$ bits. In particular, the state $|\Phi^+\rangle$, see (1), is a maximally entangled state of two qubits.

In this passion for entanglement, non-locality was however left aside from the mainstream. This was the reason why, apart from a result by Eberhard in 1993 [10] which went almost unnoticed, it took another decade after Gisin's 1991 theorem to unlock another feature of non-locality. At first sight, this feature appears as an anomaly: *for all measures of non-locality invented to date, it happens almost always* that the most non-local state is not the maximally entangled one.* It is the object of the present paper to review the evidences collected to date for this anomaly, to see what can be deduced from this anomaly and to point the possible new directions of research that it inspires.

2. The basic case shows no anomaly

A good starting point consists in reviewing first Gisin's theorem [5], thus showing a case where the anomaly does *not* show up.

*This means that counterexamples to this statement exist, as shown in Section 2.

2.1. *The CHSH inequality*

Let's introduce first the basic tool: the Bell inequality derived by Clauser, Horne, Shimony and Holt (CHSH) in 1969 [11]. Let A_1 and A_2 be two possible measurements on particle A, whose outcomes are written a_1 and a_2 In this setting, the outcomes are binary and we write them as $a_j \in \{-1, +1\}$. Let similar definitions hold for the measurements B_1 and B_2 on particle B. Let us now define, in this context, an element of reality λ has an ensemble ensemble of possible answers, the quadruple (a_1, a_2, b_1, b_2), to any measurements on particle A and B. One can then compute the function $CHSH_L(\lambda) = a_1b_1 + a_1b_2 + a_2b_1 - a_2b_2$ and convince himself that $-2 \leq CHSH_L(\lambda) \leq 2$ for any choice of λ. It is important to note that the value of this number cannot be ascertained directly in a single run of local measurements, for a_1 and a_2 cannot be measured simultaneously. The same holds for b_1 and b_2. However, by measuring several identically produced pairs with randomly chosen measurements, one can estimate the average value

$$\begin{aligned} CHSH_L \equiv & \int \rho(\lambda)\, CHSH_L(\lambda)\, d\lambda \\ =& E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2), \end{aligned} \tag{4}$$

where $E(\cdot)$ is the expectation value and $\rho(\lambda)$ is the probability distribution of λ. The CHSH inequality is just the obvious conclusion

$$|CHSH_L| \leq 2. \tag{5}$$

The CHSH inequality is remarkable since it is the unique extremal Bell inequality when restricting to two possible measurements per particle and binary outcomes [12, 13]. Let us now turn our attention to the quantum world.

2.2. *Gisin's theorem for qubits*

The most general pure state of two qubits can be written in the Schmidt basis as

$$|\psi(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \tag{6}$$

with $\theta \in [0, \frac{\pi}{4}]$. Through all this paper, when we describe qubits, we use the convention that $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli matrix σ_z for the eigenvalue $+1$ and -1 respectively. In other words, when measured in the computational basis, σ_z, the $|0\rangle$ and $|1\rangle$ state return the values $+1$ and -1 respectively. The usual measurement rules for a state in superposition of $|0\rangle$ and $|1\rangle$ applies. Any projective measurement on a qubit can be described by the projection on the eigenstates of a Pauli matrix $\vec{n} \cdot \vec{\sigma}$ where $\vec{n}$ is a normalized unit vector. Therefore we can rewrite Equation (4) as

$$CHSH_Q(\{\vec{a}_i, \vec{b}_j\}) \equiv E(\vec{a}_1, \vec{b}_1) + E(\vec{a}_1, \vec{b}_2) + E(\vec{a}_2, \vec{b}_1) - E(\vec{a}_2, \vec{b}_2), \tag{7}$$

where a simple quantum mechanical calculation yields

$$\begin{aligned} E(\vec{a}_i, \vec{b}_j) &= \langle\psi(\theta)|(\vec{a}_i \cdot \vec{\sigma}) \otimes (\vec{b}_j \cdot \vec{\sigma})|\psi(\theta)\rangle \\ &= a_z^i b_z^j \, + \, \sin(2\theta)\left(a_x^i b_x^j - a_y^i b_y^j\right). \end{aligned} \tag{8}$$

We can then put this expression into (7) and try and maximize the expression by choosing the measurements conveniently. The maximum value is found when one chooses $\vec{a}_1 = \hat{z}$, $\vec{a}_2 = \hat{x}$, $\vec{b}_1 = c\hat{z} + s\hat{x}$ and $\vec{b}_2 = c\hat{z} - s\hat{x}$ with $c = 1/\sqrt{1+\sin^2(2\theta)}$ and $s = \sin(2\theta)/\sqrt{1+\sin^2(2\theta)}$. This value is

$$CHSH_Q(\theta) = 2\sqrt{1+\sin^2(2\theta)} \tag{9}$$

which is always larger than 2 unless $\theta = 0$. In conclusion, all pure states of two qubits, but obviously the separable ones, violate the CHSH inequality.

2.3. *Comparison with entanglement*

The amount of entanglement contained in $|\psi(\theta)\rangle$ is readily computed: from

$$\rho_A = \rho_B = \begin{pmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{pmatrix} \tag{10}$$

one obtains

$$\mathcal{E}\left(|\psi(\theta)\rangle\right) = H\left(\cos^2\theta, \sin^2\theta\right) \tag{11}$$

where $H(\cdot)$ is the well known Shannon entropy. In the region $\theta \in [0, \frac{\pi}{4}]$, the entropy is increasing in function of θ, as expected. Such is also the violation $CHSH_Q(\theta)$ given in (9). Consequently, in the example studied here and in some generalisations [14], the more entangled is a state, the more non-local it is, which seems pretty natural. However, we shall see that such a state of affairs is rather an exception!

3. Escaping the detection loophole

We first review the issue of the detection loophole; being the very first example in which the anomaly of non-locality showed up [10]. We consider the same physical situation as in the previous Section, namely two binary measurements on each qubit of a pair. Ideally, for any measurement, only the two results $+$ and $-$ are possible. However, in a true experiment there is a third possible result, labelled $\perp$, corresponding to the events where the detector does not fire. Physicists normally make the natural assumption of fair sampling: the particles that are detected constitute a representative set of all the particles. In other words, the fact that the detector does not fire depends on parameters which are completely uncorrelated to the physical system that is measured. The assumption of fair sampling is reasonable and in agreement with the orthodox understanding of quantum physics. Nonetheless, when key issues like non-locality are at stake, it is also reasonable to be careful.

To study the detection loophole, one can rewrite the CHSH inequality in a form first derived by Clauser and Horne [15]:

$$\begin{aligned} \mathrm{Pr}_{A_1B_1}[++] + \mathrm{Pr}_{A_1B_2}[++] + \mathrm{Pr}_{A_2B_1}[++] - \mathrm{Pr}_{A_2B_2}[++] \\ - \mathrm{Pr}_{A_1}[+] - \mathrm{Pr}_{B_1}[+] \leq 0. \end{aligned} \tag{12}$$

This inequality can be obtained directly from Equation (13) of [10] by noticing that

$$\begin{aligned} \mathrm{Pr}_{A_1B_2}[+-] + \mathrm{Pr}_{A_1B_2}[+\perp] &= \mathrm{Pr}_{A_1}[+] - \mathrm{Pr}_{A_1B_2}[++] \\ \mathrm{Pr}_{A_2B_1}[-+] + \mathrm{Pr}_{A_2B_1}[\perp+] &= \mathrm{Pr}_{B_1}[+] - \mathrm{Pr}_{A_2B_1}[++]. \end{aligned} \tag{13}$$

Quantum mechanics tells us that if we are to perform measurements on the state $|\psi(\theta)\rangle$ with detectors of efficiency η, we would have

$$\begin{aligned} \mathrm{Pr}_{A_i}[+] &= \eta\,\frac{1}{2}\left(1+\cos(2\theta)\,a_z^i\right), \\ \mathrm{Pr}_{B_i}[+] &= \eta\,\frac{1}{2}\left(1+\cos(2\theta)\,b_z^i\right) \text{ and} \\ \mathrm{Pr}_{A_iB_j}[++] &= \eta^2\,\frac{1}{4}\left(1+\cos(2\theta)\,(a_z^i+b_z^j)+E(\vec{a}_i,\vec{b}_j)\right), \end{aligned} \tag{14}$$

where $E(\vec{a}_i,\vec{b}_j)$ is defined in Equation (8). By reinserting these expressions into the inequality (12), one finds that the inequality can be violated if and only if the efficiency of the detector is high enough, namely

$$\eta > \eta_c(\theta) \;=\; \min_{\{\vec{a}_i,\vec{b}_j\}}\left[\frac{4+2\cos(2\theta)\,(a_z^1+b_z^1)}{2+2\cos(2\theta)\,(a_z^1+b_z^1)+CHSH_Q(\{\vec{a}_i,\vec{b}_j\})}\right]. \tag{15}$$

For the present study, we want to see for which state the closure of the detection loophole requires the smallest detection efficiency. This criterion can be seen as a measure of non-locality, since (intuitively) the more non-local a state is, the easier its non-locality is to be revealed in an imperfect measurement. We have not found an explicit analytical solution for the minimization (15); a numerical approach is however perfectly convenient here. One finds that, for any $\theta < \frac{\pi}{4}$, the settings are *not* those that maximize the violation of the CHSH inequality (If one uses those settings, the required detection efficiency increases as θ decreases.): rather, they have the form $\vec{a}_1 = c_1\hat{z}+s_1\hat{x}$, $\vec{a}_2 = c_2\hat{z}+s_2\hat{x}$, $\vec{b}_1 = c_1\hat{z}-s_1\hat{x}$ and $\vec{b}_2 = c_2\hat{z}-s_2\hat{x}$ with $c_j = \cos(f_j(\theta))$ and $s_j = \sin(f_j(\theta))$ and $f_j(\theta)$ a function which can be found numerically. When these settings are used, $\eta_c(\theta)$ decreases as θ decreases. In particular, one has $\eta_c(\theta=\frac{\pi}{4}) = \frac{2}{\sqrt{2}+1} \approx 0.828$ and $\eta_c(\theta\to 0)\to\frac{2}{3}$.

One might think that this astonishing unusual characteristic is not an anomaly of non-locality or of entanglement, but of the specific inequality that has been considered. However, there exists an explicit local model which recovers the quantum predictions for the maximally entangled state (independently of any inequality) as soon as $\eta \leq \frac{3}{4}$ [16]. This means that for $\frac{2}{3} < \eta \leq \frac{3}{4}$, the maximally entangled state can in no way close the detection loophole, while some non-maximally entangled states can, namely those with $\theta \lesssim 0.145\,\pi$.

4. Two qutrits, two measurements

In the case of the detection loophole, we have seen that the anomaly arises for the simplest case of composed systems, namely two qubits†. In this Section, we discuss measures of non-locality for which the anomaly is not present for two qubits, but it appears for the next simplest case, namely when the non-locality of two *three-level systems (qutrits)* is studied using only two settings per qutrit.

To understand this Section, a sketch of the geometrical view of the problem may be useful. Once the number of parties (here, two), of settings (here, two per party) and the dimension of the outcomes (here, a trit per party) is fixed, one can represent all possible

† Other appearances of the anomaly for two qubits will be discussed in Section 5 and 6.

probability distributions as a closed set in a large-dimensional space; the borders are given by the constraints that all probabilities must be positive and sum up to one. Within this set, one can define the set of local correlations: this set is closed, convex, and has a finite number of extremal points (that is, all local distributions can be written as convex combinations of those points). Technically, such a set is called a *polytope*. A point outside the polytope of local correlations represents, quite obviously, a non-local probability distribution. In this view, a Bell inequality is a facet of the polytope, and to violate the inequality means precisely that the point lies above the facet, i.e. outside the polytope. The amount of violation is related to the geometrical distance between the facet and the point, and is thus a natural candidate for a measure of non-locality[‡].

4.1. *Violation of Bell's inequality*

We focus on Bell inequalities for two qutrits using two settings per qutrit. In this case, it has been proved [13, 17] that all the facets of the polytope are equivalent up to trivial symmetries (like relabelling of the settings and of the outcomes) either to the CHSH inequality or to the so-called CGLMP inequality [18]:

$$\begin{aligned} CGLMP_L = \; & \Pr[a_1 \equiv b_1] + \Pr[a_1 \equiv b_2] + \Pr[a_2 \equiv b_1] \\ & + \Pr[a_2 \equiv b_2 + 2] - \Pr[a_1 \equiv b_1 + 1] - \Pr[a_1 \equiv b_2 + 2] \\ & - \Pr[a_2 \equiv b_1 + 2] - \Pr[a_2 \equiv b_2] \leq 2, \end{aligned} \tag{16}$$

where $a_i, b_j \in \{0, 1, 2\}$ and the equivalence is modulo 3. The study of this inequality in general is tedious, all the same a lot of symmetry is found if we restrict to the settings that a thorough study demonstrated to be the optimal ones for the cases discussed here[§]. We can write the optimal settings explicitly in the form of projectors onto the following states[¶]:

$$A_j \;:\; \left\{ \begin{array}{lcl} |a_j = 0\rangle & = & |0\rangle + e^{i\alpha_j}|1\rangle + e^{2i\alpha_j}|2\rangle \\ |a_j = 1\rangle & = & |0\rangle + \chi e^{i\alpha_j}|1\rangle + \bar{\chi} e^{2i\alpha_j}|2\rangle \\ |a_j = 2\rangle & = & |0\rangle + \bar{\chi} e^{i\alpha_j}|1\rangle + \chi e^{2i\alpha_j}|2\rangle \end{array} \right. \text{ and} \tag{17}$$

$$B_k \;:\; \left\{ \begin{array}{lcl} |b_k = 0\rangle & = & |0\rangle + e^{i\beta_k}|1\rangle + e^{2i\beta_k}|2\rangle \\ |b_k = 1\rangle & = & |0\rangle + \bar{\chi} e^{i\beta_k}|1\rangle + \chi e^{2i\beta_k}|2\rangle \\ |b_k = 2\rangle & = & |0\rangle + \chi e^{i\beta_k}|1\rangle + \bar{\chi} e^{2i\beta_k}|2\rangle \end{array} \right. , \tag{18}$$

where we have omitted the normalization factors $1/\sqrt{3}$ for readability, have defined $\chi = e^{2i\pi/3}$ and $\bar{\chi} = e^{-2i\pi/3}$ and left α_j and β_k undefined for now[‖]. Let us consider a state which is Schmidt-diagonal in the computational basis:

$$|\psi\rangle = c_0|00\rangle + c_1|11\rangle + c_2|22\rangle, \tag{19}$$

‡It is to be noted that it is this exact measure, termed differently, that we have used in Section 2.It should also be noted that this measure is not unique: as we will see, many measures of non-locality have been put forth. They all seem *a priori* as good one another.

§This search through all possible settings has always been performed numerically [19, 20].

¶ These projectors are equivalent as first applying a phase shift ($|0\rangle \to |0\rangle, |1\rangle \to e^{i\alpha_j}|1\rangle$ and $|2\rangle \to e^{2i\alpha_j}|2\rangle$; likewise for Bob with $\alpha_j \to \beta_j$), then the Fourier transform and finally measuring in the computational basis.

‖Note that the role of χ and $\bar{\chi}$ is reversed between A and B.

with $c_n \in \mathbb{R}$. A simple calculation leads to

$$\Pr(a_j \equiv b_k + \delta) = \frac{1}{9} \sum_{n,m=0}^{3} c_n \, c_m \, \cos\left[(n-m)\left(\alpha_j + \beta_k + \frac{2\pi}{3}\delta\right)\right]. \tag{20}$$

We can now use Equation (20) in the Inequality (16) and optimize with respect to α_j and β_k for any possible state. For the maximally entangled state ($c_n = \frac{1}{\sqrt{3}}$), the best choices are $\alpha_1 = 0$, $\alpha_2 = \frac{\pi}{3}$, $\beta_1 = -\frac{\pi}{6}$ and $\beta_2 = \frac{\pi}{6}$, and one obtains $CGLMP_Q(|\Psi_3\rangle) = 4(2\sqrt{3}+3)/9 \approx 2.873$ [18]. However, Acín, Durt, Gisin and Latorre [21] found that, *for the very same choice of settings*, another state gives a higher violation. Specifically, the violation $CGLMP_Q(|\psi(\gamma)\rangle) = 1 + \sqrt{11/3} \approx 2.915$ is obtained for the non-maximally entangled state

$$|\psi(\gamma)\rangle = \frac{1}{\sqrt{2+\gamma^2}} \big(|00\rangle + \gamma|11\rangle + |22\rangle\big), \tag{21}$$

where $\gamma = (\sqrt{11} - \sqrt{3})/2 \approx 0.792$. It should be noted that no larger violation can be obtained by exploring all possible states and settings and that the violation for the maximally entangled state is also optimal. In conclusion, for a system composed of two qutrits, the unique Bell inequality which uses two settings per qutrit also exhibits an anomaly in its measure of non-locality.

4.2. *Two other measures*

The picture becomes even more involved when, keeping the two qutrits and the two settings, one explores other measures of non-locality than the violation of the Bell inequality.

The first of these measures considered here is the classical relative entropy, or Kullback-Leibler (K-L) distance, which measures the "distance" between two probability distributions P and P' in terms of information. More precisely, the K-L distance is the average amount of support in favor of P against P', when data are generated using P. Explicitly,

$$\mathcal{D}(P||P') = \sum_z P(z) \log\left(\frac{P(z)}{P'(z)}\right) \tag{22}$$

where the zs are the possible outcomes or events. Using this notion, we can define another natural measure of non-locality: *the K-L distance of the non-local probability distribution under study to the closest local probability distribution*, that is

$$D(P_{NL}) = \min_{P_L \in \mathcal{L}} \mathcal{D}(P_{NL}||P_L) \tag{23}$$

where P_L and P_{NL} are respectively the local and non-local probability distributions and $\mathcal{L}$ is the polytope of local correlations. This measure of non-locality was studied in [22], to which we refer the reader for all details. An interesting result stands out: when optimizing over the settings, the maximally entangled states can give rise to non-local correlations such that $D = 0.058$ bits, no more. Nevertheless, the largest value, $D = 0.077$ bits, can be obtained for the correlations generated from a non-maximally entangled state of the form (21), but here with $\gamma \approx 0.653$.

The other new measure of non-locality derives from a very recent idea: can one demonstrate the security of key distribution** whenever Alice and Bob share a non-local distribution, even against an adversary who would not be limited by quantum mechanics but only by causality? The partial answers found to date to this question are positive [23, 24, 25]. Then one can define a measure of "useful" non-locality: the most non-local state is the one from which one obtains the correlations that ensure the *highest rate of extractable secret key against an adversary limited only by causality.* Under several assumptions that we cannot review here, the most non-local state of two qutrits according to this criterion is again of the form (21), with a value $\gamma \approx 0.987$, different from the previously encountered ones [25].

4.3. *Summary*

We have discussed three measures of non-locality, all of which show an anomaly in the case of qutrits when the freedom of the measurement is restricted to two settings per qutrit. Interestingly, the most non-local states are always of the same form, but with different numerical coefficients according to the different measures. Actually, numerical evidence shows that this observation is true beyond the case of qutrit, that is for any $d > 3$ [21, 22, 25]. Thus, it seems that the scenario where the participants share two qubits is the *only* case where the anomaly does not appear for all the measures studied here.

The main restriction of the results reviewed in Section 2, 3,and 4 is the limitation of the number of settings to two per party. It is still possible—although improbable in our opinion—that the anomaly will disappear when increasing the number of settings. Needless to say, this is a hard open problem.

5. Simulation of entanglement with non-local resources

In the previous Section, we have considered measures of non-locality which are directly inspired by experiments or that are related to specific configurations, fixed number of settings. A novel approach was developed in the recent few years with the advent of computer scientists in the field. A different measure of non-locality has been put forth: the simulation of quantum correlations by classical non-local resources. The intuition behind this concept is "the more non-local a state is, the more non-local resources will be required to generate the same correlations". We review this framework in the present Section.

5.1. *Non-local resources*

Bell has showed that one cannot simulate the correlations arising from quantum states using only local resources. For such a negative statement, one just has to find a *gedanken* experimental setup in which a contradiction arises, and this is precisely what a Bell inequality does††. Given that local resources are not enough, how much of *non-local resources* must be added in order to simulate the quantum correlations? The goal here is to reproduce the quantum mechanical results for all possible measurements, not only for a finite number of them. This question was first formulated in 1992 by Maudlin [26]. However, the result was published in

** A cryptographic paradigm where Alice and Bob want to extend to number of secret bits they share with one another, but with no one else.

†† Incidentally, it is remarkable that a contradiction can be already found using only two measurements per particle.

a philosophical proceeding and went unnoticed from the quantum information community for several years. Independently, Brassard, Cleve and Tapp revived the field in 1999 by improving on the result of Maudlin [27][‡‡]. These authors found that one could simulate all quantum correlations that can arise from the state $|\Phi^+\rangle$, see Equation (1), by adding eight bits of communication to an infinite amount of LHVs. This result is already noteworthy, because it was not evident a priori that a finite amount of communication could do[*]. More noteworthy still, after some improvements, in 2003 Toner and Bacon provided an explicit model in which *a single bit of communication* added to local variables is enough to reproduce the correlations of $|\Phi^+\rangle$ [28].

Bits of communication are clearly a non-local resource, since they can be used to signal information. Nonetheless, they also have an unpleasant feature: they can be used to signal information. It is a well known fact that quantum correlations cannot be used to communicate. No matter how spooky the correlations appear, they remain causal. It would be much more elegant to find another non-local resource for which the no-signaling condition holds by definition. In 2004, Cerf, Gisin, Massar and Popescu (CGMP) found such a resource [31]: the *non-local box* (NLB)—a mathematical object invented ten years before by Tsirelson [29] and independently by Popescu and Rohrlich [30] to solve related but different problems. The NLB is a virtual device that has two input-output ports such that if Alice inputs a bit into her end, the NLB gives her a uniformly random bit, likewise for Bob. The non-locality appears from the fact that the exclusive-OR (sum modulo 2) of the outputs is always equal to the logical AND (product) of the inputs. CGMP proved that a single use of the NLB added to local variables allows to simulate perfectly the correlations of $|\Phi^+\rangle$.

In summary, the statistics arising from measurements on the maximally entangled state of two qubits can be simulated exactly by adding to the local variables either one bit of communication or the even weaker resource called the NLB. These results are nicely re-derived in a unified way in [32].

5.2. *The anomaly*

One might expect that the simulation of non-maximally entangled states of two qubits would follow as an easy generalization of the simulation of the maximally entangled state. Quite the opposite is true. The state-of-the-art is as follows.

For non-local resources that allow signaling: correlations arising from non-maximally entangled states can be reproduced using two bits of communication [28]—actually a weaker resource, the Oblivious-Transfer Box which is a well-known primitive of information science, is sufficient [33]. It is not known whether even weaker resources (ultimately, one bit) could do.

Using the non-signaling NLB, a sharper evidence of the anomaly has been found: a single use of the NLB is provably *not sufficient* to reproduce the statistics of non-maximally entangled states of two qubits [34].

One might conceive another physically meaningful non-local resource: a single instance of

‡‡ It is important to note that Brassard, Cleve and Tapp were blissfully ignorant of Maudlin's paper. Else they might not even have attempted to prove their theorem, since an argument against it was formulated in Maudlin's paper. Moreover, Steiner also published independently a result along these lines, merely several days after Brassard, Cleve and Tapp. However, Maudlin already had a better result then he.

* Maudlin actually claimed that it could not been done.

the maximally entangled state of two qubits. Even with this quantum resource, it has been showed that a maximally entangled state and an infinite amount of LHVs are not sufficient to simulate a non-maximally entangled state [20]. In the case where we are restricted to von Neumann measurements on the maximally entangled state of two qubits, the proof follows from the fact that we can simulate any von Neumann measurement on a maximally entangled state with one NLB and shared randomness, while these resources are not sufficient to simulate measurements on a non-maximally entangled state. The general case where we are allowed to perform any POVM on the maximally entangled state is more intricate and it is not within the scope of this paper to cover this proof.

In conclusion, the anomaly of non-locality shows up also for the "amount of non-local resources".

6. Hardy's theorem

Hardy used a different type of construction then Bell in order to show the non-local nature of entanglement [35]. Although not a measure of non-locality, we think it is fitting to present it here, for it also reveals an interesting property of entanglement. We will present here Brassard's rendition [36] of Hardy's proof for simplicity, in the same fashion as in [37]. Lets say that Alice and Bob share the state $(|01\rangle + |10\rangle + |11\rangle)/\sqrt{3}$ along the z axis. Let say that Alice and Bob are now given the choice of performing either the σ_z or the σ_x measurement. According to quantum mechanics, if Alice and Bob are to measure $\sigma_x \otimes \sigma_x$, then they will receive the output $(-1,-1)$ with probability $1/12$. Let us now assume that the state has LHVs that will produce a $(-1,-1)$ output on a $\sigma_x \otimes \sigma_x$ measurement. From the criteria of locality and realism, we now have that any local σ_x measurement on this particular state will produce the output -1. Let us now see what happens if Alice and Bob are to measure $\sigma_x \otimes \sigma_z$ or $\sigma_z \otimes \sigma_x$. From the predictions of quantum mechanics, the state should never be allowed to produce $(-1,-1)$ as output. Once again according to the criteria of locality and realism, we are forced to conclude that upon a local σ_z measurement, the state will produce $+1$ as output. Therefore, a $\sigma_z \otimes \sigma_z$ measurement on this particular instance is bound to output $(+1,+1)$, which is forbidden by quantum mechanics. So in order for the LHV theory to output $(-1,-1)$ on a $\sigma_x \otimes \sigma_x$ measurement with a non zero probability, it will also output $(+1,+1)$ on a $\sigma_z \otimes \sigma_z$ measurement with non zero probability, in clear contradiction with the predictions of quantum mechanics. It is very interesting to note that this construction works with almost any states of two qubits. Among the exceptions, we count separable states and maximally entangled states. Thus, we have an approach to non-locality, which works only if the state is non-maximally entangled. It should be noted that this fact does not depend on Hardy's construction, but that it is also true for any Hardy-type proof of non-locality [38].

7. Perspectives on non-locality

7.1. *The (partial) end of the story...*

It is through quantum theory that physicists have discovered non-locality, and the only channel known in nature that allows to distribute non-local correlations are entangled quantum particles. It is therefore understandable that entanglement and non-locality have been essentially identified for many years. Results like Eberhard's [10] were either ignored, or considered as a curiosity. When ten years later Acín, Durt, Gisin and Latorre [21] found the anomaly for Bell inequalities for qutrits, the strangeness of the result did not hit immediately, because it still might have been an anomaly of the Bell inequality (the fact that the CGLMP inequality is unique was proved later).

Four years later however, we cannot escape the evidence: *non-locality and entanglement are not only different concepts, but are really quantitatively different resources.* We have listed a large number of "measures of non-locality" such as violation of Bell inequalities, Kullback-Leibler distances, extractable secret key rate, robustness against the detection loophole and simulation of entanglement with signaling and non-signaling resources. They all seemed to be infected with the same anomaly: there exist cases, in which maximally entangled states are not maximally non-local.

At this point, one can address the following question: why couldn't we simply accept the measure of entanglement itself, see Equation (2), as a measure of non-locality? Then the anomaly would disappear by construction. The answer to this question is subtle and instructive. The quantity $\mathcal{E}\left(|\psi_{AB}\rangle\right)$ is the fraction of maximally entangled states of two qubits that one can extract out of a given entangled state with the procedure called *distillation* [39]. In distillation, two assumptions are made. The first assumption is that Alice and Bob share N copies of an entangled state $|\psi_{AB}\rangle$ and can make any local operations involving as many of their particles as they wish. In fact, the objective of distillation is to convert as many non-maximally entangled states (states with low local entropy) into maximally entangled states (states with maximal local entropy), while maybe losing a few states in the process. This is highly similar to the notion of *block-coding* in computer science, where one is interested in transforming a long string of bits, which do not necessarily have a high entropy, into a shorter string with every bit having maximum entropy. Therefore, one can see quantum distillation as a form of entanglement block-coding. However, non-locality experiments are not usually performed in such a way: Alice and Bob receive first one pair and measure it, then a second pair and measure it, and so on. In other words, non-locality appears in nature without the need of block-coding. The second assumption in distillation, and more generally in entanglement manipulation, is that Alice and Bob can communicate through a classical channel as much as they desire, because entanglement does not increase under classical communication. But *classical communication* is a non-local resource: non-locality does increase if classical communication is allowed. Now the reader can read back in the article and notice indeed that none of the measures of non-locality listed above require block coding (in particular, the probability distributions one is working with are those of repeated single-pair measurements) or classical communication.

The impossibility of classical communication also shows why our anomaly is not "fake". In entanglement manipulation, one can transform deterministically a maximally entangled state into a non-maximally entangled one, using local operations and classical communication. If this transformation were possible here, then the anomaly would disappear. However, classical communication is crucial [42, 43], and since it is not allowed in the context of non-locality, the anomaly persists.

It has long been known that non-locality and entanglement are different *concepts*. To our knowledge, the first example that demonstrated that non-locality and entanglement where different *resources* came from [34]. It is well known from Tsirelson's bound [40] that quantum mechanics cannot achieve a perfect simulation of the NLB, embodiment of non-locality. This is true independently of the amount of entanglement shared by the participants. However, Cerf, Gisin, Massar and Popescu have shown that a single NLB is sufficient to simulate bipartite measurements of a maximally entangled state[31]. Nonetheless, as pointed out in Section 5.2, it was proven in [34], that at least two NLBs are required to simulate some non-maximally entangled state of two qubits. This was the first hint that NLBs are not strictly more powerful resources than entanglement in a one-to-one comparison. The general proof was laid down in [41], where the authors have shown quantum correlations that require an exponential, in the number of maximally entangled states, amount of NLBs to simulate. The added power of entanglement, when taken in large numbers, comes from the fact that we can entangle several $|\Phi^+\rangle$ together.

7.2. *...and the many open perspectives*

We conclude on a non-exhaustive list of open problems:

1. Have we established an exhaustive list of measures of non-locality? Or, could we find others, and if yes, will they all show the anomaly?

2. What is the physical reason of the anomaly?

3. If entanglement and non-locality are really different resources, can one find a protocol in which non-locality (and not entanglement) must be optimized? Actually, such a protocol has been proposed [44, 45], but this example is artificial: the context has been invented precisely to have this feature.

4. How does the picture generalize to multipartite entanglement, where even the notion of maximal entangled is not uniquely defined?

5. Another direction of research would be to examine the properties of non-locality measures, such as additivity.

As it turns out, research in non-locality is not only the pleasure of inventing new Bell inequalities: more than forty years after Bell's work, there are very basic issues which are not well understood.

Acknowledgements

We thank Antonio Acín, Hugues Blier, Anne Broadbent, Nicolas Gisin, and Elham Kashefi for stimulating discussions. We acknowledge financial support from the European Project QAP.

References

1. A. Einstein, B. Podolsky and N. Rosen (1935), *Can quantum-mechanical description of physical reality be complete?*, Physical Review, Vol. 47, pp. 777–780.
2. J. S. Bell (1964), *On the Einstein-Podolsky-Rosen paradox*, Physics, Vol. 1, pp. 195–200.

3. A. Aspect, J. Dalibard and G. Roger (1982), *Experimental test of Bell's inequalities using time-varying analyzers*, Physical Review Letters, Vol. 49, pp. 1804–1807.
4. D. M. Greenberger, M. Horne and A. Zeilinger (1989), *Going beyond Bell's theorem*, in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, M. Kafatos (editor), Kluwer Academic, pp. 69–72.
5. N. Gisin (1991), *Bell's inequality holds for all non-product states*, Physics Letters A, Vol. 154, pp. 201–202.
6. S. Popescu and D. Rohrlich (1992), *Generic quantum nonlocality*, Physics Letters A, Vol. 166, pp. 293–297.
7. R. F. Werner (1989), *Quantum states with Einstein-Podolski-Rosen correlations admitting a hidden-variable model*, Physical Review A, Vol. 40, pp. 4277–4281.
8. R. Horodecki, P. Horodecki and M. Horodecki (1995), *Violating Bell inequality by mixed spin-$\frac{1}{2}$ states: necessary and sufficient condition*, Physics Letters A, Vol. 200, pp. 340–344.
9. M. J. Donald, M. Horodecki and O. Rudolph (2002), *The uniqueness theorem for entanglement measures*, Journal of Mathematical Physics, Vol. 43, pp. 4252–4272.
10. P. Eberhard (1993), *Background level and counter efficiencies required for a loophole free Einstein-Podolsky-Rosen experiment*, Physical Review A, Vol. 47, pp. R747–R750.
11. J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt (1969), *Proposed experiment to test local hidden-variable theories*, Physical Review Letters, Vol. 23, pp. 880–884.
12. A. Fine (1982), *Hidden variables, joint probability, and the Bell inequalities*, Physical Review Letters, Vol. 48, pp. 291–294.
13. D. Collins and N. Gisin (2004), *A relevant two qubit Bell inequality inequivalent to the CHSH inequality*, Journal of Physics A: Mathematical and General, Vo. 37, pp. 1775–1787.
14. B. S. Tsirelson (1987), *Quantum analogues of the Bell inequalities. The case of two spatially separated domains.*, Journal of Soviet Mathematics Vol. 35, pp. 557–570.
15. J. F. Clauser, and M. A. Horne (1974), *Experimental consequences of objective local theories* Physical Review D, Vol. 10, pp. 526–535.
16. N. Gisin and B. Gisin (1999), *A local hidden variable model of quantum correlation exploiting the detection loophole*, Physics Letters A, Vol. 260, pp. 323–327.
17. L. Masanes (2003), *Tight Bell inequality for d-outcome measurements correlations*, Quantum Information and Computation, Vol. 3, pp. 345–358.
18. D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu (2002), *Bell inequalities for arbitrarily high-dimensional systems*, Physical Review Letters, Vol. 88, p. 040404.
19. A. Acín, private communication.
20. N. Gisin, private communication.
21. A. Acín, T. Durt, N. Gisin and J. I. Latorre (2002), *Quantum nonlocality in two three-level systems*, Physical Review A, Vol. 65, p. 052325.
22. A. Acín, R. Gill and N. Gisin (2005), *Optimal Bell tests do not require maximally entangled states*, Physical Review Letters, Vol. 95, p. 210402.
23. J. Barrett, L. Hardy and A. Kent (2005), *No signaling and quantum key distribution*, Physical Review Letters, Vol. 95, p. 010503.
24. A. Acín, N. Gisin and L. Masanes, *From Bell's theorem to secure quantum key distribution*, preprint available at http://arxiv.org/quant-ph/0510094.
25. V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino and A. Acín, *Secrecy extraction from non local correlations*, to appear, preprint available at http://www.arxiv.org/quant-ph/0606197.
26. T. Maudlin (1992), *Bell's inequality, information transmission, and prism models*, PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association, Vol. 1, pp. 404–417.
27. G. Brassard, R. Cleve, and A. Tapp (1999), *Cost of exactly simulating quantum entanglement with classical communication*, Physical Review Letters, Vol. 83, pp. 1874–1877.
28. B. F. Toner and D. Bacon (2003), *The communication cost of simulating Bell correlations*, Physical Review Letters, Vol. 91, p. 187904.
29. B. S. Tsirelson (1993), *Some results and problems on quantum Bell-type inequalities*, Hadronic

Journal Supplement, Vol. 8, pp. 329–345.
30. S. Popescu and D. Rohrlich (1994), *Quantum nonlocality as an axiom*, Foundations of Physics, Vol. 24, pp. 379–385.
31. N. Cerf, N. Gisin, S. Massar and S. Popescu (2005), *Simulating maximal quantum entanglement without communication*, Physical Review Letters, Vol. 94, p. 220403.
32. J. Degorre, S. Laplante and J. Roland, *Simulating quantum correlations as a distributed sampling problem*, Physical Review A, **72**, pp. 062314.
33. N. Gisin, S. Popescu, V. Scarani, S. Wolf and J. Wullschleger, *Oblivious transfer and quantum channels*, preprint available at http://arxiv.org/quant-ph/0601157.
34. N. Brunner, N. Gisin and V. Scarani (2005), *Entanglement and non-locality are different resources*, New Journal of Physics, Vol. 7, p. 88.
35. L. Hardy (1992), *Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories*, Physical Review Letters, Vol. 68, pp. 2981–2984.
36. G. Brassard, *Quantum Information Processing for Computer Scientist*, MIT Press, Cambridge, to appear.
37. A. A. Méthot, *On local-hidden-variable no-go theorems*, Canadian Journal of Physics, to appear, preprint available at http://arxiv.org/quant-ph/0507149.
38. G. Brassard and A. A. Méthot, *Clear separations in Bell-theorem complexity classes*, in preparation.
39. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wooters (1996), *Purification of noisy entanglement and faithful teleportation via noisy channels*, Physical Review Letters, Vol. 76, pp. 722–725.
40. B. S. Cirel'son (1980), *Quantum generalizations of Bell's inequality*, Letters in Mathematical Physics, Vol. 4, pp. 93–100.
41. A. Broadbent and A. A. Méthot, *On the power of non-local boxes*, Theoretical Computer Science C, **358**, pp. 3–14.
42. P. Hayden and A. Winter (2003), *Communication cost of entanglement transformations*, Physical Review A Vol. 67, pp. 012326.
43. W. van Dam and P. Hayden (2003), *Universal entanglement transformations without communication*, Physical Review A Vol. 67, pp. 060302R.
44. Č. Brukner, M. Zukowski and A. Zeilinger (2002), *Quantum Communication Complexity Protocol with Two Entangled Qutrits*, Physical Review Letters, Vol. 89, pp. 197901.
45. Č. Brukner, M. Zukowski, J.-W. Pan and A. Zeilinger (2004), *Bell's Inequalities and Quantum Communication Complexity*, Physical Review Letters, Vol. 92, pp. 127901.