Bounds on quantum non-locality via partial transposition

Karol Horodecki[1,2], Gláucia Murta[2,3]
[1] *Institute of Informatics, University of Gdańsk, 80–952 Gdańsk, Poland*
[2] *National Quantum Information Centre in Gdańsk, 81–824 Sopot, Poland and*
[3] *Departamento de Física, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil*

We explore the link between two concepts: the level of violation of a Bell inequality by a quantum state and discrimination between two states by means of local operations and classical communication (LOCC). For any bipartite Bell inequality, we show that its value on a given quantum state can not exceed the classical bound by more than the maximal quantum violation shrunk by a factor reporting distinguishability of this state from the separable set by means of LOCC. We then consider the general scenarios where the parties are allowed to perform a local pre-processing of many copies of the state before the Bell test (asymptotic and hidden-non-locality scenarios). We define the rate of non-locality and, for PPT states, we bound this quantity by the relative entropy of entanglement of the partially transposed state. The bounds are strong enough to limit the use of certain states containing private key in the device-independent scenario.

The quantitative study of non-locality has two different approaches, one is to ask, for a fixed Bell scenario, what is the best one can obtain optimizing over all possible quantum resources (states and measurements) [1–7]. A converse approach is to ask for a fixed quantum state, or a class of states, what is the best one can obtain using this state as a resource, *i.e.* optimizing over all Bell scenarios. Some references in this second approach include the seminal work of Werner [8] exhibiting a local model for projective measurements for $U \otimes U$-invariant states (see also [9]). Another result showing that typically the violation of correlation Bell inequalities by multipartite qudit states is very small [10]. And an hierarchy of semidefinite programs that allows to bound the violation achievable by PPT states [11].

Here we follow the second approach, with the aim to show that certain states, despite being entangled, exhibit very limited gain of non-locality.

To achieve this, we develop a not well explored link between the subject of state discrimination via restricted class of operations and violation of a Bell inequality [12]. This idea turned out to be fruitful, because the subject of state discrimination by the restricted operations like e.g. Local Operations and Classical Communication (LOCC), is well established in quantum information theory (see e.g. [13] for recent results, and references therein). The link between quantum non-locality and state discrimination that we start from, amounts to a simple observation that if a given state is hardly distinguishable from some separable one, it can not exhibit large violation in any Bell scenario, or else, one could use the procedure of checking the violation of a Bell inequality to discriminate between these two states (a quantitative version of this fact has been derived in [12]). Here we refine these ideas, using partial transposition to explore the fact that Bell inequalities are implemented by a small class of operations, the local ones. It is vital for our examples, that certain entangled states containing bits of privacy are at the same time almost indistinguishable from some separable states by LOCC operations i.e. they have hidden security [14, 15]. This fact has recently ruled them out as a potential resource for swapping of a private key, in the so called quantum key repeaters [15], and interestingly the techniques introduced there can be applied in our context.

We prove limited gain of nonlocality for states in the class of the so called *private states*, and some approximate private states which has *positive partial transposition* (PPT) [16, 17]. In [18, 19] it is shown, that both private states and the approximate private states which are PPT, can be used to perform QKD protocols, secure under the most general quantum (coherent) attacks. In [20] it is shown that any perfect private state violate a Bell inequality. We therefore bound the non-locality obtainable from such states, in order to qualify their usefulness in the so called Device-Independent Quantum Key Distribution protocols [21–23]. Recently it has been shown, that certain PPT bipartite states can exhibit non-zero violation of some Bell inequality [12], disproving the famous *Peres conjecture* [24]. We then focus on the question of how much non-locality can be obtained from PPT states.

Our findings are general, as we provide upper bounds on the amount of quantum non-locality for the scenarios which are now mainly under consideration: the single copy scenario, and (for states with positive partial transposition) the asymptotic as well as the hidden-nonlocality scenario. To the best of our knowledge, this is the first quantitative approach for the latter two scenarios. The bounds are powerful enough to limit the use of certain approximate private states (useful for quantum key distribution) in the device-independent scenario, which is a counterintuitive result showing a fundamental gap between quantum and device independent cryptography due to the presence of noise.

Our first result is a bound on the violation of a Bell inequality $\mathcal{S}$, on a single copy of a bipartite quantum state ρ, which we denote by $Q_S(\rho_{AB})$. We show, that it exceeds the classical value $C(\mathcal{S})$ by the maximal quantum value $Q(\mathcal{S})$ for this Bell inequality, shrunk by a factor related to distinguishability between the state and separable states

(SEP). More precisely, for any bipartite Bell expression $\mathcal{S}$, and bipartite state ρ_{AB}, there is:

$$Q_{\mathcal{S}}(\rho_{AB}) \leq C(\mathcal{S}) + Q(\mathcal{S}) \times \inf_{\sigma \in SEP} ||\rho_{AB}^{\Gamma} - \sigma^{\Gamma}||. \tag{1}$$

Where $||.||$ denotes the trace norm, and Γ denotes partial transposition i.e. $\rho^{\Gamma} \equiv (\mathrm{I} \otimes T)\rho$. The above bound is significant for the states which are hardly distinguishable from separable ones by the so called PPT operations, as the term $||\rho^{\Gamma} - \sigma^{\Gamma}||$ upper bounds distinguishability between ρ and σ by this class of operations. The bound is trivial for ρ which is close in trace norm to a separable σ. However, as we show in examples, some private and approximate private states, are both far in trance norm-distance from separable states, and close to some separable state in distance based on partial transposition, proving that the above bound has non-trivial implications. Focusing then, on the states ρ for which there exists some separable state σ so that $||\rho^{\Gamma} - \sigma^{\Gamma}|| \leq \epsilon$ (we denote it as $\rho \in D(\epsilon)$), we observe that, for any bipartite Bell expression $\mathcal{S}$ and $\epsilon > 0$, there is:

$$\sup_{\rho \in D(\epsilon)} Q_{\mathcal{S}}(\rho) \leq C(\mathcal{S}) + \epsilon \times Q(\mathcal{S}). \tag{2}$$

The above inequality shows, that all states which are ϵ distinguishable from separable ones by restricted class of operations (such as LOCC or separable operations), can violate the classical bound $C(\mathcal{S})$ of any Bell inequality $\mathcal{S}$ only by an ϵ fraction of the maximal quantum bound.

We now describe the results regarding multiple copies of the input state, which are bounds on quantum non-locality in the *asymptotic* and *hidden non-locality* scenarios. Let us fist recall, that in the asymptotic scenario we quantify how much non-locality can be obtained using bipartite states, after pre-processing n copies of the state by the so called Local Operations and Classical Communication (LOCC) in asymptotic limit. Following [25] we measure non-locality of a bipartite state using the relative entropy measure. Namely, given a behavior $\mathcal{P} = P(ab|xy)$, where for fixed inputs x, y we have distribution $P_{xy}(ab|xy)$ of outputs a and b, its non-locality is quantified by:

$$\mathcal{N}(\mathcal{P}) = \sup_{\{p(x,y)\}} \inf_{P_L \in L} \sum_{x,y} p(x,y) D(P_{xy}(ab|xy)||P_L(ab|x,y)) \tag{3}$$

where supremum in the above is taken over distribution of inputs $\{p(x,y)\}$, and infimum is taken over all behaviors admitting a local model (belonging to set L) and $D(P||Q)$ is the relative entropy between distributions P and Q. We then define the *rate of non-locality* for a bipartite state ρ_{AB}:

$$R(\rho_{AB}) \equiv \overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda \in LOCC} \sup_{\{M_{xy}\}} \mathcal{N}(\{Tr M_{xy} \Lambda(\rho_{AB}^{\otimes n})\}), \tag{4}$$

where $\overline{\lim}$ denotes the supremum limit, and the family of probability distributions $\{Tr M_{xy}\rho\}$ represents the behavior obtained via performing so called local POVMs (positive operator valued measures) $\{M_{xy}\} \equiv \{M_{a|x} \otimes M_{b|y}\}$ on state ρ where x, y denotes the inputs and a, b the ouputs of the behaviour.

Before giving the bound for R, let us consider also the hidden non-locality scenario due to S. Popescu [26], in which the parties can perform a 'filtering' operation prior to the Bell test. He showed that by performing a 'filtering' operation, and given that this operation succeeds, it is possible to obtain much larger violation of the CHSH game on the resulting state, not bounded as we claimed. However, we note that it is also important to take into account the probability of obtaining the 'filtered' result. For this reason, in order to quantify the effect of postselection, we propose to consider the *rate of hidden non-locality*, $R_H(\rho_{AB})$, which is defined as the product of the gained non-locality by the probability of obtaining this gain:

$$R_H(\rho_{AB}) \equiv \overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda \in LOCC} \sup_{\{M_{xy}\}} \sup_{F_0} p^{F_0} \mathcal{N}(\{Tr M_{xy} F_0(\Lambda(\rho_{AB}^{\otimes n}))\}). \tag{5}$$

Here, a filtering process, F_0, takes state $\Lambda(\rho_{AB}^{\otimes n})$ to flag form, $F(\rho) = \sum_i |i\rangle\langle i| \otimes F_i \rho F_i^{\dagger}$, and later erasures all other results except the "good" one that leads to the highest violation of the Bell inequality. $p^{F_0} = Tr F_0 \Lambda(\rho_{AB}^{\otimes n}) F_0^{\dagger}$ is the probability that the filter results in the desired outcome.

Having defined the important quantities, we are ready to state our main result. These are the upper-bounds on non-locality via entanglement measures and partial transposition, which hold for both the rate of non-locality as well as the rate of *hidden non-locality*. Namely, for any bipartite state ρ_{AB}, which is positive under partial transposition (PPT), there is:

$$\max\{R(\rho_{AB}), R_H(\rho_{AB})\} \leq \min\{E_r(\rho_{AB}), E_r(\rho_{AB}^{\Gamma})\}, \tag{6}$$

where E_r is the relative entropy of entanglement, i.e. $E_r \equiv \inf_{\sigma \in SEP} S(\rho||\sigma)$.

We present now important implications of the bounds shown above, starting from the single-copy case. We apply the bounds to private bits [16, 17], and to states which approximate private bits in trance norm distance (approximate private bits). For certain private bit γ of dimension $4d^2$, we obtain the following bound on violation of the CHSH inequality on it:

$$Q_{CHSH}(\gamma) \leq 2 + \frac{\sqrt{2}+1}{2\sqrt{2}d}. \tag{7}$$

This proves, that in spite of the fact, that all private states are distillable [27], and more importantly non-local [20], the non-locality gain can be severely limited for some of them. We then consider a family of approximate private states ρ_d, also of dimension $4d^2$, which are PPT [15, 28], and obtain a general bound: $Q_{\mathcal{S}}(\rho_d) \leq C(\mathcal{S}) + Q(\mathcal{S})\frac{1}{\sqrt{d}}$. Since it holds that $Q(\mathcal{S}) \leq C(\mathcal{S}) \min\{X, A\}$ where X is the number of settings and A is the number of outputs of the Bell inequality $\mathcal{S}$ [4], we conclude in this case with:

$$Q_{\mathcal{S}}(\rho_d) \leq C(\mathcal{S})(1 + \min\{X, A\} \times \frac{1}{\sqrt{d}}). \tag{8}$$

The above inequality shows that, if the Bell inequality $\mathcal{S}$ under consideration, has number of either inputs or outputs growing significantly slower than $\sqrt{d}$, one can observe only negligible violation of the inequality $\mathcal{S}$, although the states ρ_d contain 1 bit of secure key (in limit of large d), and are shown to be useful for Quantum Key Distribution. Let us then focus on implication of the above fact to Device Independent Quantum Key Distribution (DI QKD) [21–23]. Any DI QKD protocol bases on some Bell inequality $\mathcal{S}$, and admits certain level of violation, say ϵ_v below which it aborts. First note, that due to eq. (8) there are approximate private bits, which exhibit violation of inequality $\mathcal{S}$ only up to $\epsilon' < \epsilon_v$, and hence will be aborted. This rules out such states from usage in this DI QKD protocol. Second, every realization of such a protocol admits inevitable errors due to decoherence. In such a case, the level of violation ϵ' can be even below the precision of the protocol. For this reason, unless the Bell inequality has impractically high number of inputs and outputs (scaling exponentially with the number of qubits which is $\approx 2 \log d$), the use of these exemplary states in DI QKD appears to be strongly limited.

We can pass to the next important examples, showing that even with access to many copies of the initial state, no matter what LOCC protocol one performs, the yield of non-locality is negligible, for the hiding security states presented above. Indeed, from the bound (6) due to asymptotic continuity of the relative entropy of entanglement, one obtains, that for states $\rho_\epsilon \in D(\epsilon)$ i.e. for which ρ_ϵ^Γ is ϵ-close in trace norm distance to some separable state, there is:

$$\max\{R(\rho_\epsilon), R_H(\rho_\epsilon)\} \leq 4\epsilon \log d + 2h(\epsilon) \tag{9}$$

where $h(.)$ is the binary Shannon entropy. This proves, that for the states ρ_d considered above, both R and R_H vanishes, when dimension d of the states increases. Indeed, for these states, ϵ decreases exponentially fast in the number of qubits $\log d$ (there is $\epsilon \in O(\frac{1}{\sqrt{d}})$) . This is a striking result, as at the same time, the so called distillable key K_D which quantifies amount of key in state ρ_d approaches 1 with increasing d, since ρ_d approaches certain private bit.

With the above results we initiate the quest for upper bounds for non-locality in the two well known many-copies scenarios: asymptotic and the hidden-nonlocality ones. We also explore the area to study the interrelation between quantum state discrimination with restricted class of operations, and the Bell non-locality, which proves powerful even in single-copy scenario. There are several interesting extensions of our approach. In particular, any result already known for discrimination with the so called *separable* operations, can be directly applied to our framework, noting that the bound (1) can be considered as much stronger, when so called SEP-norm is considered in place of the norm based on partial transposition [31]. It would be also interesting to consider distance not only to separable, but also to states admitting hidden variable model [8]. Another promising approach is to develop non-locality measures other than relative-entropy based ones. It would be also interesting to find bounds on asymptotic and hidden non-locality scenarios for states which are not PPT as the private states are. Finally let us note that, in our findings, we are close to the idea that any Bell inequality witnesses entanglement [29, 30], it would be interesting to develop the results in this context.

[1] B. S. Tsirelson, J. Soviet. Math. **36**, 557 (1987).

[2] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).
[3] M. Junge, C. Palazuelos, D. Prez-Garca, I. Villanueva, and M. Wolf, Communications in Mathematical Physics **300**, 715 (2010).
[4] M. Junge and C. Palazuelos, Communications in Mathematical Physics **306**, 695 (2011).
[5] C. Palazuelos (2012), arXiv:1206.3695.
[6] D. Prez-Garca, M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, Communications in Mathematical Physics **279**, 455 (2008).
[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[8] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[9] J. Barrett, Phys. Rev. A **65**, 042302 (2002).
[10] R. C. Drumond and R. I. Oliveira, Phys. Rev. A **86**, 012117 (2012).
[11] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).
[12] N. Brunner and T. Vértesi, Phys. Rev. A **86**, 042113 (2012).
[13] N. Yu, R. Duan, and M. Ying, IEEE Trans. Inf. Theory **60**, 2069 (2014).
[14] K. Horodecki, Ph.D. thesis, University of Warsaw (2008).
[15] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter (2014), arXiv:1402.5927.
[16] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[17] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[18] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, IEEE Trans. Inf. Theory **54**, 2604 (2008).
[19] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Phys. Rev. Lett. **96**, 070501 (2006).
[20] R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acin, Phys. Rev. Lett. **104**, 230401 (2010).
[21] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[22] E. Hanggi, R. Renner, and S. Wolf, EUROCRYPT pp. 216–234 (2010).
[23] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012).
[24] A. Peres, Found Phys. **29**, 589 (1999).
[25] W. van Dam, R. Gill, and P. Grunwald, IEEE Trans. Inf. Theory **51**, 2812 (2005).
[26] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
[27] P. Horodecki and R. Augusiak, Phys. Rev. A **74**, 010302 (2006).
[28] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[29] P. Hyllus, O. Gühne, D. Bruß, and M. Lewenstein, Phys. Rev. A **72**, 012321 (2005).
[30] B. M. Terhal, Physics Letters A **271**, 319 (2000).
[31] SEP-norm is $||X||_{sep} \equiv \sup_{M \in sep, M \leq \mathbb{1}} TrMX$, where $M = \sum_i \alpha_i A_i \otimes B_i$ for $\alpha_i \geq 0$ and A_i and B_i are positive operators.