Bounds on quantum non-locality via partial transposition

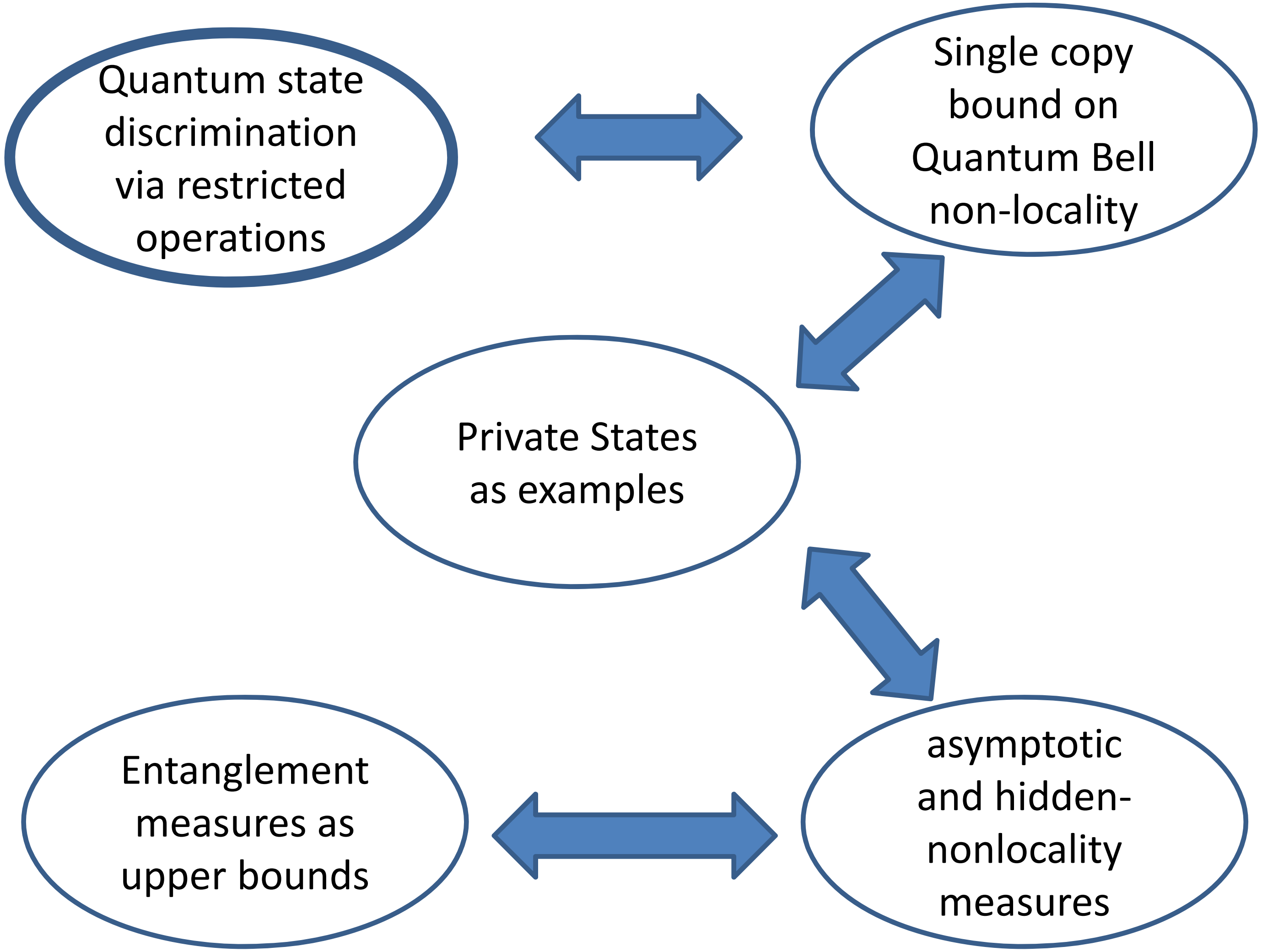
Karol Horodecki[1,2] & Glàucia Murta[2]
[1]Institute of Informatics University of Gdańsk &
[2]National Quantum Information Centre in Gdańsk

Phys. Rev. A 92, 010301(R) (2015)

Workshop on Quantum Nonlocality, Causal Structures and Device Independent Quantum Information
National Cheng Kung University, Taiwan Dec 2015

We acknowledge grants: QOLAPS, Ideas Plus, Maestro

Outline of the talk:



Restricted classes of operations

Alice

Classical **C**ommunication

Bob

Local quantum **O**perations

Local quantum **O**perations

LOCC operations

Separable operations $\Lambda \in SEP$ $\Lambda(\rho) = \sum_i A_i \otimes B_i(\rho) A_i^{\dagger} \otimes B_i^{\dagger}$

PPT operations : the ones with elements of POVM
which has positive partial transposition $\{\mathrm{F_i}\}, F_i^{\Gamma} \geq 0 \; where \; \Gamma = I \otimes T$

$LOCC \subset SEP \subset PPT \subset ALL$

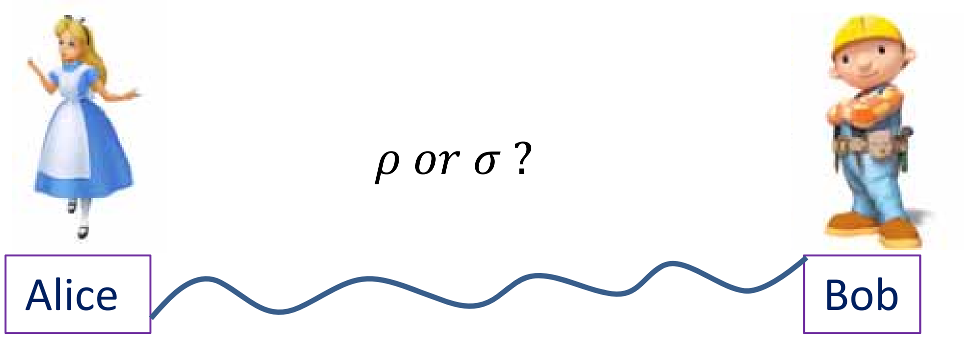
State discrimination by restricted operations

Discriminating between ρ and σ
by **global operations** [Helstrom]

$$p_s(\rho,\sigma)_{ALL} = \frac{1}{2} + \frac{1}{4}||\rho - \sigma||$$

- Quantum non-locality without entanglmenet [Bennett et al. 1998]

One can not discriminate some full basis of orthogonal product states by LOCC



Discriminating between two states
by **PPT operations**

[Eggeling & Werner 2000]

$$p_s(\rho,\sigma)_{PPT} \leq \frac{1}{2} + \frac{1}{4}||\rho^{\Gamma} - \sigma^{\Gamma}||$$

$$\rho^{\Gamma} = I \otimes T(\rho)$$

Partial transposition

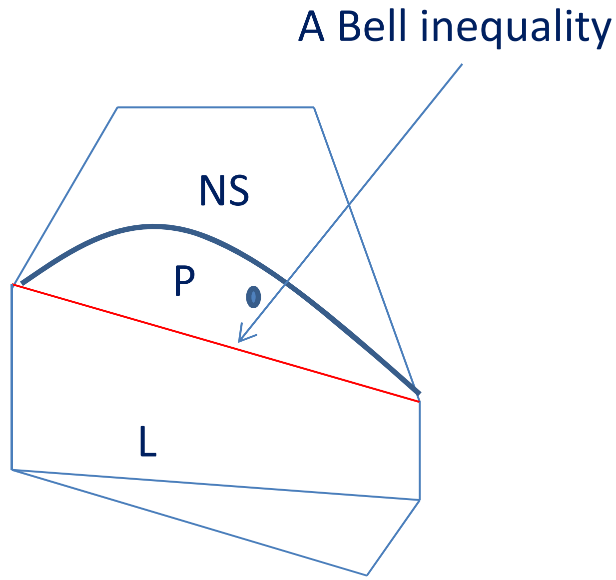
Bell (quantum) non-locality as a resource

Quantum bipartite state + set of measuremetns = quantum box

$$\{Tr M_{a|x} \otimes M_{b|y} \rho\} = P(a, b|x, y)$$

outputs Inputs

It satisfies the non-signaling condition
(change of input does not affect remote output)



The state is non-local if violates some Bell inequality $S = \{s_{x,y}^{a,b}\}$

$$\sum_{a,b,x,y} s_{x,y}^{a,b} P(a, b|x, y) \leq C(S)$$

Motivation: link the state discrimination with Bell inequalities

Preliminary observation:
If ρ is almost indistinguishable from σ via LOCC (SEP, PPT)
then the level of violation of any Bell inequality S by ρ is close to that by σ

Idea of the proof :
If not, then : via checking the level of violation one could discriminate between σ and ρ by LOCC (SEP, PPT)

Contradiction !

$$|S(\rho) - S(\sigma)| \leq C \times dist(\rho, \sigma)$$

Main task: express the above observation quantitatively

Single copy bound on quantum non-locality via partial transposition

For given:

1) quantum bipartite state ρ
2) Bell inequality S

$$Q(\rho, S) \leq C(S) + Q \times \inf_{\sigma \in SEP} ||\rho^{\Gamma} - \sigma^{\Gamma}||$$

The **maximal** value of **violation of** a Bell inequality **S** on a quantum state ρ over choices of measurements

Maximal classical value of inequality **S**

Maximal quantum value of the Bell inequality **S** over measurements and states

Shrinking factor, smaller than 1
If state ρ is indistinguishable from separable σ (which bounds distinguishability via PPT operations)

Proof of the key theorem for single copy bound

$$S(\rho) - S(\sigma) = \sum_{a,b,x,y} Tr s_{x,y}^{a,b} A_{a|x} \otimes B_{b|y} (\rho - \sigma) =$$

$$= \sum_{a,b,x,y} Tr s_{x,y}^{a,b} A_{a|x} \otimes (B_{b|y})^T (\rho - \sigma)^\Gamma$$

$$Tr\, A\, B = Tr\, A^\Gamma B^\Gamma$$

$$= Tr S^\Gamma (\rho^\Gamma - \sigma^\Gamma) = ||S^\Gamma||_\infty Tr \frac{S^\Gamma}{||S^\Gamma||_\infty} (\rho^\Gamma - \sigma^\Gamma)$$

$$\leq \sup_{M \geq 0, M \leq \mathbb{1}} ||S^\Gamma||_\infty Tr M (\rho^\Gamma - \sigma^\Gamma) = ||S^\Gamma||_\infty ||\rho^\Gamma - \sigma^\Gamma||$$

Maximal quantum value of
The Bell inequlaity related to S
by partial transposition

Recall the Eggeling-Werner bound:

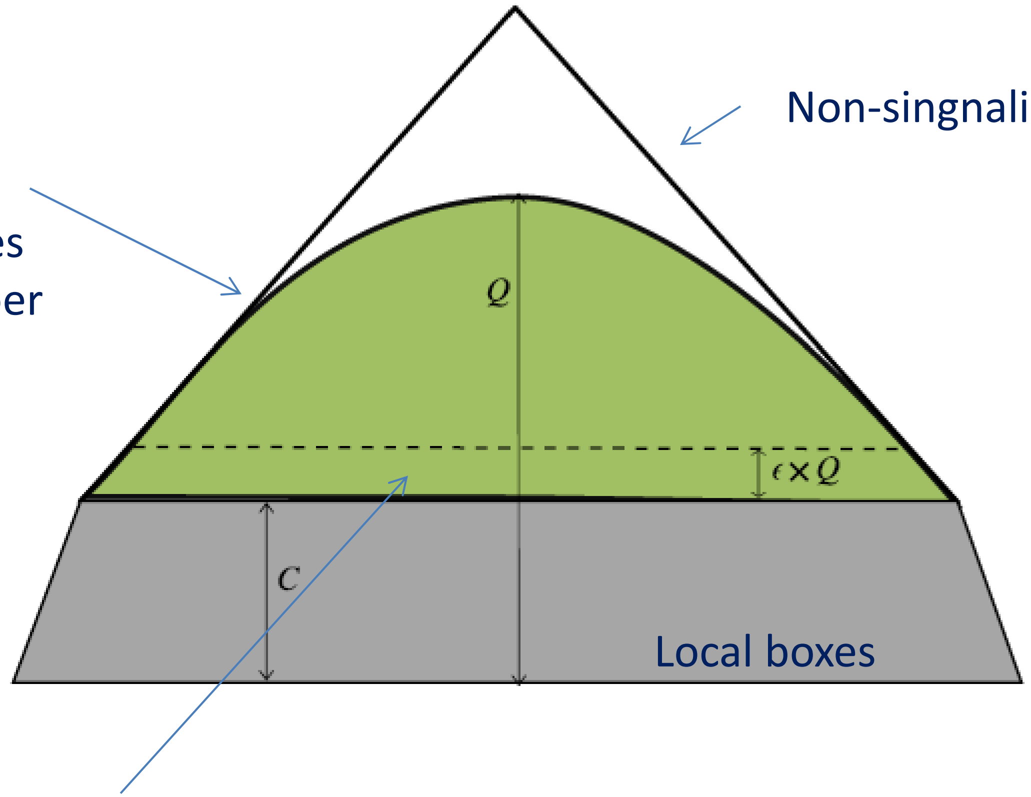
$$p_s(\rho, \sigma)_{PPT} \leq \frac{1}{2} + \frac{1}{4} ||\rho^\Gamma - \sigma^\Gamma||$$

This term reports how much is distinguishable ρ from σ

Vizualizing the result

Non-singnaling boxes

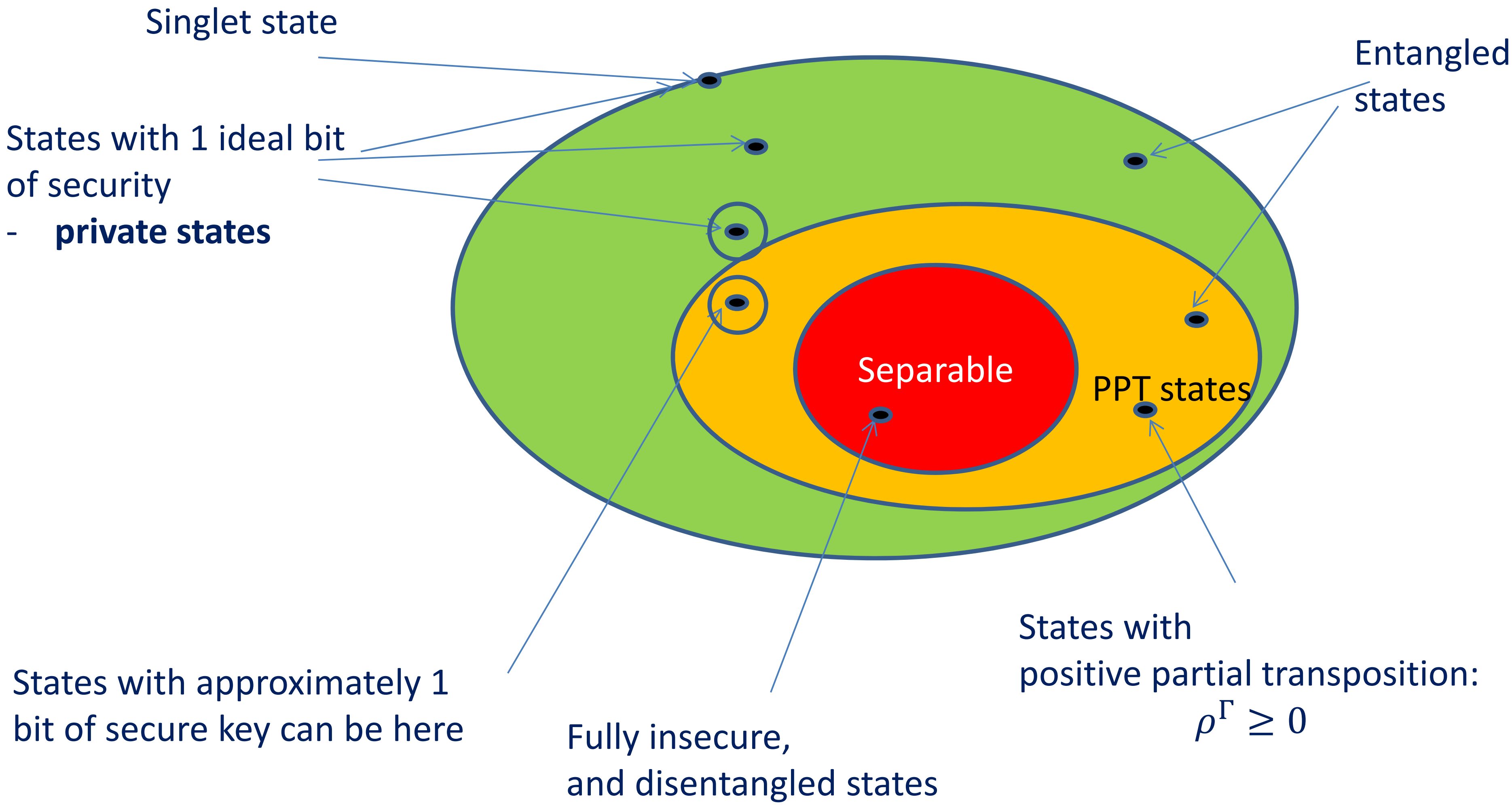
The set of all
Quantum boxes
for fixed number
of inputs and
outputs



States which are only ϵ distinguishable from separable,
can violate Bell inequality up to dashed line

Question: are there entangled states far from separable, but indistinguishable from them ?

Entangled, separable and private states



[K. M, P. Horodeccy,
J. Oppenheim PRL 2005]

Two depictions of a private bit

Private bit has systems A B A' and B': AA' with Alice, BB' with Bob

1) Arbitrary private bit is represented by an operator X such that $||X||_{tr} = 1$:

$$\gamma_X = \frac{1}{2}[|00\rangle\langle 00| \otimes \sqrt{XX^\dagger} + |00\rangle\langle 11| \otimes X + |11\rangle\langle 00| \otimes X^\dagger + |11\rangle\langle 11| \otimes \sqrt{X^\dagger X}].$$

operator „amplitudes"

2) Arbitrary private bit is a singlet state correlated to arbitrary „junk" state

$$\gamma = U\psi_+ \otimes \rho_{junk}\, U^\dagger \quad U = \sum |ij\rangle\langle ij| \otimes U_{ij}$$

Examples: $\psi_{+,}$ $\psi_+ \otimes \rho_{junk}$, $U_{BL}\psi_+ \otimes \rho_{junk} U_{BL}^\dagger$,

Locally equivalnet to singlet

$$U_{BL} = (\sum_i |i\rangle \otimes U_i)_{AA'} \otimes (\sum_j |j\rangle \otimes U_j)_{BB'}$$

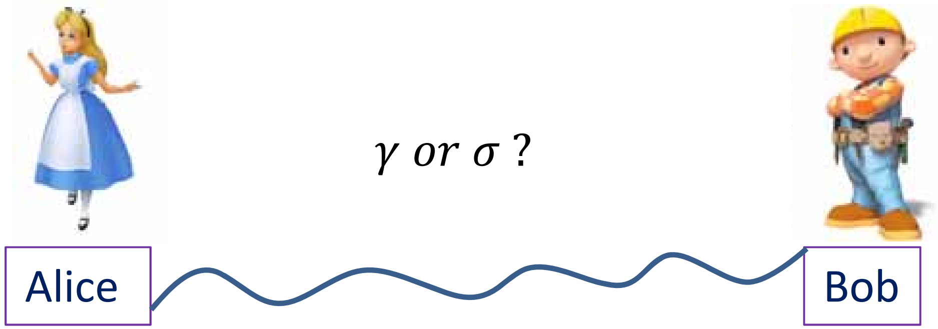
Non trivial example : $U_{00} = I$, U_{11}= V, $\rho_{junk} = I/d^2$

Some (approximate) private bits can hide security

γ − *private bit* (secure)
σ − *separable state* (insecure)

Dim = $2d^2$

γ *or* σ ?



$$p_{PPT}(\gamma,\sigma) \leq \frac{1}{2} + \frac{c}{d}$$

c>0 independent from d

γ *or* σ ?

$$p_{ALL}(\rho,\sigma) \approx 1$$

γ − *state hiding security*

[KH Phd thesis ’08]

Applying the bound to private states

- Private states: violate CHSH [Augusiak et al. 2006]
- How much ?

example of the private

$$\gamma_X = \frac{1}{2}[|00\rangle\langle 00| \otimes \sqrt{XX^\dagger} + |00\rangle\langle 11| \otimes X + |11\rangle\langle 00| \otimes X^\dagger + |11\rangle\langle 11| \otimes \sqrt{X^\dagger X}].$$

$$X = \frac{V}{d^2}$$

separable State: γ_X after attack

$$\sigma = \frac{1}{2}[|00\rangle\langle 00| \otimes \sqrt{XX^\dagger} + |11\rangle\langle 11| \otimes \sqrt{X^\dagger X}]$$

$$\left\|\gamma^\Gamma{}_X - \sigma^\Gamma\right\| = \left\|X^\Gamma\right\| = \frac{1}{d}$$

$$Q_{CHSH}(\gamma_X) \leq 2 + \frac{2\sqrt{2}}{d} \longrightarrow 2$$

with increasing dimension d

Classical value

Conclusion: some states, although entangled, having 1 bit of secure key, violate very weakly any Bell inequality with small (not scaling with d) number of mueasurements

From single copy to asymptotic bounds

Problem: The trace norm is not extensive measure – not useful for many copies of states

Wayout: We adopt the measure of non-locality „strength of non-locality proof" in:

W. van Dam, P. Grunwald, and R. Gill, IEEE Trans. Inf. Theory **51**, 2812 (2005), arXiv:quant-ph/0307125.

$$P = P(ab|xy)$$

$$N(\mathrm{P}) = \sup_{p(x,y)} \inf_{L \in Local} \sum_{x,y} p(x,y)\ D(P(ab|xy)|L(ab|xy))$$

Relative entropy function

$$\sum_i P(i) \log \frac{P(i)}{Q(i)}$$

„Local" mens the set of local boxes in the non-signaling polytope

This measure is shown to be additive on extremal boxes such as the PR box

[Grudka et al. PRL 2013]

Asymptotic relative entropy of non-locality - definition

Main question: what is the most non-local box one can get from n copies of the states ? Here is the recipy:

ρ	Input state
↓	
$\rho \otimes \rho \otimes \cdots \otimes \rho$	n copies
↓	
$\Lambda_{LOCC}[\rho \otimes \rho \otimes \cdots \otimes \rho] = \rho_{out}$	$\Lambda_{LOCC} \in LOCC$ (the best one)
↓	
$Tr\, M_{a\|x} \otimes M_{b\|y} \rho_{out} = \mathrm{P(a, b\|x, y)}$	$M_{a\|x}, M_{b\|y}$ - POVMs
↓	
N(P(a,b|x,y))	Single box measure
↓	
$\lim_{n} \frac{1}{n} N(P(a,b\|x,y))$	

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

Bound on asymptotic relative entropy of non-locality for PPT states

Theorem 2 For PPT state ρ_{AB} there is:

$$R(\rho_{AB}) \leq \min\left\{E_r(\rho_{AB}^{\Gamma}), E_r(\rho_{AB})\right\}$$

Where E_r is the relative entropy of entanglement measure:

$$E_r(\rho_{AB}) = \inf_{\sigma \in SEP} S(\rho||\sigma)$$

Quantum relative entropy function

$Tr\rho \log \rho \ - Tr\rho \log \sigma$

Exemplary appliacation:

$$R(\rho_d) \leq \frac{4}{\sqrt{d}} \log \mathrm{d} + \mathrm{h}\left(\frac{1}{\sqrt{d}}\right) \longrightarrow 0$$

$\rho_d \in PPT$

Dimension $2d^2$

[K. H.et al. IEEE 2005]

Conclusion: even asymptoti cally it is hard to access the non-locality of this state

Asymptotic relative entropy of hidden non-locality

- **Hidden non-locality:** a state admiting hidden variable model, conditionally after successful preprocessing becomes non-local. [S. Popescu 1995]

Preprocessing – it is a non-trace preserving LOCC map.

$F(\rho) \ = \ \sum_i |i\rangle\langle i| \otimes F_i \rho F_i^\dagger$ i =1 means „success" 0 outcome is ereased

How to quantify such obtained non-locality ?

Multiply the non-locality of output by probability of success:

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

Result is the same: $R_H(\rho_{AB}) \leq \min\left\{E_r(\rho_{AB}^\Gamma), E_r(\rho_{AB})\right\}$

Relation to other results

1) **Peres' Conjecture:** all bipartite PPT states do not violate any Bell inequality

Invalidation: [N. Brunner T. Vertesi PRL 2014]

Our result: PPT states sometimes poorely violate any Bell inequality with small number of settings

2) **device independent security** ?
no known DI QKD protcol works for private states which are hiding security.

3) **Entanglemet measures**, related to non-locality
other inequlities based on entanglement witnesses
are welcome [see F.G.S.L. Brandao 2005]

Summary & open questions

We provided bounds on quantum non-locality of bipartite quantum states,
in 3 scenarios: -single copy -asymptotic -hidden-nonlocality one
For some private states, only Bell inequalities with many settins can be violated

- Use of **entangled states but with a hidden variable model** (Werner states)

-may lead to single copy bounds
-rather not for asymptotic ones

- Our bound bases on PPT operations

what about **other restricted classes** of operations ?

- **PT invariant states** escape the technique to bound them. What about them ?

and multipartite states ?

- **Technique** borrowed from S. Baeuml et al. Nat. Comm. 20015

„Limitatonis to quantum key repeaters" Is it just a coincidence ?

Thank you for your attention

Relation to number of settings

- [Junge & Palazuelos CMP 2011]

$$Q(\mathcal{S}) \leq C(\mathcal{S}) \min\{n, k\}$$

Max of inputs (n) — Max of outputs (k)

Hence:

$$\mathrm{Q}(\rho, S) \leq C(S) + Q(S) \times \inf_{\sigma \in SEP} \left|\left|\rho^{\Gamma} - \sigma^{\Gamma}\right|\right|$$

$$\leq C(S)[1 + \min\{n, k\} \times \inf_{\sigma \in SEP} \left|\left|\rho^{\Gamma} - \sigma^{\Gamma}\right|\right|]$$

Tradeoff between dimension of box and distinguishability

Tighter bound: $|\mathbf{S}(\rho) - \mathbf{S}(\sigma)| \leq ||\mathbf{S}^{\Gamma}||_{\infty} ||\rho^{\Gamma} - \sigma^{\Gamma}||_{sep}$

Idea of the proof

We first partially symmetrize arguments of the quantity

$$R(\rho) = \overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda\in LOCC} \sup_{\{M_{xy}\}} \sup_{p(x,y)} \inf_{\sigma\in SEP} \sum_{x,y} p(x,y) D(\{Tr M_{xy}\Lambda(\rho^{\otimes n})\}||\{Tr M_{xy} \quad \sigma \quad)$$

$\leq$ [narrow the set of separable states over which infinum is taken

$$\overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda\in LOCC} \sup_{\{M_{xy}\}} \sup_{p(x,y)} \inf_{\sigma\in SEP} \sum_{x,y} p(x,y) D(\{Tr M_{xy}\Lambda(\rho^{\otimes n})\}||\{Tr M_{xy}\Lambda(\sigma^{\otimes n})\}) \quad := T^{\infty}(\rho)$$

$\leq$ [use double monotonicity of the relative entropy function]

$$\overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda\in LOCC} \sup_{\{M_{xy}\}} \sup_{p(x,y)} \inf_{\sigma\in SEP} \sum_{x,y} p(x,y) D(\{Tr M_{xy} \rho^{\otimes n}\}||\{Tr M_{xy} \sigma^{\otimes n} \})$$

[partial transposition property: $Tr M\rho = Tr M^{\Gamma}\rho^{\Gamma}$+monotonicity and additivity under tensor product]

$$\leq \inf_{\sigma\in SEP} S(\rho^{\Gamma}||\sigma) = E_R(\rho)$$

Bound on asymptotic relative entropy of non-locality for PPT states

Theorem 2 For PPT state ρ_{AB} there is:

$$R(\rho_{AB}) \leq \min\{E_r(\rho_{AB}^{\Gamma}), E_r(\rho_{AB})\}$$

Where E_r is the relative entropy of entanglement measure:

$$E_r(\rho_{AB}) = \inf_{\sigma \in SEP} S(\rho||\sigma)$$

Quantum relative entropy function

$Tr\rho \log \rho \; - Tr\rho \log \sigma$

Exemplary appliacation:

$$\rho_p = \frac{1-p}{2}\gamma_X + \frac{p}{2}[|01\rangle\langle 01| \otimes \sqrt{YY^\dagger} + |10\rangle\langle 10| \otimes \sqrt{Y^\dagger Y}]$$

$$X = \frac{1}{d_s\sqrt{d_s}} \sum_{i,j=0}^{d_s-1} u_{ij}|ij\rangle\langle ji|$$

$$Y = \sqrt{d_s} X^{\Gamma}$$

$$p = \frac{1}{1+\sqrt{d_s}} \qquad \rho_p \in PPT$$

$$R(\rho_p) \leq \frac{4}{\sqrt{d}} \log \mathrm{d} + \mathrm{h}\left(\frac{1}{\sqrt{d}}\right) \longrightarrow 0$$

[K. H.et al. IEEE 2005]

Conclusion: even asymptoti cally it is hard to access the non-locality of this state

Useful theorem

- Comparing Bell values of two states:

Theorem 1 *Given two bipartite states $\rho_{AB}, \sigma_{AB} \in B(\mathcal{C}^d \otimes \mathcal{C}^d)$, a Bell inequality $\{s_{x,y}^{a,b}\}$ and a set of quantum POVMs $\{A_{a|x} \otimes B_{b|y}\}$, it holds that:*

$$\Big|S(\rho) - S(\sigma)\Big| \leq ||S^\Gamma||_\infty ||\rho^\Gamma - \sigma^\Gamma||. \qquad (1)$$

where $||.||$ denotes the trace norm, $||X||_\infty$ is the largest eigenvalue in modulus of operator X, and Γ denotes partial transposition.

where $S = \sum_{a,b,x,y} s_{x,y}^{a,b} A_{a|x} \otimes B_{b|y}$.

Asymptotic relative entropy of non-locality - definition

Main question: what is the most non-local box one can get from n copies of the states by ? Here is the recipy:

1) Take many copies n of a state ρ

2) Perform the best LOCC trace preserving map Λ on $\rho^{\otimes n}$ to get ρ_{out}

3) Choose the best POVMs $M_{a|x} \otimes M_{b|y} \equiv M_{xy}$
and the size of inputs x and y and outputs a and b

4) On such obtained box $\{Tr M_{a|x} \otimes M_{b|y} \rho_{out}\}$
compute some extensive nonlocality measure

5) Divide the result by n, and take asymptotic limit (limsup)

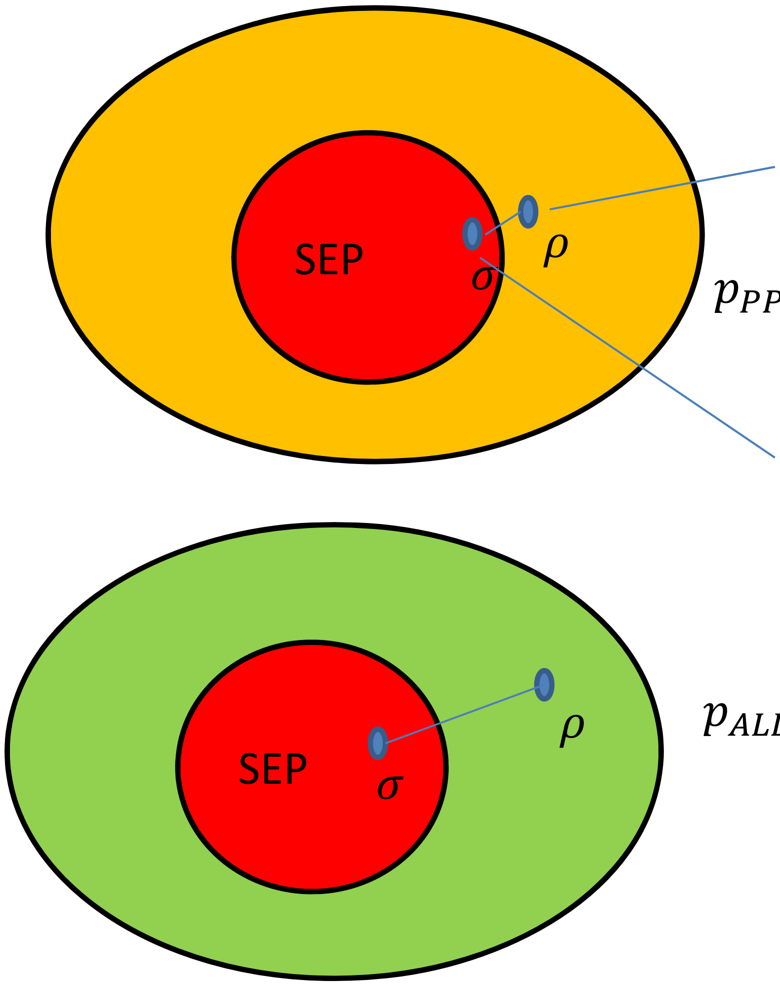
Definition: (asymptotic relative entopy of non-locality)

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

Some (approximate) private bits can hide security

Alice and Bob at a distance:

LOCC distinguishing



approximate private state

$$p_{PPT}(\rho,\sigma) \le \frac{1}{2} + \frac{c}{\sqrt{d}}$$

insecure (separable) state

$\exists \sigma \in SEP$

Alice and Bob meet:

Global distinguishing

$$p_{ALL}(\rho,\sigma) \approx 1$$

$\forall \sigma \in SEP$

Hiding security states

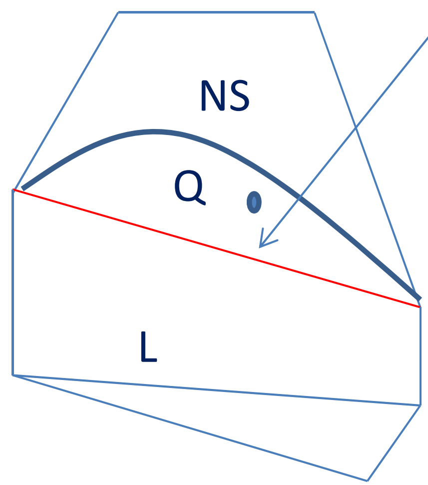
[K.H. Phd thesis '08]

Bell (quantum) non-locality as a resource

Quantum bipartite state + set of measuremetns = quantum black box

$$\{Tr M_{a|x} \otimes M_{b|y} \rho\} = P(a,b|x,y)$$

outputs Inputs



It satifsies the non-signaling condition
(change of input does not affect remote output)

Local boxes : $P(a,b|x,y) = \sum_{\lambda} p(\lambda)\, P(a|x\lambda) P(b|y\lambda)$ Obtained from separable states

If the box is non-local, it is useful e.g. for

- Quantum (or general) device-independent security
- Lower communication complexity

Non – locality is a resource

The state is non-local if violates some Bell inequality $S = \{s^{a,b}_{x,y}\}$

$$\sum_{a,b,x,y} s^{a,b}_{x,y} P(a,b|x,y) \le C(S)$$

Outline

- Restricted operations scenario
- State discrimination by restricted classes of operations
- Non-locality scenario
- Relating Bell inequalities to state discrimination
- Result 1: Single copy bound
- Private states as examples
- Result 2: Relative entropy of non-locality
- Result 3: Asymptotic and hidden-nonlocality bounds
- Conclusions and Open questions

Motivation: link the state discrimination with Bell inequalities

Let ρ be almost indistinguishable from σ via LOCC (SEP, PPT)

Main question: How much the state ρ can voilate a Bell inequality S ?

The Answere: close to violation of S by σ

Idea of the proof :
If not, then : via checking the level of violation one could discriminate between σ and ρ by LOCC.

Contradiction !

Main task: express the above fact quantitatively