Semi-Device-Independent Entanglement Quantification

WQNCSDIQI 2015 -- Tainan

Jean-Daniel Bancal

University of Basel

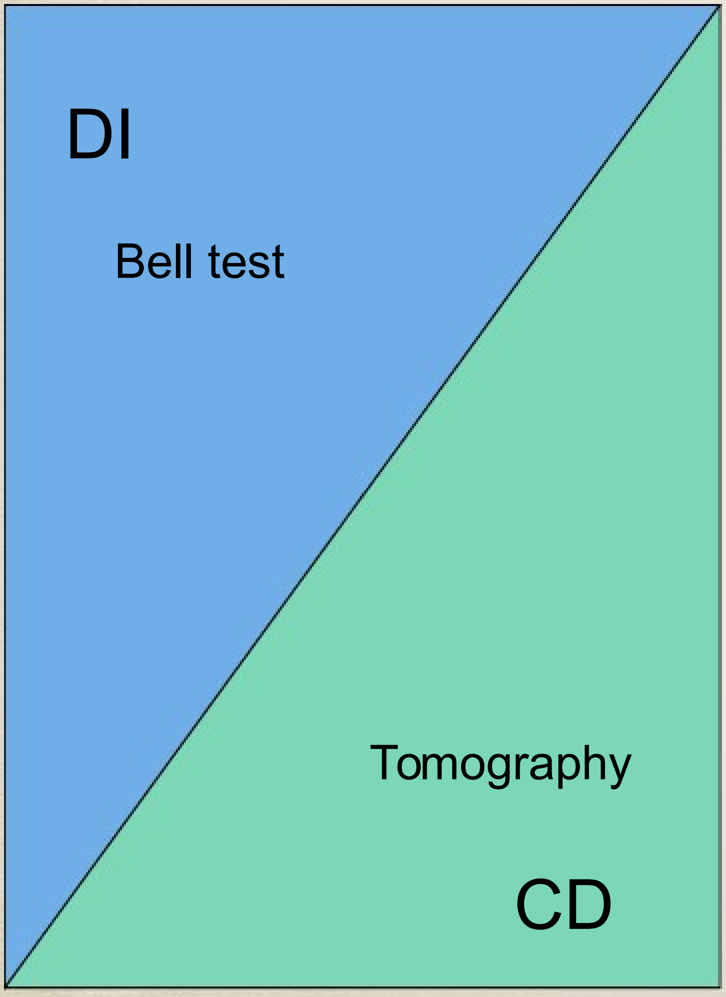
Joint work with

Koon Tong Goh, Valerio Scarani

From the Center for Quantum Technologies, Singapore

[arXiv:1509.08682]

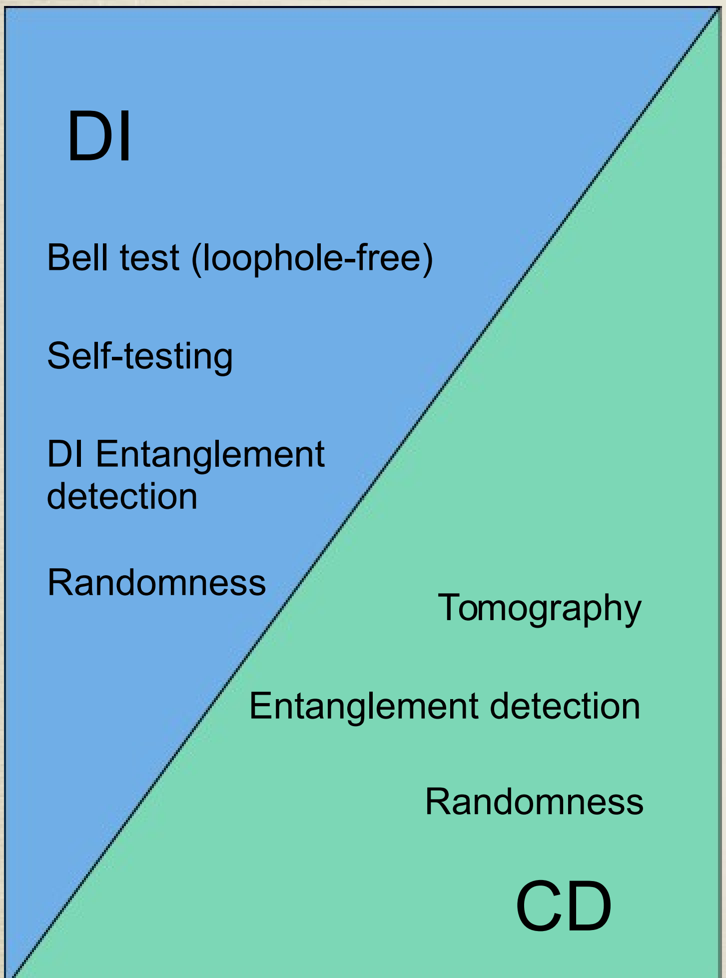
Characterized devices (CD) vs Device-independent (DI)



- CD:
  - Is the default way of analysing an experiment
  - Is convenient
  - But: is susceptible to errors
- DI:
  - Relies on few assumptions
  - Provides robust conclusions
  - But: requires very good setups
  - Is often too pessimistic

We would like robust and optimistic conclusions

Characterized devices (CD) vs Device-independent (DI)

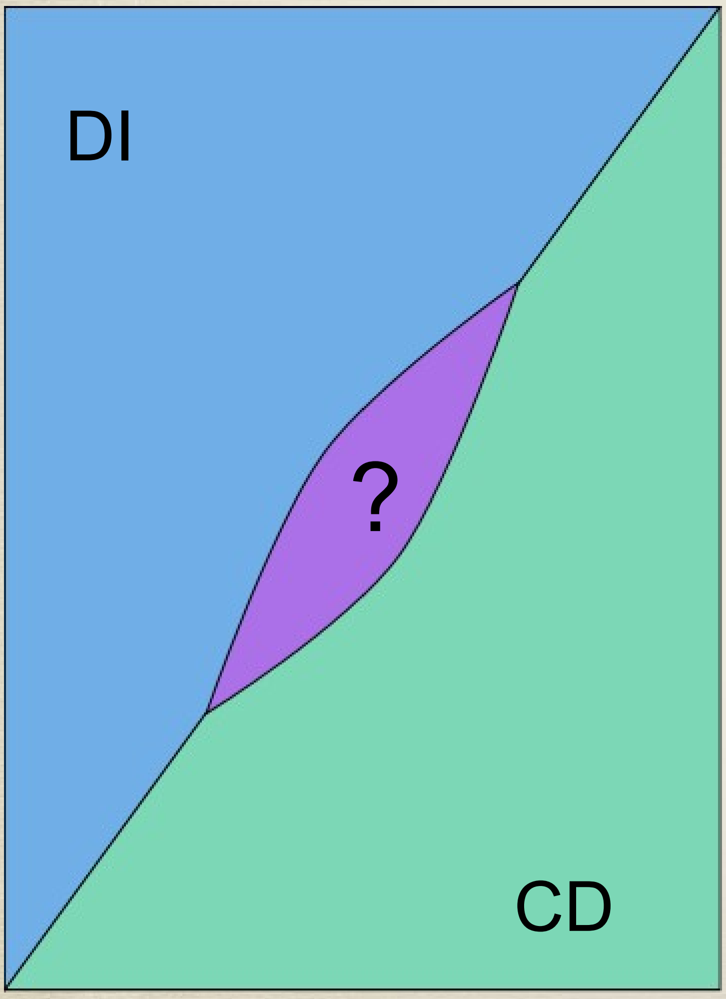


[S. Pironio et al, Nature 464, 1021 (2010)
S. Pironio, arXiv:1510.00248]

1. DI assumptions:
   - Separation between the devices
   - Independence of the settings
2. CD requirements:
   - Accurate description of the devices
3. Are these assumptions fulfilled in...
   - DI certification of randomness without space-like separation [Pironio10]?
   - Bell test with settings from Twitter [Pironio15]?

All loopholes don't need to be closed in every DI assessement.

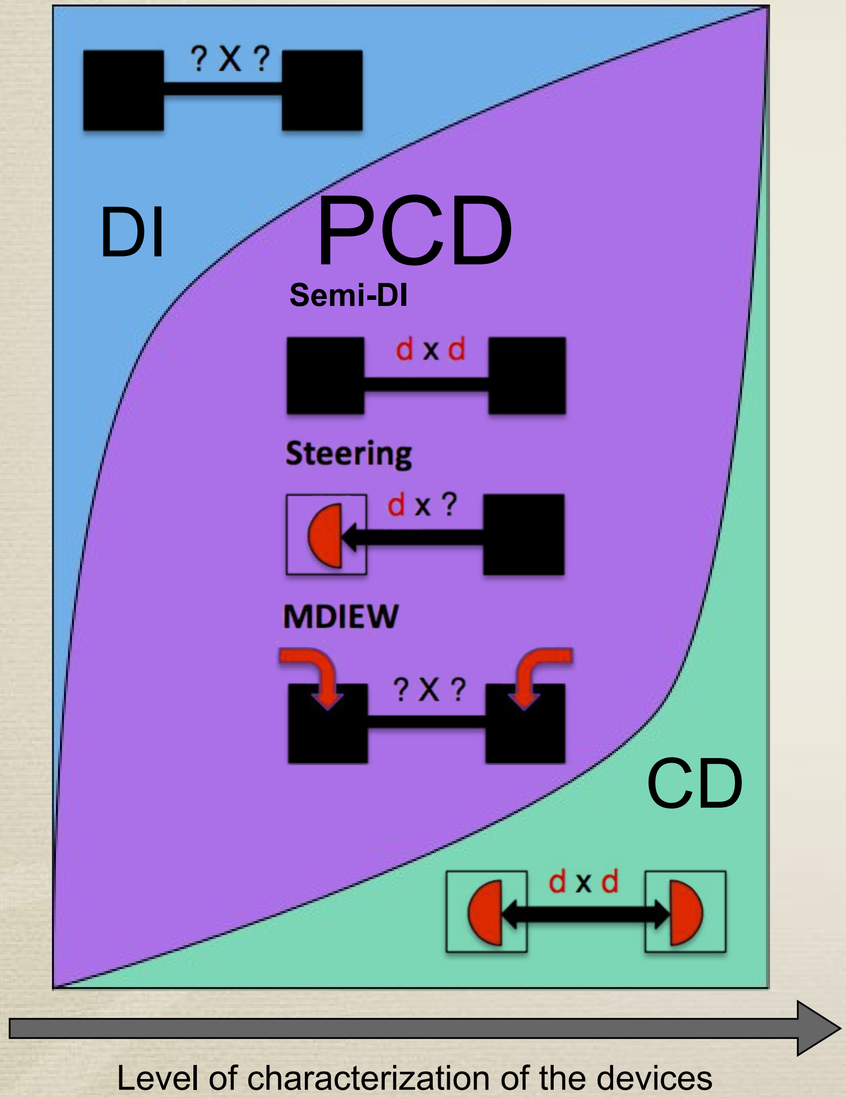
Partially characterized devices (PCD)



We would like robust and optimistic conclusions...

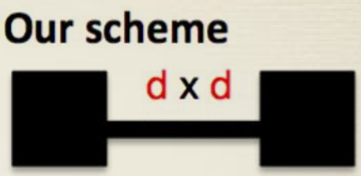
- Rely on fewer assumptions than CD
- Be less demanding than DI

Partially characterized devices (PCD)



1. To trust or not to trust... the description of :
   - Sources
     - Dimension
     - State
   - Measurements
     - Commutation relation
     - Dimension
     - Sharpness
2. When satisfied, such conditions can provide an improvement over both CD and DI

Partially characterized devices (PCD)
Trusting the dimension of the source



1. State is unknown
   - But lives in a space of given dimension
2. Measurements are unknown
3. Statistics

$$P(a,b|x,y) = \mathrm{tr}\left(\rho\, \Pi^A_{a|x} \otimes \Pi^B_{b|y}\right)$$

with $\rho \in \mathcal{L}\left(\mathcal{H}^2 \otimes \mathcal{H}^2\right)$

Partially characterized devices (PCD)
Trusting the dimension of the source

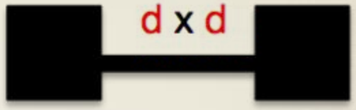
1. Known results:

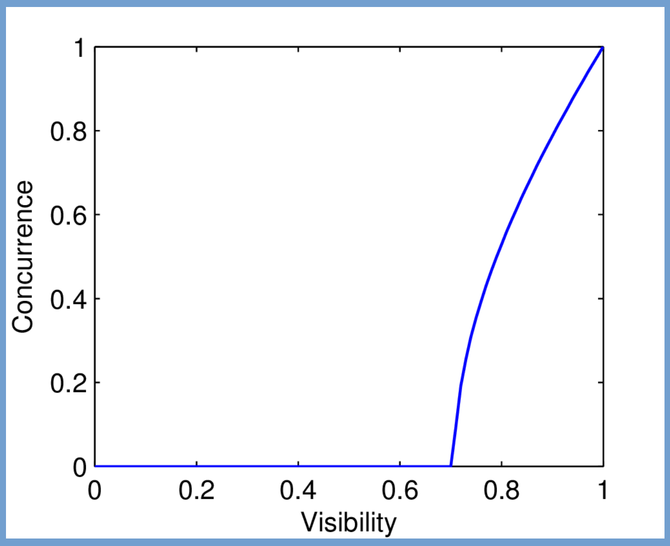
   - Lower bound on the concurrence [VW02, LVB11]

     $$C \geq \mathrm{Re}\left(\sqrt{S^2_{CHSH} - 4}\right)/2$$

   - Upper bounds on entanglement [LVB11]
   - A convex combination of separable correlations can be entangled [MG12]
   - By non-convexity, entanglement certified as soon as W>1/3 for the isotropic case [MG12]

Our scheme





[F. Verstraete and M. Wolf , PRL 89, 170401 (2002)
Y-C. Liang, T. Vertesi and N. Brunner, PRA 83, 022108 (2011)
T. Moroder and O. Gittsovich, PRA 85, 032301 (2012)]

Partially characterized devices (PCD) Trusting the dimension of the source

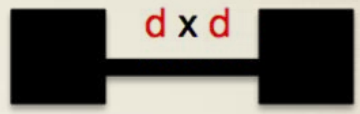
1. Known results:

- Lower bound on the concurrence [VW02, LVB11]

$$C \geq \mathrm{Re}\left(\sqrt{S^2_{CHSH} - 4}\right)/2$$

- Upper bounds on entanglement [LVB11]
- A convex combination of separable correlations can be entangled [MG12]
- By non-convexity, entanglement certified as soon as W>1/3 for the isotropic case [MG12]

Our scheme



$$P(a,b|x,y) = \mathrm{tr}\left(\rho_{\mathrm{sep}}\ \Pi^A_{a|x} \otimes \Pi^B_{b|y}\right)$$

$$P'(a,b|x,y) = \mathrm{tr}\left(\rho'_{\mathrm{sep}}\ \Pi'^A_{a|x} \otimes \Pi'^B_{b|y}\right)$$

$$\bar{\rho}_{\mathrm{sep}} = \frac{\rho_{\mathrm{sep}} + \rho'_{\mathrm{sep}}}{2}$$ well-defined

But $\Pi^{A/B}$ and $\Pi'^{A/B}$ may not be reconciliable...

[F. Verstraete and M. Wolf , PRL 89, 170401 (2002)
Y-C. Liang, T. Vertesi and N. Brunner, PRA 83, 022108 (2011)
T. Moroder and O. Gittsovich, PRA 85, 032301 (2012)]

Method

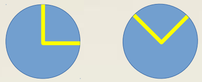
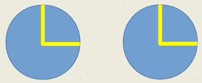
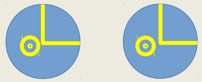
- We perform the following optimization:

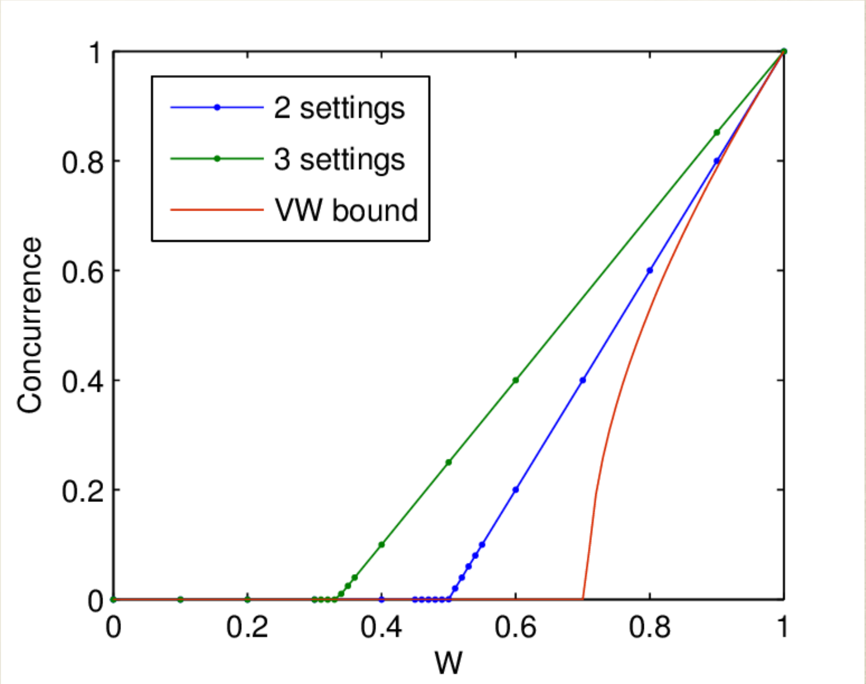
$$c(p) := \min_{\rho,\Pi_x^a,\Pi_y^b} C(\rho),$$

$$\begin{aligned} s.t.\ \ & p(a,b|x,y) = \mathrm{tr}\left(\rho \cdot \Pi_x^a \otimes \Pi_y^b\right) \ \ \forall x,y,a \,\&\, b, \\ & \sum_a \Pi_x^a = \sum_b \Pi_y^b = \mathbb{I} \ \ \forall x \,\&\, y, \\ & \Pi_x^a, \Pi_y^b \geq 0 \ \ \forall x,y,a \,\&\, b, \\ & \rho \in \mathcal{L}\left(\mathcal{H}^2 \otimes \mathcal{H}^2\right). \end{aligned}$$

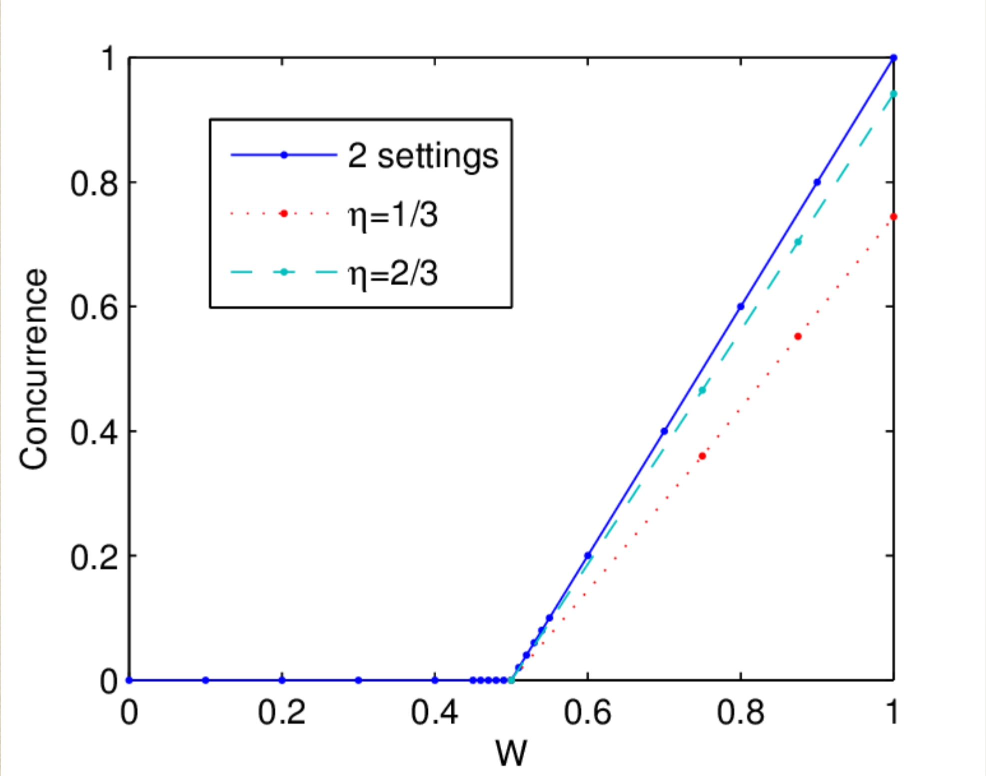
- Non-linear objective function, non-convex optimization set
- Few free parameters, so can be tackled by heuristic numerical optimization for small dimension
- Explicit optimization -> solution is tight

Werner state

- Measure state $\rho = W|\phi^+\rangle\langle\phi^+| + (1-W)\mathbb{I}/4$
- With:
  - CHSH settings 
  - BB84 settings 
  - 6-state settings 
- Moroder-Gittsovich thresholds recovered
- No advantage in testing a Bell inequality
- Exact concurrence of the state certified
- For W=1, both the state and measurements are perfectly self-tested

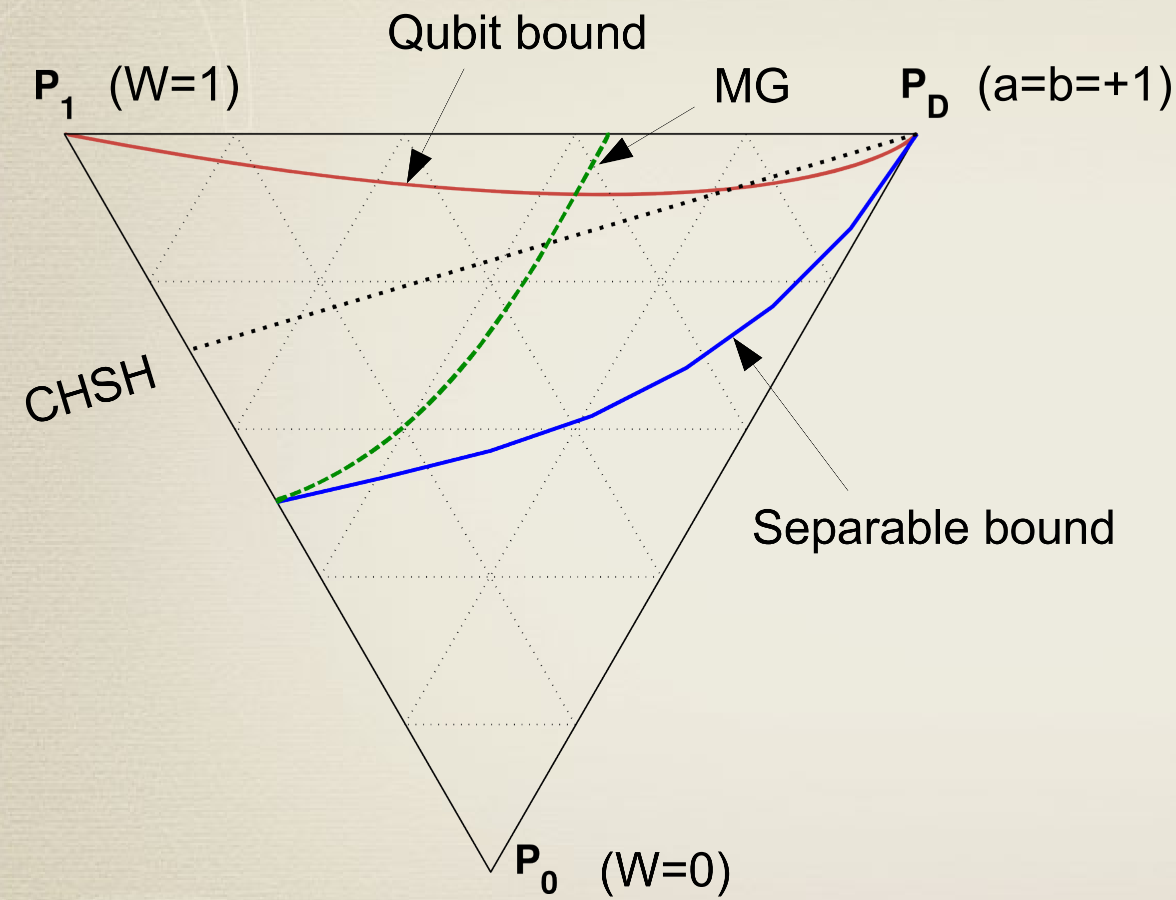


Finite detection efficiency



- eta_A = eta_B = 1/3, 2/3
- 3-outcome statistics
- Amount of certified entanglement reduces
- Entanglement detection threshold is not affected

Slice of the 2222 polytope



- Qubit set is not convex [DW15]
- Some local points cannot be obtained with qubit measurements
- Clear difference with DI certification
- Moroder-Gittsovich bound optimal when the marginals are uniform

[J. M. Donohue, E. Wolf, arXiv:1506.01119
T. Moroder and O. Gittsovich, PRA 85, 032301 (2012)]

Tomographically-complete SIC-POVM

- Measure state

$$|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$$

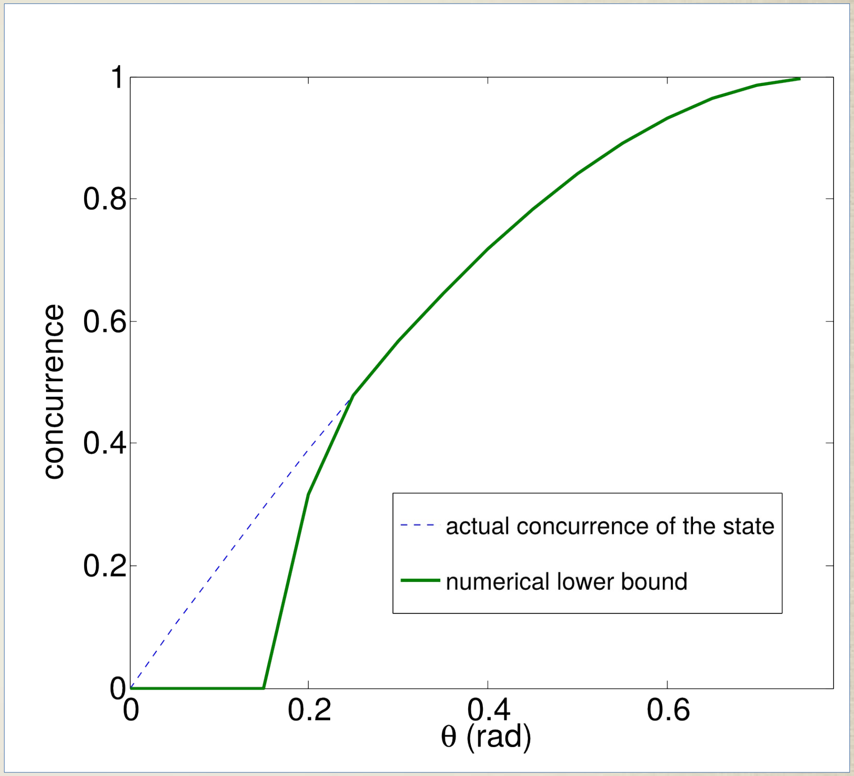
- With

$$\Sigma_0 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}, \ \Sigma_1 = \begin{pmatrix} \frac{1}{6} & \frac{1}{3\sqrt{2}} \\ \frac{1}{3\sqrt{2}} & \frac{1}{3} \end{pmatrix}$$

$$\Sigma_2 = \begin{pmatrix} \frac{1}{6} & \frac{\chi}{3\sqrt{2}} \\ \frac{\chi^*}{3\sqrt{2}} & \frac{1}{3} \end{pmatrix}, \ \Sigma_3 = \begin{pmatrix} \frac{1}{6} & \frac{\chi^*}{3\sqrt{2}} \\ \frac{\chi}{3\sqrt{2}} & \frac{1}{3} \end{pmatrix}$$

- The state is entangled for all theta>0

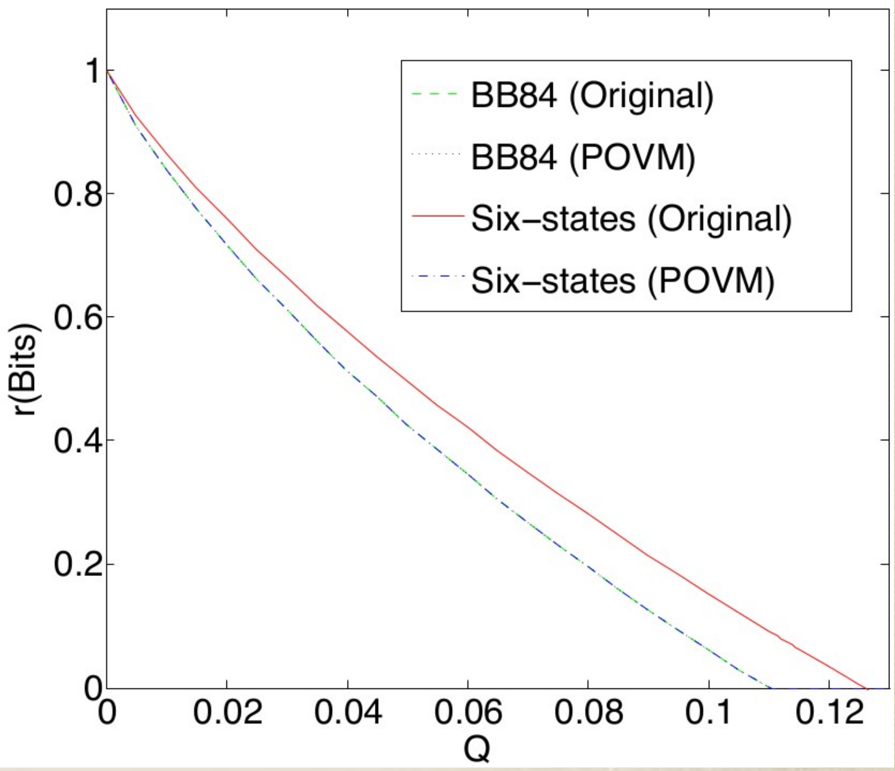
- Separable qubit state and measurements can reproduce the statistics for small theta



Semi-DI is not equivalent to CD

Application to QKD

- Optimization of the key rate
$$r = 1 - h(Q) - \chi(A:E)$$
- Relaxation of the measurement assumption doesn't affect the BB84 keyrate [GM12, W15]
- 6-state protocol key rate becomes BB84 one
- Critical detection efficiency of 84% for BB84
- Does this advantage remain in more sophisticated security proofs?



[O. Gittsovich and T. Moroder, proceedings of the QCMC 2012 conference
E. Woodhead, arXiv:1512.03387
M. Pawlowski and N. Brunner, PRA 84, 010302 (2011)]

Conclusion

- A lot of the certifying power lost in the DI framework can be recovered with an hypothesis on the dimension
- No hypothesis on the measurements required
- The De Finetti theorem applies to finite dimensional systems
  - Easy application to the non-iid case?
- Better techniques needed to describe the non-convex set of correlations with fixed dimension
  - Find an efficient relaxation of the qubit set?
- Other partial characterization of the devices allowing for comparable advantages?

Thank you for your attention.