Geometry of the quantum set of correlations and its implications for self-testing and device-independent cryptography

Jędrzej Kaniewski
University of Warsaw
jkaniewski.fuw.edu.pl

Düsseldorf Quantum Info Seminar
3rd July 2020

Foundation for Polish Science

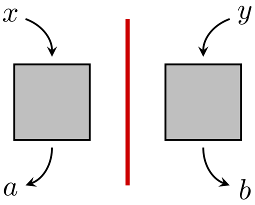
Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

A Bell experiment



$P(a, b|x, y)$

Local-realistic ($\mathcal{L}$): $P(a, b|x, y) = \sum_\lambda p(\lambda) q_A(a|x, \lambda) q_B(b|y, \lambda)$

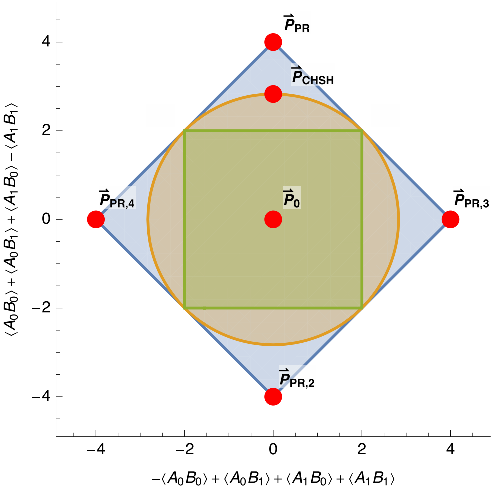
Quantum ($\mathcal{Q}$): $P(a, b|x, y) = \mathrm{tr}\left[(P_a^x \otimes Q_b^y)\rho_{AB}\right]$

No-signalling ($\mathcal{NS}$): $\sum_b P(a, b|x, y) = \sum_b P(a, b|x, y')$

$\sum_a P(a, b|x, y) = \sum_a P(a, b|x', y)$

A Bell experiment

The simplest non-trivial Bell scenario corresponds to 2 players, 2 settings, 2 outcomes and is usually referred to as the **Clauser–Horne–Shimony–Holt (CHSH)** scenario.



$\mathcal{L}$: local set

$\mathcal{Q}$: quantum set

$\mathcal{NS}$: no-signalling set

(2-dimensional slice of 8-dimensional objects)

Self-testing of quantum devices

Self-testing (rigidity) statement:

"In quantum mechanics the probabilities $P(a,b|x,y)$ can be achieved in an essentially unique manner"

or

"Once you observe the probabilities $P(a,b|x,y)$, you know exactly how the devices work!"

(a) "essentially unique" means up to auxiliary degrees of freedom and choice of local bases

(b) this can only hold for points which are extremal in $\mathcal{Q}$

(c) sometimes phrased as "if we observe the maximal violation of Bell inequality"

Self-testing is a type of **device-independent certification**

Self-testing of quantum devices

- Let A_x, B_y be observables of Alice and Bob, respectively, whose outcomes are $\{+1, -1\}$. The CHSH functional reads

$$\beta := \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle.$$

- Well known that $\beta_{\mathcal{L}} = 2$ and $\beta_{\mathcal{Q}} = 2\sqrt{2}$.
- Any quantum realisation (ρ_{AB}, A_x, B_y) that achieves $\beta = 2\sqrt{2}$ is equivalent (up to local unitaries on A and B) to

$$\begin{aligned} \rho_{AB} &= \Phi^+_{A'B'} \otimes \tau_{A''B''}, \\ A_0 &= \mathsf{X} \otimes \mathbb{1} \qquad B_0 = \frac{\mathsf{X} + \mathsf{Z}}{\sqrt{2}} \otimes \mathbb{1}, \\ A_1 &= \mathsf{Z} \otimes \mathbb{1} \qquad B_1 = \frac{\mathsf{X} - \mathsf{Z}}{\sqrt{2}} \otimes \mathbb{1}, \end{aligned}$$

where $|\Phi^+\rangle := \big(|00\rangle + |11\rangle\big)/\sqrt{2}$.[1]

[1] [Tsirelson '87], [Summers and Werner '87], [Popescu and Rohrlich '92]

Device-independent cryptography

- The goal of entanglement-based **quantum key distribution (QKD)** is for Alice and Bob to distill secure key using an untrusted shared state.
- In **standard QKD** Alice and Bob trust their measurement devices:

$$A_0 = B_0 = \mathsf{X} \quad \text{and} \quad A_1 = B_1 = \mathsf{Z}.$$

  If they observe

$$\operatorname{tr}(A_0 \otimes B_0 \, \rho_{AB}) = \operatorname{tr}(A_1 \otimes B_1 \, \rho_{AB}) = 1,$$

  they can immediately deduce that $\rho_{AB} = \Phi^+_{AB}$. Since ρ_{AB} is pure, Eve is uncorrelated and the randomness generated is secure.
- In the **device-independent** version Alice and Bob do not trust their measurement devices. Nevertheless, they can use self-testing to prove that they basically perform rank-1 projective measurements on a singlet. Purity of the **relevant part of their state** ensures that Eve is uncorrelated.

Summary

The maximal violation of a "typical" Bell inequality:

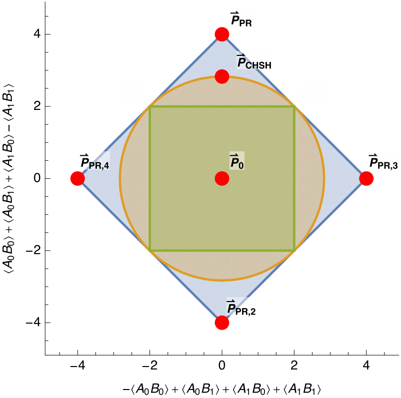
- is achieved by a unique probability point
- completely characterises the state and measurements (up to simple, well-understood equivalences)
- therefore, it can be used to guarantee security of device-independent cryptography

In this talk I will give explicit examples of objects which do not follow this simple pattern

Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

Geometry of the quantum set



The quantum set looks "simple", one might conjecture that:

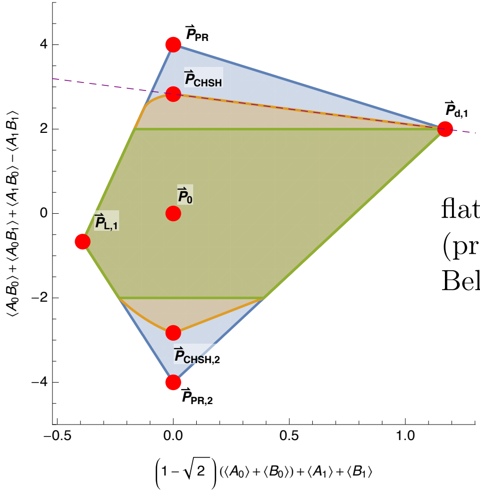
(a) the non-trivial part of the boundary has no flat regions

(b) for every extremal point there exists an exposing functional

(c) non-trivial Bell functionals have unique maximisers

Geometry of the quantum set

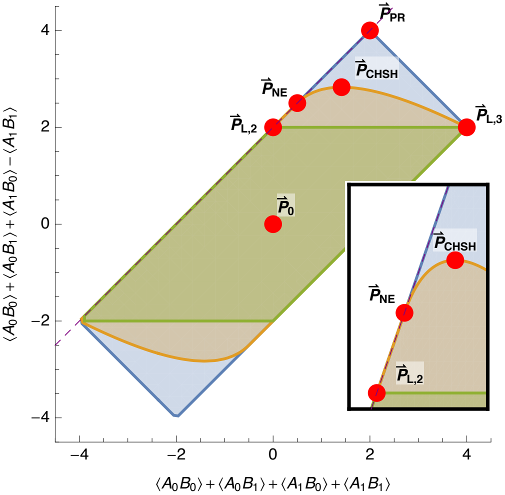
However, counterexamples are easy to find already in the simplest non-trivial Bell scenario[2]



flat region on the boundary (proven by finding the right Bell functional)

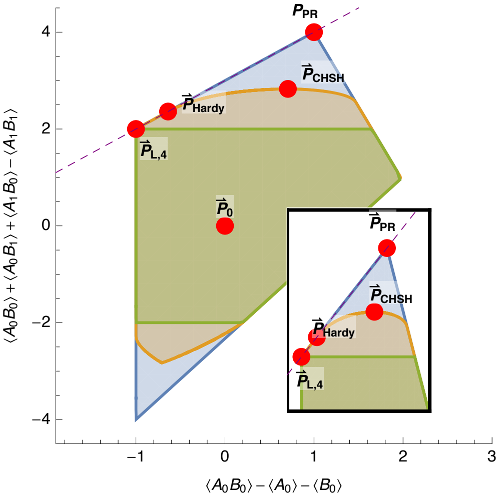
[2] [Goh, K, Wolfe, Vértesi, Wu, Cai, Liang, Scarani, PRA 2018]

Geometry of the quantum set



P_{NE} is extremal but not exposed (proven using analytic characterisation)

Geometry of the quantum set



P_{Hardy} is extremal but not exposed (proven using linear programming)

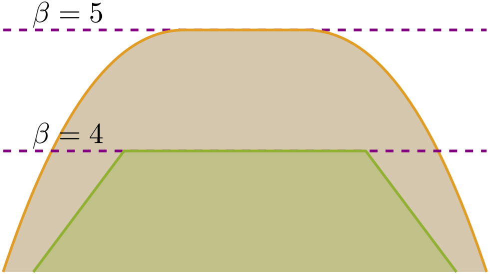
$\implies$ cannot find a Bell inequality maximally violated only by P_{Hardy}

Geometry of the quantum set

For non-uniqueness of maximisers consider the bipartite scenario with 3 settings and 2 outcomes:

$$\beta = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_0 B_2 \rangle + \langle A_1 B_0 \rangle + \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_0 \rangle - \langle A_2 B_1 \rangle$$

Easy to show that $\beta_{\mathcal{L}} = 4$, $\beta_{\mathcal{Q}} = 5$, $\beta_{\mathcal{NS}} = 8$



entire segment can be realised by projective measurements on $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$

$\beta = 5$ **will not** certify observables, but **might** be sufficient to certify the state

Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

A weak form of self-testing

Result: For the functional

$$\beta = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_0 B_2 \rangle + \langle A_1 B_0 \rangle + \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_0 \rangle - \langle A_2 B_1 \rangle .$$

there exists a 1-parameter family of 2-qubit realisations that achieves $\beta = 5$. Every realisation that achieves the maximal violation is a convex combination of those. The set of probability points achieving $\beta = 5$ is a line segment.[3]

For these 2-qubit realisations:

- the state is always $|\Phi^+\rangle$
- the measurements are always rank-1 projective; the angle between A_0 and A_1 is fixed, but there is some freedom in choosing A_2

[3] [K, arXiv:1910.00706]

A weak form of self-testing

Conclusions:

- the maximal violation certifies the maximally entangled state of 2 qubits (and this can be made robust)
- the maximal violation partially determines the arrangement of observables
- the maximal violation certifies that the randomness generated is unknown to Eve, can be used e.g. for QKD
- rigidity is not necessary for device-independent cryptography (it is not necessary to fully characterise the devices, partial characterisation might be sufficient)

Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

An extremal non-rigid point based on MUBs

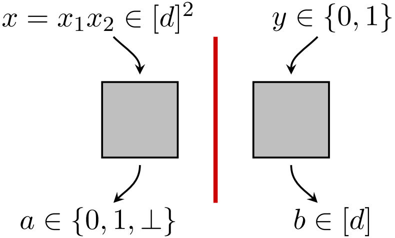
Question: Are all extremal points of the quantum set self-tests?

Seemingly unrelated question: Can we construct a Bell inequality maximally violated by a pair of mutually unbiased bases (MUBs) in dimension d?

Yes! (and it has some interesting properties)[4]

[4] [Tavakoli, Farkas, Rosset, Bancal, K, `arXiv:1912.03225`]

An extremal non-rigid point based on MUBs



$d \geq 2$

$[d] := \{0, 1, \ldots, d-1\}$

inputs chosen uniformly

$$\beta := \sum_{xy} P(a = y \wedge b = x_y | x, y) - P(a = 1 - y \wedge b = x_y | x, y)$$
$$- \gamma_d \sum_{x} \big(P(a = 0 | x) + P(a = 1 | x) \big) \quad \text{for} \quad \gamma_d := \sqrt{1 - d^{-1}}/2$$

- If $a = \perp$ no points are won or lost regardless of Bob's actions
- If $a \in \{0, 1\}$ the game is played: a fixed "fee" is deducted and further points might be won or lost

An extremal non-rigid point based on MUBs

The Bell functional might look complicated

$$\beta = \sum_{xy} P(a = y \wedge b = x_y | x, y) - P(a = 1 - y \wedge b = x_y | x, y)$$
$$- \gamma_d \sum_x \big(P(a = 0|x) + P(a = 1|x) \big) \quad \text{for} \quad \gamma_d := \sqrt{1 - d^{-1}}/2$$

but the resulting Bell operator is simple

$$W = \sum_x \big[(A_0^x - A_1^x) \otimes (P_{x_0} - Q_{x_1}) - \gamma_d (A_0^x + A_1^x) \otimes \mathbb{1} \big]$$

where $\{A_a^x\}$ are the measurement operators of Alice and $\{P_b\}$ and $\{Q_b\}$ represent the two measurements of Bob

This Bell operator is simple enough so that a **tight bound on the quantum value** can be computed **analytically**

An extremal non-rigid point based on MUBs

Quantum realisation achieving the quantum value:

- Alice and Bob share $|\Phi_d^+\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$
- Bob performs measurements in two mutually unbiased bases $\{P_b\}$ and $\{Q_b\}$
- Alice's measurements are determined by the spectral decomposition of

$$P_{x_0} - Q_{x_1} = \sqrt{\frac{d-1}{d}} \big(|e^0_{x_0 x_1}\rangle\langle e^0_{x_0 x_1}| - |e^1_{x_0 x_1}\rangle\langle e^1_{x_0 x_1}| \big).$$

$$A^x_j = \big(|e^j_{x_0 x_1}\rangle\langle e^j_{x_0 x_1}| \big)^{\mathrm{T}} \quad \text{for} \quad j \in \{0,1\},$$
$$A^x_\perp = \mathbb{1} - A^x_0 - A^x_1.$$

- The maximal violation can be achieved by **any pair of MUBs** in dimension d: since in some dimensions there exist inequivalent pairs of MUBs this inequality **cannot be a self-test**!

An extremal non-rigid point based on MUBs

What can we actually deduce if we observe the maximal violation?

- The shared state ρ_{AB} **contains** Φ_d^+
- The measurements of Bob satisfy **sandwich relations**

$$P_u Q_v P_u = \frac{1}{d} P_u \quad \text{and} \quad Q_v P_u Q_v = \frac{1}{d} Q_v$$

which turn out to be equivalent to

$$\langle\psi|P_u|\psi\rangle = 1 \implies \langle\psi|Q_v|\psi\rangle = \frac{1}{d},$$
$$\langle\psi|Q_v|\psi\rangle = 1 \implies \langle\psi|P_u|\psi\rangle = \frac{1}{d},$$

"operational definition of MUBs"

- $\{P_u\}$ and $\{Q_v\}$ are not necessarily (direct sums of) MUBs

Finally, the maximal violation is achieved by a unique probability point $\implies$ **non-rigid exposed point of the quantum set**

An extremal non-rigid point based on MUBs

Outline

- Preliminaries
- Geometry of the quantum set
- A weak form of self-testing
- An extremal non-rigid point based on mutually unbiased bases
- Summary and open questions

Summary and open questions

Summary:

- The quantum set is a convex set with highly non-trivial geometry even in the simplest Bell scenario.
- The maximal violation of a Bell inequality can certify the state but only partially characterise the measurements. Such inequalities can still be used for device-independent cryptography.
- There exist extremal points of the quantum set which are not rigid.

Open questions:

- Can we find a bipartite Bell inequality maximally violated by inequivalent states? (tripartite examples are known)
- Which extremal points of the quantum set are self-tests? What is the generic behaviour?
- Can we define an elegant hierarchy of relaxed self-testing criteria?

Thank you for your attention!