Robust self-testing of quantum devices

Jędrzej Kaniewski

QMATH, Department of Mathematical Sciences

University of Copenhagen, Denmark

University of Basel

28 November 2017

Outline

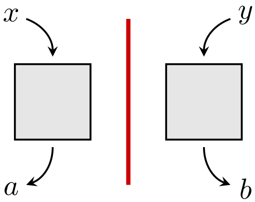
- Bell nonlocality
- Self-testing
- Robust self-testing
- Summary and open questions

Outline

- Bell nonlocality
- Self-testing
- Robust self-testing
- Summary and open questions

Bell nonlocality

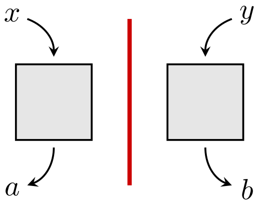
Bell scenario



$$\Pr[a, b|x, y]$$

Bell nonlocality

Bell scenario



$\Pr[a, b|x, y]$

Def.: $\Pr[a, b|x, y]$ is **local** if

$$\Pr[a, b|x, y] = \sum_{\lambda} p(\lambda)\, p_A(a|x, \lambda)\, p_B(b|y, \lambda).$$

Otherwise $\implies$ **nonlocal** or it **violates (some) Bell inequality**

Bell nonlocality

Obs.: Separable states give local statistics (for all measurements)

$$\rho_{AB} = \sum_{\lambda} p_\lambda \sigma_\lambda \otimes \tau_\lambda,$$

$$\Pr[a,b|x,y] = \mathrm{tr}\left[(F_a^x \otimes G_b^y)\rho_{AB}\right] = \sum_{\lambda} p_\lambda \cdot \underbrace{\mathrm{tr}\left(F_a^x \sigma_\lambda\right)}_{p_A(a|x,\lambda)} \cdot \underbrace{\mathrm{tr}\left(G_b^y \tau_\lambda\right)}_{p_B(b|y,\lambda)}.$$

Bell nonlocality

$$\rho_{AB} \text{ is separable} \implies \text{statistics are } \textbf{local}$$

$$\Pr[a,b|x,y] \text{ is } \textbf{nonlocal} \implies \rho_{AB} \text{ is entangled}$$

Bell nonlocality

$$\rho_{AB} \text{ is separable} \implies \text{statistics are } \textbf{local}$$

$$\Pr[a,b|x,y] \text{ is } \textbf{nonlocal} \implies \rho_{AB} \text{ is entangled}$$

Question: can we make any more refined statements?

Bell nonlocality

ρ_{AB} is separable $\implies$ statistics are **local**

$\Pr[a, b|x, y]$ is **nonlocal** $\implies$ ρ_{AB} is entangled

Question: can we make any more refined statements?

Answer: self-testing

Outline

- Bell nonlocality
- Self-testing
- Robust self-testing
- Summary and open questions

Self-testing

Self-testing

Given $\Pr[a,b|x,y] = \mathrm{tr}\left[(F_a^x \otimes G_b^y)\rho_{AB}\right]$

deduce properties of ρ_{AB}, $\{F_a^x\}$, $\{G_b^y\}$

Self-testing

Self-testing

Given $\Pr[a,b|x,y] = \mathrm{tr}\left[(F_a^x \otimes G_b^y)\rho_{AB}\right]$

deduce properties of ρ_{AB}, $\{F_a^x\}$, $\{G_b^y\}$

(i) we do not assume that ρ_{AB} is pure
or that the measurements are projective
(we want to rigorously deduce it!)

Self-testing

Self-testing

Given $\Pr[a,b|x,y] = \mathrm{tr}\left[(F_a^x \otimes G_b^y)\rho_{AB}\right]$

deduce properties of ρ_{AB}, $\{F_a^x\}$, $\{G_b^y\}$

(i) we do not assume that ρ_{AB} is pure
or that the measurements are projective
(we want to rigorously deduce it!)

(ii) often only promised some Bell violation

$$\sum_{abxy} c_{ab}^{xy} \Pr[a,b|x,y] = \beta$$

Self-testing

Measurement: resolution of $\mathbb{1}$ into positive semidefinite operators

Self-testing

Measurement: resolution of $\mathbb{1}$ into positive semidefinite operators

Measurements with **two outcomes**, i.e.

$$\begin{aligned} F_j &= F_j^\dagger, \\ F_j &\geq 0, \\ F_0 + F_1 &= \mathbb{1} \end{aligned}$$

Self-testing

Measurement: resolution of $\mathbb{1}$ into positive semidefinite operators

Measurements with **two outcomes**, i.e.

$$\begin{aligned} F_j &= F_j^\dagger, \\ F_j &\geq 0, \\ F_0 + F_1 &= \mathbb{1} \end{aligned}$$

are conveniently written as **observables**

$$A = F_0 - F_1.$$

Self-testing

Measurement: resolution of $\mathbb{1}$ into positive semidefinite operators

Measurements with **two outcomes**, i.e.

$$\begin{aligned} F_j &= F_j^\dagger, \\ F_j &\geq 0, \\ F_0 + F_1 &= \mathbb{1} \end{aligned}$$

are conveniently written as **observables**

$$A = F_0 - F_1.$$

This mapping is one-to-one: any A such that

$$A = A^\dagger \quad \text{and} \quad -\mathbb{1} \leq A \leq \mathbb{1}.$$

defines a valid measurement

Self-testing

Example: the CHSH inequality [1, 2]

$$\beta := \mathrm{tr}\left(W\rho_{AB}\right) \quad \text{for} \quad W := A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)$$

Classically $\beta \leq 2$, but quantumly we can reach up to $2\sqrt{2}$

Self-testing

Example: the CHSH inequality [1, 2]

$$\beta := \operatorname{tr}\left(W\rho_{AB}\right) \quad \text{for} \quad W := A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)$$

Classically $\beta \leq 2$, but quantumly we can reach up to $2\sqrt{2}$

$$|\Phi_{A'B'}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$A_0 = \sigma_x, \quad B_0 = \frac{\sigma_x + \sigma_z}{\sqrt{2}},$$

$$A_1 = \sigma_z, \quad B_1 = \frac{\sigma_x - \sigma_z}{\sqrt{2}}.$$

canonical realisation

Self-testing

CHSH is a self-test, i.e. every realisation that achieves $\beta = 2\sqrt{2}$ is **equivalent** to the canonical one.

Self-testing

CHSH is a self-test, i.e. every realisation that achieves $\beta = 2\sqrt{2}$ is **equivalent** to the canonical one.

$$\rho_{AB} = \Phi_{A'B'}$$

$$A_0 = \sigma_x \qquad B_0 = \frac{\sigma_x+\sigma_z}{\sqrt{2}}$$

$$A_1 = \sigma_z \qquad B_1 = \frac{\sigma_x-\sigma_z}{\sqrt{2}}$$

Self-testing

CHSH is a self-test, i.e. every realisation that achieves $\beta = 2\sqrt{2}$ is **equivalent** to the canonical one.

$$\rho_{AB} = \Phi_{A'B'} \otimes \tau_{A''B''}$$

$$A_0 = \sigma_x \otimes \mathbb{1} \qquad B_0 = \tfrac{\sigma_x + \sigma_z}{\sqrt{2}} \otimes \mathbb{1}$$

$$A_1 = \sigma_z \otimes \mathbb{1} \qquad B_1 = \tfrac{\sigma_x - \sigma_z}{\sqrt{2}} \otimes \mathbb{1}$$

Inherent limitations

- cannot see auxiliary systems (ignored by measurements)

Self-testing

CHSH is a self-test, i.e. every realisation that achieves $\beta = 2\sqrt{2}$ is **equivalent** to the canonical one.

$$\rho_{AB} = U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger \qquad \text{for } U = U_A \otimes U_B$$

$$A_0 = U_A\big(\sigma_x \otimes \mathbb{1}\big)U_A^\dagger \qquad B_0 = U_B\big(\tfrac{\sigma_x+\sigma_z}{\sqrt{2}} \otimes \mathbb{1}\big)U_B^\dagger$$

$$A_1 = U_A\big(\sigma_z \otimes \mathbb{1}\big)U_A^\dagger \qquad B_1 = U_B\big(\tfrac{\sigma_x-\sigma_z}{\sqrt{2}} \otimes \mathbb{1}\big)U_B^\dagger$$

Inherent limitations

- cannot see auxiliary systems (ignored by measurements)
- cannot see local unitaries

Self-testing

CHSH is a self-test, i.e. every realisation that achieves $\beta = 2\sqrt{2}$ is **equivalent** to the canonical one.

$$\rho_{AB} = U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger \qquad \text{for } U = U_A \otimes U_B$$

$$A_0 = U_A\big(\sigma_x \otimes \mathbb{1}\big)U_A^\dagger \qquad B_0 = U_B\big(\tfrac{\sigma_x+\sigma_z}{\sqrt{2}} \otimes \mathbb{1}\big)U_B^\dagger$$

$$A_1 = U_A\big(\sigma_z \otimes \mathbb{1}\big)U_A^\dagger \qquad B_1 = U_B\big(\tfrac{\sigma_x-\sigma_z}{\sqrt{2}} \otimes \mathbb{1}\big)U_B^\dagger$$

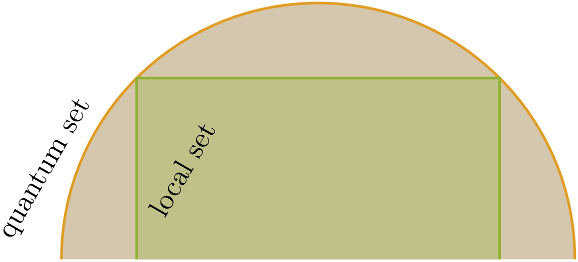
Inherent limitations

- cannot see auxiliary systems (ignored by measurements)
- cannot see local unitaries

"CHSH is rigid"

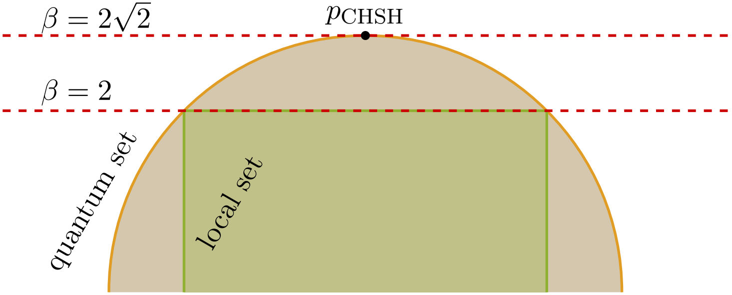
Self-testing

Rigidity is related to the **geometry of the quantum set of correlations**, e.g. for the CHSH inequality we have



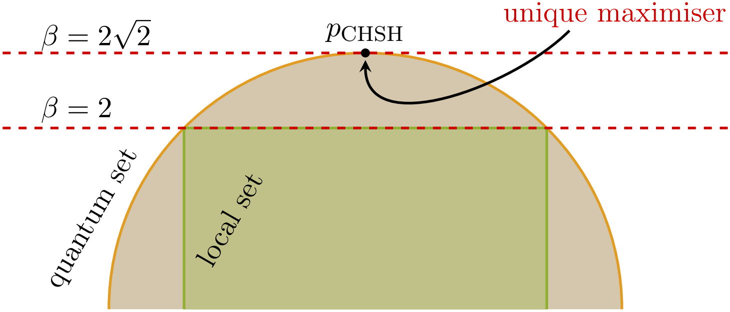
Self-testing

Rigidity is related to the **geometry of the quantum set of correlations**, e.g. for the CHSH inequality we have



Self-testing

Rigidity is related to the **geometry of the quantum set of correlations**, e.g. for the CHSH inequality we have

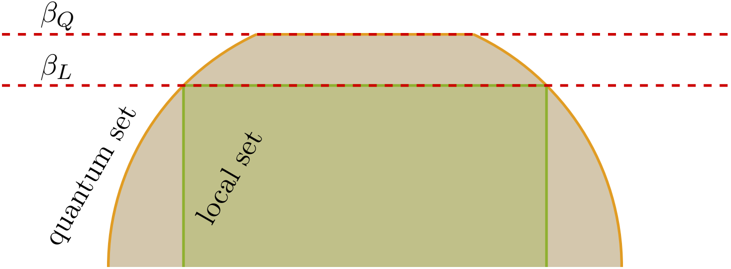


Self-testing

but for some other inequalities [3, 4, 5]

Self-testing

but for some other inequalities [3, 4, 5]



no unique maximiser $\implies$ no rigidity statement

Self-testing

Rigidity has been shown for:

- CHSH inequality [1, 2]
- tilted/biased CHSH inequality [6, 7, 8]
- chained Bell inequalities [9]
- tripartite Mermin inequality [10], MABK inequalities [8]
- magic square [11] and magic pentagram game [12]
- ...

Self-testing

Rigidity has been shown for:

- CHSH inequality [1, 2]
- tilted/biased CHSH inequality [6, 7, 8]
- chained Bell inequalities [9]
- tripartite Mermin inequality [10], MABK inequalities [8]
- magic square [11] and magic pentagram game [12]
- ...

Exciting, can I see it in an **experiment**?

Outline

- Bell nonlocality
- Self-testing
- Robust self-testing
- Summary and open questions

Robust self-testing

In the lab we **never** measure $\beta = 2\sqrt{2}$

Robust self-testing

In the lab we **never** measure $\beta = 2\sqrt{2}$
(i) no perfect experiments
(ii) finite statistics

Robust self-testing

In the lab we **never** measure $\beta = 2\sqrt{2}$
(i) no perfect experiments
(ii) finite statistics

Instead, we may observe $\beta \approx 2.7$ or 2.4

Robust self-testing

In the lab we **never** measure $\beta = 2\sqrt{2}$
(i) no perfect experiments
(ii) finite statistics

Instead, we may observe $\beta \approx 2.7$ or 2.4

In such a case, we would still expect that the quantum realisation must somehow **resemble** the canonical one

Robust self-testing

In the lab we **never** measure $\beta = 2\sqrt{2}$
(i) no perfect experiments
(ii) finite statistics

Instead, we may observe $\beta \approx 2.7$ or 2.4

In such a case, we would still expect that the quantum realisation must somehow **resemble** the canonical one

What is the right **mathematical formulation** of this statement?

Robust self-testing

Approach 1 (generic): require all equalities to hold up to some ε

$$\begin{aligned}
\beta = 2\sqrt{2} \quad &\Longrightarrow \quad \rho_{AB} = U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger, \\
\beta = 2\sqrt{2} - \varepsilon \quad &\Longrightarrow \quad \left\| \rho_{AB} - U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger \right\|_1 \leq f(\varepsilon).
\end{aligned}$$

Robust self-testing

Approach 1 (generic): require all equalities to hold up to some ε

$$\begin{aligned} \beta = 2\sqrt{2} \quad &\Longrightarrow \quad \rho_{AB} = U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger, \\ \beta = 2\sqrt{2} - \varepsilon \quad &\Longrightarrow \quad \left\| \rho_{AB} - U(\Phi_{A'B'} \otimes \tau_{A''B''})U^\dagger \right\|_1 \leq f(\varepsilon). \end{aligned}$$

In such a stringent formulation $f(\varepsilon)$ grows very fast, non-trivial statement **only for almost maximal violations** (for CHSH only if $\varepsilon < 10^{-4}$)

Might be good enough for complexity-theoretic applications, but is it relevant from the physics point of view?

Robust self-testing

Approach 1 (generic): require all equalities to hold up to some ε

$$\begin{aligned} \beta = 2\sqrt{2} \quad &\Longrightarrow \quad \rho_{AB} = U(\Phi_{A'B'} \otimes \tau_{A''B''})U^{\dagger}, \\ \beta = 2\sqrt{2} - \varepsilon \quad &\Longrightarrow \quad \left\| \rho_{AB} - U(\Phi_{A'B'} \otimes \tau_{A''B''})U^{\dagger} \right\|_1 \leq f(\varepsilon). \end{aligned}$$

In such a stringent formulation $f(\varepsilon)$ grows very fast, non-trivial statement **only for almost maximal violations** (for CHSH only if $\varepsilon < 10^{-4}$)

Might be good enough for complexity-theoretic applications, but is it relevant from the physics point of view?

Approach 2 (specific): choose one particular property and use a measure tailored to certify that property

Robust self-testing

Robust certification of quantum states

$$\rho_{AB} = U(\Psi_{A'B'} \otimes \tau_{A''B''})U^\dagger$$

$$\Longleftrightarrow$$

$$\exists \Lambda_A : A \to A',$$

$$\Lambda_B : B \to B'$$

$$\text{s.t.} \quad (\Lambda_A \otimes \Lambda_B)(\rho_{AB}) = \Psi_{A'B'}$$

Robust self-testing

Robust certification of quantum states

$$\rho_{AB} = U(\Psi_{A'B'} \otimes \tau_{A''B''})U^\dagger$$

$$\Longleftrightarrow$$

$$\exists \Lambda_A : A \to A',$$

$$\Lambda_B : B \to B'$$

$$\text{s.t.} \quad (\Lambda_A \otimes \Lambda_B)(\rho_{AB}) = \Psi_{A'B'}$$

If cannot extract a **perfect** copy, then...?

Robust self-testing

Extractability of $\Psi_{A'B'}$ from ρ_{AB} [13, 14]

$$\Xi(\rho_{AB} \to \Psi_{A'B'}) := \max_{\Lambda_A, \Lambda_B} F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big)$$

local extraction channels

fidelity

Robust self-testing

Extractability of $\Psi_{A'B'}$ from ρ_{AB} [13, 14]

$$\Xi(\rho_{AB} \to \Psi_{A'B'}) := \max_{\Lambda_A, \Lambda_B} F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big)$$

local extraction channels

fidelity

Obs1: $\Xi(\rho_{AB} \to \Psi_{A'B'}) = 1 \iff \rho_{AB} = U(\Psi_{A'B'} \otimes \sigma_{A''B''})U^\dagger$

Robust self-testing

Extractability of $\Psi_{A'B'}$ from ρ_{AB} [13, 14]

$$\Xi(\rho_{AB} \to \Psi_{A'B'}) := \max_{\Lambda_A, \Lambda_B} F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big)$$

local extraction channels

fidelity

Obs1: $\Xi(\rho_{AB} \to \Psi_{A'B'}) = 1 \iff \rho_{AB} = U(\Psi_{A'B'} \otimes \sigma_{A''B''})U^\dagger$

Obs2: $\Xi(\rho_{AB} \to \Psi_{A'B'}) \in [\lambda_{\max}^2, 1]$

largest Schmidt coefficient

Robust self-testing

Extractability is an operational quantity – once we have a good quality singlet, we can use it for any task for which a perfect singlet can be used

Given a state $\sigma_{AB} \in \mathcal{S}(\mathbb{C}^d \otimes \mathbb{C}^d)$ the **singlet fraction** is defined as

$$\max_{U=U_A \otimes U_B} F\big(U\sigma_{AB}U^\dagger, \Phi^d_{AB}\big)$$

for $\Phi^d = \frac{1}{\sqrt{d}} \sum_j |j\rangle|j\rangle$

Singlet fraction captures how useful σ_{AB} is for **teleporting a qudit** [15]

Extractability is a slightly more general notion (can deal with dimension mismatch), but has similar operational significance

Robust self-testing

In this formulation the goal is to derive **lower bounds**

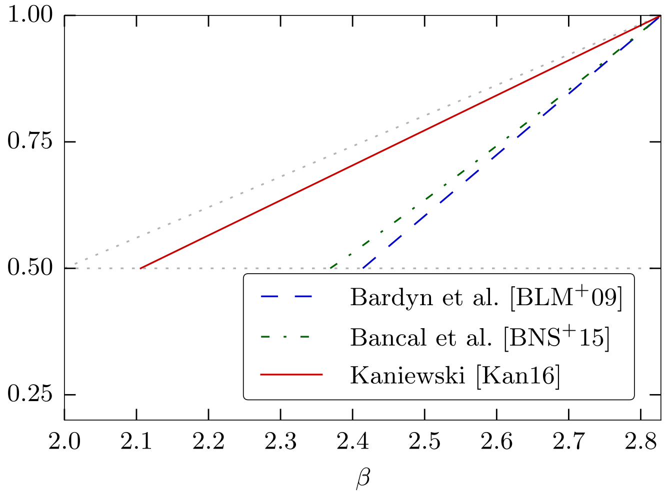
$$\Xi(\rho_{AB} \to \Psi_{A'B'}) \geq f(\beta)$$

The bound is **nontrivial** if

$$f(\beta) > \lambda_{\max}^2$$

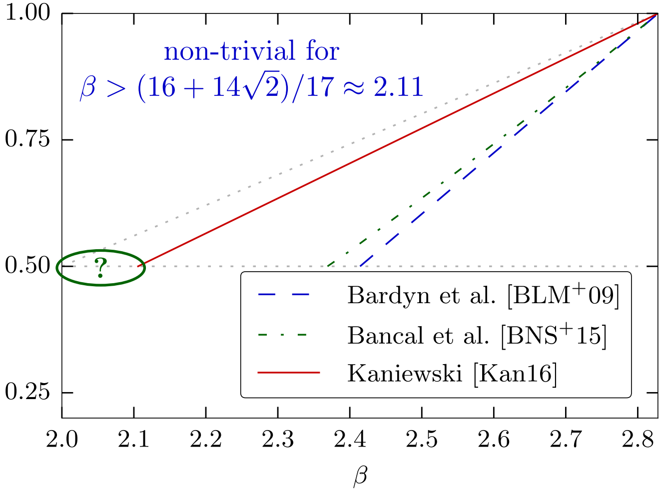
Robust self-testing

Example 1: CHSH inequality ($\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$) [13, 16, 14]
Lower bounds on extractability of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



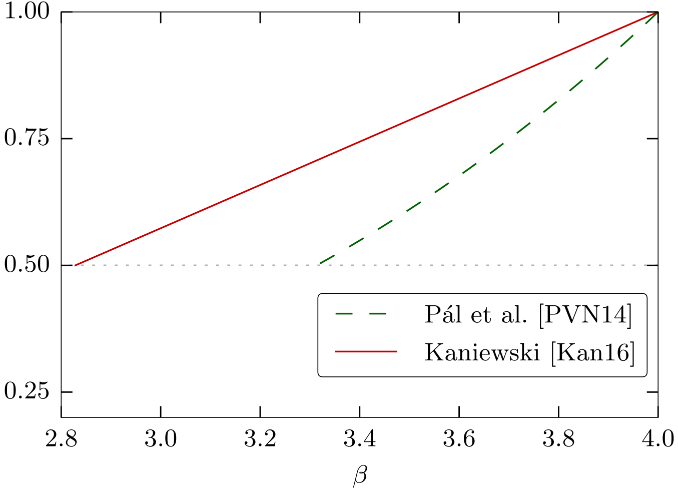
Robust self-testing

Example 1: CHSH inequality ($\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$) [13, 16, 14]
Lower bounds on extractability of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



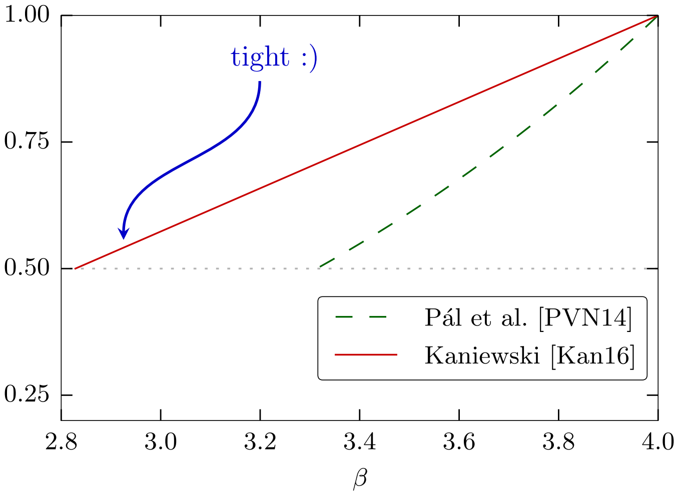
Robust self-testing

Example 2: Mermin inequality ($\beta_C = 2$ and $\beta_Q = 4$) [17, 14]
Lower bounds on extractability of $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$



Robust self-testing

Example 2: Mermin inequality ($\beta_C = 2$ and $\beta_Q = 4$) [17, 14]
Lower bounds on extractability of $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$



Robust self-testing

Certification of measurements

The optimal CHSH measurements

$$A_0 = U_A \big(\sigma_x \otimes \mathbb{1}\big) U_A^\dagger$$
$$A_1 = U_A \big(\sigma_z \otimes \mathbb{1}\big) U_A^\dagger$$

Robust self-testing

Certification of measurements

The optimal CHSH measurements

$$A_0 = U_A(\sigma_x \otimes \mathbb{1})U_A^\dagger$$
$$A_1 = U_A(\sigma_z \otimes \mathbb{1})U_A^\dagger$$

Equivalent formulation in terms of algebraic relations

$$A_0^2 = A_1^2 = \mathbb{1} \qquad \text{(projectiveness)}$$
$$A_0 A_1 + A_1 A_0 = 0 \qquad \text{(anticommutation)}$$

Robust self-testing

Idea: instead of certifying closeness to the canonical realisation certify **algebraic relations between observables** [8]

Convenient because

- it is clear how to measure "approximate" satisfaction of algebraic relations
- such quantities appear naturally in the analysis of the Bell operator
- non-trivial statements can be made for arbitrarily small violations
- can be used to guarantee uncertainty (useful for DI cryptography)

Robust self-testing

Idea: instead of certifying closeness to the canonical realisation certify **algebraic relations between observables** [8]

Convenient because

- it is clear how to measure "approximate" satisfaction of algebraic relations
- such quantities appear naturally in the analysis of the Bell operator
- non-trivial statements can be made for arbitrarily small violations
- can be used to guarantee uncertainty (useful for DI cryptography)

This might not be the **ultimate answer**, but for binary observables these quantities have all the **desired properties**

Outline

- Bell nonlocality
- Self-testing
- Robust self-testing
- Summary and open questions

Summary and open questions

Summary:

- self-testing = certification of bi- or multipartite quantum systems under minimal assumptions
- direct link between the macroscopic and microscopic worlds
- insight into the geometry of the quantum set of correlations
- applications for device-independent cryptography

Summary and open questions

Open questions:

- which Bell inequalities are rigid and why? how generic is this phenomenon?
- all bipartite pure states can be self-tested [18], but some tripartite cannot: why?
- which arrangements of measurements can be self-tested and how?
- what is the "correct" formulation for robust self-testing of measurements?


So you can really certify quantum systems without trusting the devices at all?
Yes, Pooh, quantum mechanics is very strange and nobody really understands it, but let's talk about it another day. . .
THE END

References I

[1] S. Popescu and D. Rohrlich. "Which states violate Bell's inequality maximally?" *Phys. Lett. A* 169 (6 1992). DOI: `10.1016/0375-9601(92)90819-8`.

[2] M. McKague, T. H. Yang, and V. Scarani. "Robust self-testing of the singlet". *J. Phys. A: Math. Theor.* 45.455304 (45 2012). DOI: `10.1088/1751-8113/45/45/455304`.

[3] W. Slofstra. "Lower bounds on the entanglement needed to play XOR non-local games". *J. Math. Phys.* 52.102202 (10 2011). DOI: `10.1063/1.3652924`.

[4] R. Ramanathan and P. Mironowicz. "Trade-offs in multi-party Bell inequality violations in qubit networks". (2017).

[5] K. T. Goh et al. "Geometry of the quantum set of correlations". (2017).

[6] T. H. Yang and M. Navascués. "Robust self-testing of unknown quantum systems into any entangled two-qubit states". *Phys. Rev. A* 87.050102(R) (5 2013). DOI: `10.1103/PhysRevA.87.050102`.

[7] C. Bamps and S. Pironio. "Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing". *Phys. Rev. A* 91.052111 (5 2015). DOI: `10.1103/PhysRevA.91.052111`.

[8] J. Kaniewski. "Self-testing of binary observables based on commutation". *Phys. Rev. A* 95.062323 (6 2017). DOI: `10.1103/PhysRevA.95.062323`.

References II

[9] I. Šupić et al. "Self-testing protocols based on the chained Bell inequalities". *New J. Phys.* 18.035013 (2016). DOI: 10.1088/1367-2630/18/3/035013.

[10] R. Colbeck. "Quantum and relativistic protocols for secure multi-party computation". PhD thesis. University of Cambridge, 2006.

[11] X. Wu et al. "Device-independent parallel self-testing of two singlets". *Phys. Rev. A* 93.062121 (6 2016). DOI: 10.1103/PhysRevA.93.062121.

[12] A. Kalev and C. A. Miller. "Rigidity of the magic pentagram game". (2017).

[13] C.-E. Bardyn et al. "Device independent state estimation based on Bell's inequalities". *Phys. Rev. A* 80.062327 (6 2009). DOI: 10.1103/PhysRevA.80.062327.

[14] J. Kaniewski. "Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities". *Phys. Rev. Lett.* 117.070402 (7 2016). DOI: 10.1103/PhysRevLett.117.070402.

[15] M. Horodecki, P. Horodecki, and R. Horodecki. "General teleportation channel, singlet fraction, and quasidistillation". *Phys. Rev. A* 60.1888 (3 1999). DOI: 10.1103/PhysRevA.60.1888.

[16] J.-D. Bancal et al. "Physical characterization of quantum devices from nonlocal correlations". *Phys. Rev. A* 91.022115 (2 2015). DOI: 10.1103/PhysRevA.91.022115.

[17] K. F. Pál, T. Vértesi, and M. Navascués. "Device-independent tomography of multipartite quantum states". *Phys. Rev. A* 90.042340 (4 2014). DOI: 10.1103/PhysRevA.90.042340.

References III

[18] A. W. Coladangelo, K. T. Goh, and V. Scarani. "All pure bipartite entangled states can be self-tested". *Nat. Commun.* 8.15485 (2017). DOI: 10.1038/ncomms15485.