Self-testing of binary observables based on commutation

[arXiv:1702.06845, Phys. Rev. A **95**, 062323 (2017)]

Jed Kaniewski

QMATH, Department of Mathematical Sciences
University of Copenhagen, Denmark

AQIS '17, Singapore
5 Sept 2017

Centre for the Mathematics of Quantum Theory

Outline

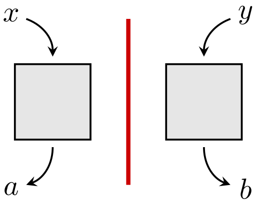
- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

Outline

- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

What is nonlocality?

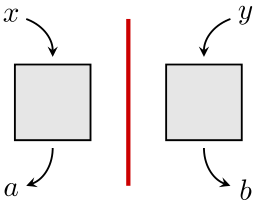
Bell scenario



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

What is nonlocality?

Bell scenario



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

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

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

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

What is nonlocality?

Assume quantum mechanics. . . what can I deduce about my system?

What is nonlocality?

Assume quantum mechanics. . . what can I deduce about my system?

Entanglement: separable states **always** produce local statistics

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

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

What is nonlocality?

Assume quantum mechanics… what can I deduce about my system?

Entanglement: separable states **always** produce local statistics

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

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

What is nonlocality?

Assume quantum mechanics... what can I deduce about my system?

Entanglement: separable states **always** produce local statistics

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

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

What is self-testing?

Self-testing

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

deduce properties of ρ_{AB}, (P_a^x), (Q_b^y)

What is self-testing?

Self-testing

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

deduce properties of ρ_{AB}, (P_a^x), (Q_b^y)
(don't assume that ρ_{AB} is pure or measurements are projective, deduce it instead!)

What is self-testing?

Self-testing

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

deduce properties of ρ_{AB}, (P_a^x), (Q_b^y)
(don't assume that ρ_{AB} is pure or measurements are projective, deduce it instead!)

often only promised some Bell violation

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

What is self-testing?

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

What is self-testing?

?

ρ_{AB}

state
certification

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

What is self-testing?

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

?

ρ_{AB}

state certification

P_a^x, Q_b^y

?

measurement certification

What is self-testing?

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

?

$\cancel{\rho}$

~~**state**~~
certification

P_a^x, Q_b^y

?

measurement
certification

What is self-testing?

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

?

$\cancel{\rho}$

~~state~~ certification

P_a^x, Q_b^y

?

measurement certification

Which measurements can be certified?

What is self-testing?

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

$\overset{?}{\cancel{\rho}}$

~~state~~ certification

$\underset{?}{P_a^x, Q_b^y}$

measurement certification

Which measurements can be certified?

IN A TRULY ROBUST FASHION...

What is self-testing?

Why care about self-testing of measurements?

- significantly less studied (particularly in the robust regime)
- relevant for (two-party) device-independent cryptography
- pinning down the optimal measurements immediately gives the optimal state

Outline

- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

The CHSH inequality

Measurements with **two outcomes**

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

The CHSH inequality

Measurements with **two outcomes**

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

Conveniently written as **observables**

$$A = F_0 - F_1$$

One-to-one mapping, i.e. any

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

corresponds to a valid measurement
[for projective measurements $A^2 = \mathbb{1}$]

The CHSH inequality

The CHSH value

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

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

The CHSH inequality

The CHSH value

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

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

What can we deduce from $\beta > 2$?

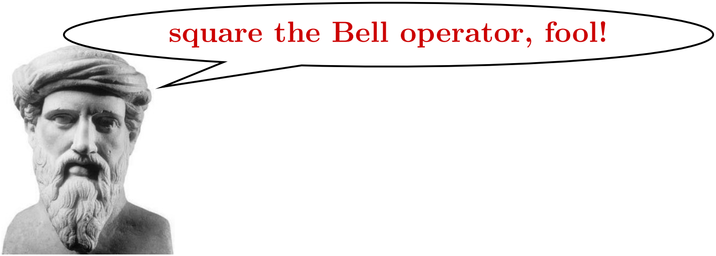
The CHSH inequality

The CHSH value

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

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

What can we deduce from $\beta > 2$?



The CHSH inequality

If $A_j^2 = B_k^2 = \mathbb{1}$, then

$$W^2 = 4 \cdot \mathbb{1} \otimes \mathbb{1} - [A_0, A_1] \otimes [B_0, B_1].$$

The CHSH inequality

If $A_j^2 = B_k^2 = \mathbb{1}$, then

$$W^2 = 4 \cdot \mathbb{1} \otimes \mathbb{1} - [A_0, A_1] \otimes [B_0, B_1].$$

In general ($A_j^2, B_k^2 \leq \mathbb{1}$)

$$W^2 \leq 4 \cdot \mathbb{1} \otimes \mathbb{1} - [A_0, A_1] \otimes [B_0, B_1].$$

Simple upper bounds

$$\begin{aligned} W^2 &\leq 4 \cdot \mathbb{1} \otimes \mathbb{1} + |[A_0, A_1] \otimes [B_0, B_1]| \\ &= 4 \cdot \mathbb{1} \otimes \mathbb{1} + |[A_0, A_1]| \otimes |[B_0, B_1]| \\ &\leq 4 \cdot \mathbb{1} \otimes \mathbb{1} + 2|[A_0, A_1]| \otimes \mathbb{1}. \end{aligned}$$

The CHSH inequality

$$W^2 \leq 4 \cdot \mathbb{1} \otimes \mathbb{1} + 2|[A_0, A_1]| \otimes \mathbb{1}.$$

The CHSH inequality

$$W^2 \leq 4 \cdot \mathbb{1} \otimes \mathbb{1} + 2|[A_0, A_1]| \otimes \mathbb{1}.$$

The Cauchy-Schwarz inequality

$$\big[\,\mathrm{tr}(W\rho_{AB})\big]^2 \leq \mathrm{tr}(W^2\rho_{AB}) \cdot \mathrm{tr}\,\rho_{AB} = \mathrm{tr}(W^2\rho_{AB})$$

The CHSH inequality

$$W^2 \leq 4 \cdot \mathbb{1} \otimes \mathbb{1} + 2|[A_0, A_1]| \otimes \mathbb{1}.$$

The Cauchy-Schwarz inequality

$$\left[\, \mathrm{tr}(W\rho_{AB})\right]^2 \leq \mathrm{tr}(W^2\rho_{AB}) \cdot \mathrm{tr}\,\rho_{AB} = \mathrm{tr}(W^2\rho_{AB})$$

leads to

$$\beta \leq 2\sqrt{1+t},$$

where $t := \frac{1}{2}\,\mathrm{tr}\left(|[A_0, A_1]|\rho_A\right)$.

Bell violation certifies incompatibility of observables!

The CHSH inequality

The quantity

$$t := \frac{1}{2}\,\mathrm{tr}\left(|[A_0, A_1]|\rho_A\right)$$

- invariant under local unitaries and adding auxiliary systems
- easy to compute
- clear operational interpretation as "weighted average"
- $t = 1$ (max. value) implies

$$UA_0U^\dagger = \sigma_x \otimes \mathbb{1},$$
$$UA_1U^\dagger = \sigma_y \otimes \mathbb{1}.$$

[assuming ρ_A is full-rank]

The CHSH inequality

The quantity

$$t := \frac{1}{2}\operatorname{tr}\left(|[A_0, A_1]|\rho_A\right)$$

- invariant under local unitaries and adding auxiliary systems
- easy to compute
- clear operational interpretation as "weighted average"
- $t = 1$ (max. value) implies

$$UA_0U^\dagger = \sigma_x \otimes \mathbb{1},$$
$$UA_1U^\dagger = \sigma_y \otimes \mathbb{1}.$$

[assuming ρ_A is full-rank]

$\Longrightarrow$ $t =$ "**distance from the optimal arrangement**"

The CHSH inequality

The relation

$$\beta \leq 2\sqrt{1+t},$$

- is non-trivial as soon as $\beta > 2$
- is tight

The CHSH inequality

The relation

$$\beta \leq 2\sqrt{1+t},$$

- is non-trivial as soon as $\beta > 2$
- is tight

CHSH violation certifies closeness to the optimal arrangement

The CHSH inequality

The relation

$$\beta \leq 2\sqrt{1+t},$$

- is non-trivial as soon as $\beta > 2$
- is tight

CHSH violation certifies closeness to the optimal arrangement

BONUS: $\beta = 2\sqrt{2}$ implies $t = 1$ and so

$$UA_0U^\dagger = \sigma_x \otimes \mathbb{1},$$
$$UA_1U^\dagger = \sigma_y \otimes \mathbb{1}$$

By symmetry the same applies to Bob, so W (up to local unitaries) is just a **two-qubit operator tensored with identity** $\implies$ finding the optimal state is easy

The CHSH inequality

Complete rigidity statement: if $\beta = 2\sqrt{2}$ then there exists $U = U_A \otimes U_B$ and $\tau_{A'B'}$

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

where $\Phi_{AB} =$ EPR pair and

$$U_A A_0 U_A^\dagger = \sigma_x \otimes \mathbb{1},$$
$$U_A A_1 U_A^\dagger = \sigma_y \otimes \mathbb{1},$$
$$U_B B_0 U_B^\dagger = \sigma_x \otimes \mathbb{1},$$
$$U_B B_1 U_B^\dagger = \sigma_y \otimes \mathbb{1}.$$

The CHSH inequality

Complete rigidity statement: if $\beta = 2\sqrt{2}$ then there exists $U = U_A \otimes U_B$ and $\tau_{A'B'}$

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

where $\Phi_{AB} =$ EPR pair and

$$\begin{aligned} U_A A_0 U_A^\dagger &= \sigma_x \otimes \mathbb{1}, \\ U_A A_1 U_A^\dagger &= \sigma_y \otimes \mathbb{1}, \\ U_B B_0 U_B^\dagger &= \sigma_x \otimes \mathbb{1}, \\ U_B B_1 U_B^\dagger &= \sigma_y \otimes \mathbb{1}. \end{aligned}$$

very similar to the **original proof by Popescu and Rohrlich**

The CHSH inequality

Complete rigidity statement: if $\beta = 2\sqrt{2}$ then there exists $U = U_A \otimes U_B$ and $\tau_{A'B'}$

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

where Φ_{AB} = EPR pair and

$$\begin{aligned} U_A A_0 U_A^\dagger &= \sigma_x \otimes \mathbb{1}, \\ U_A A_1 U_A^\dagger &= \sigma_y \otimes \mathbb{1}, \\ U_B B_0 U_B^\dagger &= \sigma_x \otimes \mathbb{1}, \\ U_B B_1 U_B^\dagger &= \sigma_y \otimes \mathbb{1}. \end{aligned}$$

very similar to the **original proof by Popescu and Rohrlich**
[generalises straightforwardly to multipartite inequalities: Mermin/MABK inequalities]

Outline

- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

The biased CHSH inequality

For $\alpha \geq 1$ the biased CHSH value

$$\beta := \operatorname{tr}\left(W_\alpha \rho_{AB}\right)$$

for

$$W_\alpha := \alpha(A_0 + A_1) \otimes B_0 + (A_0 - A_1) \otimes B_1.$$

Classically $\beta \leq 2\alpha$, but quantumly we can reach up to $2\sqrt{\alpha^2 + 1}$.

- optimal state: maximally entangled of 2 qubits
- optimal observables of Bob: maximally incompatible
- optimal observables of Alice: **non-maximally incompatible!**

The biased CHSH inequality

Analogous argument leads to

$$\beta_\alpha \leq 2\sqrt{\alpha^2 + t_\alpha}$$

for $t_\alpha := \mathrm{tr}(T_\alpha \rho_A)$, where

$$T_\alpha := \frac{\alpha^2 - 1}{4}\big(\{A_0, A_1\} - 2 \cdot \mathbb{1}\big) + \frac{\alpha}{2}|[A_0, A_1]|.$$

The biased CHSH inequality

Analogous argument leads to

$$\beta_\alpha \leq 2\sqrt{\alpha^2 + t_\alpha}$$

for $t_\alpha := \mathrm{tr}(T_\alpha \rho_A)$, where

$$T_\alpha := \frac{\alpha^2 - 1}{4}\big(\{A_0, A_1\} - 2 \cdot \mathbb{1}\big) + \frac{\alpha}{2}|[A_0, A_1]|.$$

- for $\alpha = 1$ we recover CHSH
- setting $[A_0, A_1] = 0$ yields the classical bound
- $t_\alpha = 1$ (max. value) implies

$$\begin{aligned} UA_0U^\dagger &= \sigma_x \otimes \mathbb{1} \\ UA_1U^\dagger &= (\cos\theta_\alpha\, \sigma_x + \sin\theta_\alpha\, \sigma_y) \otimes \mathbb{1} \end{aligned}$$

The biased CHSH inequality

Analogous argument leads to

$$\beta_\alpha \leq 2\sqrt{\alpha^2 + t_\alpha}$$

for $t_\alpha := \mathrm{tr}(T_\alpha \rho_A)$, where

$$T_\alpha := \frac{\alpha^2 - 1}{4}\big(\{A_0, A_1\} - 2 \cdot \mathbb{1}\big) + \frac{\alpha}{2}|[A_0, A_1]|.$$

- for $\alpha = 1$ we recover CHSH
- setting $[A_0, A_1] = 0$ yields the classical bound
- $t_\alpha = 1$ (max. value) implies

$$UA_0U^\dagger = \sigma_x \otimes \mathbb{1}$$
$$UA_1U^\dagger = (\cos\theta_\alpha\, \sigma_x + \sin\theta_\alpha\, \sigma_y) \otimes \mathbb{1}$$

Any pair of qubit observables can be robustly certified!

Outline

- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

Multiple anticommuting observables

Problem with 3 anticommuting observables: cannot distinguish

$$(\sigma_x, \sigma_y, \sigma_z) \quad \text{vs.} \quad (\sigma_x, -\sigma_y, \sigma_z)$$

[not unitarily equivalent; related by transposition]

Multiple anticommuting observables

Problem with 3 anticommuting observables: cannot distinguish

$$(\sigma_x, \sigma_y, \sigma_z) \quad \text{vs.} \quad (\sigma_x, -\sigma_y, \sigma_z)$$

[not unitarily equivalent; related by transposition]

Standard self-testing statement: exists projective observable Υ ($\Upsilon^2 = \mathbb{1}$):

$$\begin{aligned} U A_0 U^\dagger &= \sigma_x \otimes \mathbb{1} \\ U A_1 U^\dagger &= \sigma_y \otimes \Upsilon \\ U A_2 U^\dagger &= \sigma_z \otimes \mathbb{1} \end{aligned}$$

[direct sum of the two arrangements]

Multiple anticommuting observables

Problem with 3 anticommuting observables: cannot distinguish

$$(\sigma_x, \sigma_y, \sigma_z) \quad \text{vs.} \quad (\sigma_x, -\sigma_y, \sigma_z)$$

[not unitarily equivalent; related by transposition]

Standard self-testing statement: exists projective observable Υ ($\Upsilon^2 = \mathbb{1}$):

$$\begin{aligned} UA_0U^\dagger =& \sigma_x \otimes \mathbb{1} \\ UA_1U^\dagger =& \sigma_y \otimes \Upsilon \\ UA_2U^\dagger =& \sigma_z \otimes \mathbb{1} \end{aligned}$$

[direct sum of the two arrangements]

Not symmetric 

Multiple anticommuting observables

A simple extension of CHSH gives

$$\mathrm{tr}\left(|[A_0, A_1]|\rho_A\right) = \mathrm{tr}\left(|[A_0, A_2]|\rho_A\right) = \mathrm{tr}\left(|[A_1, A_2]|\rho_A\right) = 2$$

[generalises straightforwardly to arbitrary number]

Simple and **symmetric** 

Multiple anticommuting observables

A simple extension of CHSH gives

$$\mathrm{tr}\left(|[A_0, A_1]|\rho_A\right) = \mathrm{tr}\left(|[A_0, A_2]|\rho_A\right) = \mathrm{tr}\left(|[A_1, A_2]|\rho_A\right) = 2$$

[generalises straightforwardly to arbitrary number]

Simple and **symmetric** 

Good news: **the two are equivalent!**

It is "natural" to formulate self-testing statements in terms of commutation

Outline

- What is nonlocality?
- What is self-testing?
- The CHSH inequality
- The biased CHSH inequality
- Multiple anticommuting observables
- Summary and open problems

Summary

- Commutation-based formulation is convenient: tight self-testing relations from elementary algebra
- For every angle on a qubit there exists a simple (easy to evaluate) **commutation-based function which measures distance to this arrangement**
- Every such arrangement can be **certified in a robust manner**
- Knowing the commutation structure immediately gives a **full rigidity statement**

Open problems

- What about arrangements of observables that "do not fit" into a qubit? E.g. the maximal violation of I_{3322} requires large dimension (in fact, conjectured to be ∞).
  What is the commutation structure of the optimal observables?
- What about observables with more outcomes?
  E.g. Heisenberg-Weyl observables satisfy "twisted commutation relation"
  $$Z_d X_d = \omega X_d Z_d \qquad \left(\omega = e^{2\pi i/d}\right).$$
  Can we find an inequality which certifies precisely this relation?


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