Self-testing of binary observables based on commutation


Jed Kaniewski

QMATH, Department of Mathematical Sciences
University of Copenhagen, Denmark

AQIS ’17, Singapore
5 Sept 2017
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**

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

**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 \( \Rightarrow \) nonlocal or it violates (some) Bell inequality.
What is nonlocality?

**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 \( \Rightarrow \) **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

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

\[
\Pr[a, b|x, y] = \text{tr} \left[ (P_{a}^{x} \otimes Q_{b}^{y}) \rho_{AB} \right] = \sum_{\lambda} p_{\lambda} \cdot \frac{\text{tr}(P_{a}^{x} \sigma_{\lambda})}{p(a|x,\lambda)} \cdot \frac{\text{tr}(Q_{b}^{y} \tau_{\lambda})}{p(b|y,\lambda)}
\]
What is nonlocality?

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

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

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

$$\Pr[a, b|x, y] = \text{tr} \left[ (P_{a}^{x} \otimes Q_{b}^{y}) \rho_{AB} \right] = \sum_{\lambda} p_{\lambda} \cdot \text{tr}(P_{a}^{x} \sigma_{\lambda}) \cdot \text{tr}(Q_{b}^{y} \tau_{\lambda}) \frac{p(a|x,\lambda)}{p(a|x,\lambda)} \cdot \frac{p(b|y,\lambda)}{p(b|y,\lambda)}$$

what else?
What is nonlocality?

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

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

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

\[ \Pr[a, b|x, y] = \text{tr} \left[ (P^x_a \otimes Q^y_b) \rho_{AB} \right] = \sum_{\lambda} p_\lambda \cdot \text{tr}(P^x_a \sigma_\lambda) \cdot \text{tr}(Q^y_b \tau_\lambda) \]

what else?

self-testing study

you must
What is self-testing?

Given $\Pr[a, b|x, y] = \text{tr} [(P^x_a \otimes Q^y_b) \rho_{AB}]$

deduce properties of $\rho_{AB}, (P^x_a), (Q^y_b)$
What is self-testing?

**Self-testing**

Given $\text{Pr}[a, b|x, y] = \text{tr} \left[ (P^x_a \otimes Q^y_b) \rho_{AB} \right]$

**deduce properties** of $\rho_{AB}$, $(P^x_a)$, $(Q^y_b)$

(don’t assume that $\rho_{AB}$ is pure or measurements are projective, deduce it instead!)
What is self-testing?

**Self-testing**

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

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

(don’t assume that \( \rho_{AB} \) 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?

\[ \sum_{abxy} c_{ab}^{xy} \Pr[a, b \mid x, y] = \beta \]
What is self-testing?

\[ \sum_{abxy} c_{ab}^{xy} \Pr[a, b|x, y] = \beta \]
What is self-testing?

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

\[ \rho_{AB} \]

\[ P_x^a, Q_y^b \]

state certification

measurement certification
What is self-testing?

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

- State certification
- Measurement certification

\[ \rho \]

\[ P_a^x, Q_b^y \]
What is self-testing?

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

Which measurements can be certified?

\[ \rho \]

state certification

\[ P_{a}^{x} , Q_{b}^{y} \]

measurement certification

\( (P_{a}^{x})? \)
What is self-testing?

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

Which measurements can be certified?

IN A TRULY ROBUST FASHION...

\[ P_x, Q_y \]

\[ (P_x) ? \]
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
Measurements with two outcomes

\[ F_j = F_j^\dagger, \]
\[ F_j \geq 0, \]
\[ F_0 + F_1 = 1 \]
The CHSH inequality

Measurements with two outcomes

\[ F_j = F_j^\dagger, \]
\[ F_j \geq 0, \]
\[ F_0 + F_1 = 1 \]

Conveniently written as observables

\[ A = F_0 - F_1 \]

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

\[ A = A^\dagger \quad \text{and} \quad -1 \leq A \leq 1 \]

corresponds to a valid measurement

[for projective measurements \( A^2 = 1 \)]
The CHSH inequality

The CHSH value

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

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

The CHSH value

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

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

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

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

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

square the Bell operator, fool!
The CHSH inequality

If $A_j^2 = B_k^2 = 1$, then

$$W^2 = 4 \cdot 1 \otimes 1 - [A_0, A_1] \otimes [B_0, B_1].$$
The CHSH inequality

If \(A_j^2 = B_k^2 = 1\), then

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

In general \((A_j^2, B_k^2 \leq 1)\)

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

Simple upper bounds

\[ W^2 \leq 4 \cdot 1 \otimes 1 + |[A_0, A_1] \otimes [B_0, B_1]| \]
\[ = 4 \cdot 1 \otimes 1 + |[A_0, A_1]| \otimes |[B_0, B_1]| \]
\[ \leq 4 \cdot 1 \otimes 1 + 2|[A_0, A_1]| \otimes 1. \]
The CHSH inequality

\[ W^2 \leq 4 \cdot 1 \otimes 1 + 2| [A_0, A_1] | \otimes 1. \]
The CHSH inequality

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

The Cauchy-Schwarz inequality

\[ \left[ \text{tr}(W \rho_{AB}) \right]^2 \leq \text{tr}(W^2 \rho_{AB}) \cdot \text{tr} \rho_{AB} = \text{tr}(W^2 \rho_{AB}) \]
The CHSH inequality

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

The Cauchy-Schwarz inequality

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

leads to

\[ \beta \leq 2\sqrt{1 + t}, \]

where \( t := \frac{1}{2} \text{tr} \left( |[A_0, A_1]| \rho_{A} \right) \).

Bell violation certifies incompatibility of observables!
The CHSH inequality

The quantity

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

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

\[
UA_0 U^\dagger = \sigma_x \otimes 1, \\
UA_1 U^\dagger = \sigma_y \otimes 1.
\]

[assuming \( \rho_A \) is full-rank]
The CHSH inequality

The quantity

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

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

\[ UA_0 U^\dagger = \sigma_x \otimes 1, \]
\[ UA_1 U^\dagger = \sigma_y \otimes 1. \]

[assuming \( \rho_A \) is full-rank]

\( \implies t = “\text{distance from the optimal arrangement}” \)
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

\[
UA_0U^\dagger = \sigma_x \otimes 1, \\
UA_1U^\dagger = \sigma_y \otimes 1
\]

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

$$U_A A_0 U_A^\dagger = \sigma_x \otimes 1,$$

$$U_A A_1 U_A^\dagger = \sigma_y \otimes 1,$$

$$U_B B_0 U_B^\dagger = \sigma_x \otimes 1,$$

$$U_B B_1 U_B^\dagger = \sigma_y \otimes 1.$$
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 $\Phi_{AB} = \text{EPR pair}$ and

$$U_A A_0 U_A^\dagger = \sigma_x \otimes 1,$$

$$U_A A_1 U_A^\dagger = \sigma_y \otimes 1,$$

$$U_B B_0 U_B^\dagger = \sigma_x \otimes 1,$$

$$U_B B_1 U_B^\dagger = \sigma_y \otimes 1.$$

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

$$U_A A_0 U_A^\dagger = \sigma_x \otimes 1,$$

$$U_A A_1 U_A^\dagger = \sigma_y \otimes 1,$$

$$U_B B_0 U_B^\dagger = \sigma_x \otimes 1,$$

$$U_B B_1 U_B^\dagger = \sigma_y \otimes 1.$$

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

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

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 \( t_\alpha := \text{tr}(T_\alpha \rho_A) \), where

\[ T_\alpha := \frac{\alpha^2 - 1}{4} \left( \{A_0, A_1\} - 2 \cdot \mathbb{1} \right) + \frac{\alpha}{2} |[A_0, A_1]|. \]
The biased CHSH inequality

Analogous argument leads to

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

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

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

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

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

Any pair of qubit observables can be robustly certified!
The biased CHSH inequality

Analogous argument leads to

\[ \beta_\alpha \leq 2\sqrt{\alpha^2 + t_\alpha} \]

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

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

- for \( \alpha = 1 \) we recover CHSH
- setting \([A_0, A_1] = 0\) yields the classical bound
- \( t_\alpha = 1 \) (max. value) implies
  
  \[ UA_0 U^\dagger = \sigma_x \otimes \mathbb{1} \]
  \[ UA_1 U^\dagger = (\cos \theta_\alpha \sigma_x + \sin \theta_\alpha \sigma_y) \otimes \mathbb{1} \]

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

\[(\sigma_x, \sigma_y, \sigma_z) \text{ vs. } (\sigma_x, -\sigma_y, \sigma_z)\]

[not unitarily equivalent; related by transposition]
Multiple anticommuting observables

Problem with 3 anticommuting observables: cannot distinguish

\[(\sigma_x, \sigma_y, \sigma_z) \text{ vs. } (\sigma_x, -\sigma_y, \sigma_z)\]

[not unitarily equivalent; related by transposition]

Standard self-testing statement: exists projective observable \(\Upsilon\) \((\Upsilon^2 = 1)\):

\[
UA_0 U^\dagger = \sigma_x \otimes 1 \\
UA_1 U^\dagger = \sigma_y \otimes \Upsilon \\
UA_2 U^\dagger = \sigma_z \otimes 1
\]

[direct sum of the two arrangements]
Multiple anticommuting observables

Problem with 3 anticommuting observables: cannot distinguish

\((\sigma_x, \sigma_y, \sigma_z)\) vs. \((\sigma_x, -\sigma_y, \sigma_z)\)

[not unitarily equivalent; related by transposition]

Standard self-testing statement: exists projective observable \(\Upsilon\) \((\Upsilon^2 = 1)\):

\[
UA_0 U^\dagger = \sigma_x \otimes 1 \\
UA_1 U^\dagger = \sigma_y \otimes \Upsilon \\
UA_2 U^\dagger = \sigma_z \otimes 1
\]

[direct sum of the two arrangements]

Not symmetric 😞
A simple extension of CHSH gives

\[
\text{tr} (| [A_0, A_1] \rangle \langle \rho_A |) = \text{tr} (| [A_0, A_2] \rangle \langle \rho_A |) = \text{tr} (| [A_1, A_2] \rangle \langle \rho_A |) = 2
\]

[generalises straightforwardly to arbitrary number]

Simple and symmetric 😊
Multiple anticommuting observables

A simple extension of CHSH gives

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

[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
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 $\infty$).

**What is the commutation structure of the optimal observables?**

- What about observables with more outcomes? E.g. Heisenberg-Weyl observables satisfy “twisted commutation relation”

$$Z_d X_d = \omega X_d Z_d \quad (\omega = e^{2\pi i/d}).$$

**Can we find an inequality which certifies precisely this relation?**
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 some other day...