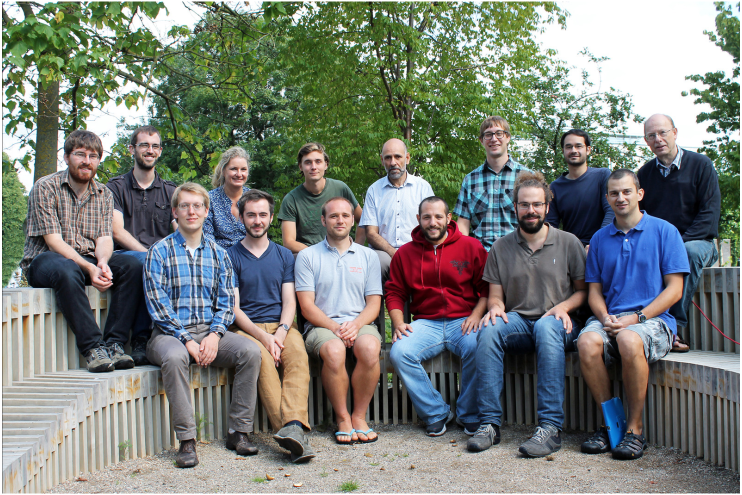
Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities

Phys. Rev. Lett. **117**, 070402 (2016)
[arXiv:1604.08176]

Jed Kaniewski
QMATH, Department of Mathematical Sciences
University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark

17 June 2016

CEQIP '16



http://qmath.ku.dk/

Outline

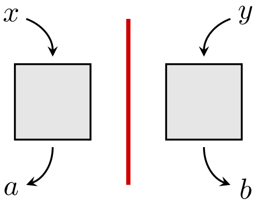
- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

Outline

- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

What is self-testing?

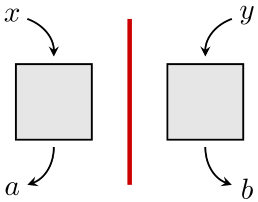
Bell scenario



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

What is self-testing?

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 self-testing?

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

$$\rho_{AB} = \sum_{\lambda} p_{\lambda} \alpha_{\lambda} \otimes \beta_{\lambda},$$

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

What is self-testing?

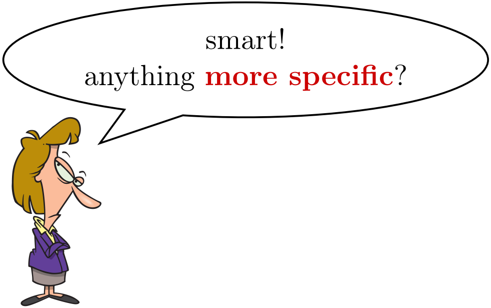
$$\rho_{AB} \text{ is separable} \implies \text{statistics are } \textbf{local}$$

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

What is self-testing?

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

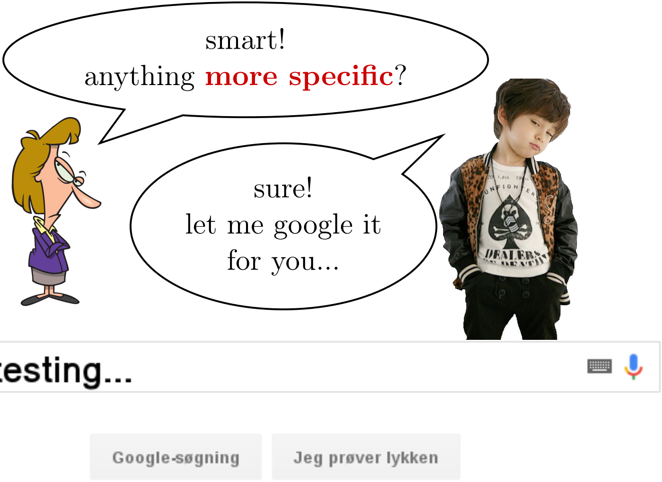
$\Pr[a, b|x, y]$ is **nonlocal** $\implies$ ρ_{AB} is entangled



What is self-testing?

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

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



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}, $\{P_a^x\}$, $\{Q_b^y\}$
We don't assume that ρ_{AB} is pure and it's **important**! (ask me if you want to know more)

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

We don't assume that ρ_{AB} is pure and it's **important**! (ask me if you want to know more)

often only promised some Bell violation

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

What is self-testing?

Example: the CHSH inequality [Popescu, Rohrlich '92]

$$\beta_{\text{CHSH}} := \sum_{abxy} (-1)^{a+b+xy} \Pr[a,b|x,y] \quad \text{for} \quad a,b,x,y \in \{0,1\}$$

$\beta_{\text{CHSH}} = 2\sqrt{2}$ (max) $\implies \rho_{AB} \simeq \Phi_{AB}$ for $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

What is self-testing?

Example: the CHSH inequality [Popescu, Rohrlich '92]

$$\beta_{\text{CHSH}} := \sum_{abxy} (-1)^{a+b+xy} \Pr[a,b|x,y] \quad \text{for} \quad a,b,x,y \in \{0,1\}$$

$$\beta_{\text{CHSH}} = 2\sqrt{2} \text{ (max)} \implies \rho_{AB} \simeq \Phi_{AB} \text{ for } |\Phi_{AB}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

$$\rho_{AB} \;=\; \quad \Phi_{AB}$$

Inherent limitations

What is self-testing?

Example: the CHSH inequality [Popescu, Rohrlich '92]

$$\beta_{\mathrm{CHSH}} := \sum_{abxy} (-1)^{a+b+xy} \Pr[a,b|x,y] \quad \text{for} \quad a,b,x,y \in \{0,1\}$$

$$\beta_{\mathrm{CHSH}} = 2\sqrt{2} \text{ (max)} \implies \rho_{AB} \simeq \Phi_{AB} \text{ for } |\Phi_{AB}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

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

Inherent limitations

- cannot see auxiliary systems (measurements act trivially)

What is self-testing?

Example: the CHSH inequality [Popescu, Rohrlich '92]

$$\beta_{\text{CHSH}} := \sum_{abxy} (-1)^{a+b+xy} \Pr[a, b|x, y] \quad \text{for} \quad a, b, x, y \in \{0, 1\}$$

$$\beta_{\text{CHSH}} = 2\sqrt{2} \text{ (max)} \implies \rho_{AB} \simeq \Phi_{AB} \text{ for } |\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

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

Inherent limitations

- cannot see auxiliary systems (measurements act trivially)
- cannot see local unitaries

What is self-testing?

Example: the CHSH inequality [Popescu, Rohrlich '92]

$$\beta_{\text{CHSH}} := \sum_{abxy} (-1)^{a+b+xy} \Pr[a, b|x, y] \quad \text{for} \quad a, b, x, y \in \{0, 1\}$$

$$\beta_{\text{CHSH}} = 2\sqrt{2} \text{ (max)} \implies \rho_{AB} \simeq \Phi_{AB} \text{ for } |\Phi_{AB}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

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

Inherent limitations

- cannot see auxiliary systems (measurements act trivially)
- cannot see local unitaries

Necessary... but also **sufficient!**

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

$P_a^x, Q_b^y(\rho_{AB})$

?

measurement
certification

What is self-testing?

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

?

ρ_{AB}

state certification

$P_a^x, Q_b^y, \rho_{AB})$

?

measurement certification

What is self-testing?

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

?
ρ_{AB}

state
certification

$P_a^x, Q_b^y, \rho_{AB})$
?

measurement
certification

Which states can be certified?

What is self-testing?

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

?

ρ_{AB}

state certification

$P_a^x, Q_b^y, \rho_{AB})$

?

measurement certification

Which states can be certified?

IN A TRULY ROBUST FASHION...

What is self-testing?

What is **experimentally-relevant**?

The CHSH inequality: $\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$

What is self-testing?

What is **experimentally-relevant**?

The CHSH inequality: $\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$

Non-trivial bounds for...

[Bardyn et al. '09]: $\beta \geq 1 + \sqrt{2} \approx 2.41$

[McKague et al. '12]: $\beta \geq \beta_Q - 2 \cdot 10^{-5}$

What is self-testing?

What is **experimentally-relevant**?

The CHSH inequality: $\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$

Non-trivial bounds for...

[Bardyn et al. '09]: $\beta \geq 1 + \sqrt{2} \approx 2.41$ ✓

[McKague et al. '12]: $\beta \geq \beta_Q - 2 \cdot 10^{-5}$ ✗

What is self-testing?

What is **experimentally-relevant**?

The CHSH inequality: $\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$

Non-trivial bounds for...

[Bardyn et al. '09]: $\beta \geq 1 + \sqrt{2} \approx 2.41$ ✓

[McKague et al. '12]: $\beta \geq \beta_Q - 2 \cdot 10^{-5}$ ✗

The loophole-free Bell experiment from Delft

$$\beta = 2.4 \pm 0.2$$

What is self-testing?

What is **experimentally-relevant**?

The CHSH inequality: $\beta_C = 2$ and $\beta_Q = 2\sqrt{2}$

Non-trivial bounds for...

[Bardyn et al. '09]: $\beta \geq 1 + \sqrt{2} \approx 2.41$ ✓

[McKague et al. '12]: $\beta \geq \beta_Q - 2 \cdot 10^{-5}$ ✗

The loophole-free Bell experiment from Delft

$$\beta = 2.4 \pm 0.2$$

4 orders of magnitude off!

Outline

- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

Previous results

Self-testable

- the singlet [McKague et al. '12]
- graph states [McKague '14]
- high-dimensional maximally entangled state [Slofstra '11, Yang, Navascués '13, McKague '16, Salavrakos et al. '16 + ...]
- non-maximally entangled states of 2 qubits [Bamps, Pironio '15]

Only for **almost perfect** statistics ($\varepsilon \approx 10^{-4}$).

Previous results

Self-testable

- the singlet [McKague et al. '12]
- graph states [McKague '14]
- high-dimensional maximally entangled state [Slofstra '11, Yang, Navascués '13, McKague '16, Salavrakos et al. '16 + ...]
- non-maximally entangled states of 2 qubits [Bamps, Pironio '15]

Only for **almost perfect** statistics ($\varepsilon \approx 10^{-4}$).

Experimentally-relevant robustness

- a single analytic result for the singlet-CHSH case [Bardyn et al. '09]
- swap trick: a numerical method, versatile but computationally expensive (so far up to 4 qubits or 2 qutrits) [Yang et al. '14, Bancal et al. '15]

[see `arXiv:1604.08176` for references]

New findings

New approach for analytic self-testing bounds

- improvement for the CHSH and Mermin_3
- Mermin_3 is actually **tight** (!)
- self-testing problem $\rightsquigarrow$ operator inequalities

Outline

- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

Self-testing from operator inequalities

Extractability of $\Psi_{A'B'}$ from ρ_{AB}

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

local extraction channels

fidelity

Self-testing from operator inequalities

Extractability of $\Psi_{A'B'}$ from ρ_{AB}

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

local extraction channels

fidelity

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

for $V = V_{A'A'' \to A} \otimes V_{B'B'' \to B}$

Self-testing from operator inequalities

Extractability of $\Psi_{A'B'}$ from ρ_{AB}

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

local extraction channels

fidelity

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

for $V = V_{A'A''\to A} \otimes V_{B'B''\to B}$

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

largest Schmidt coefficient

Self-testing from operator inequalities

Idea: measurement operators $\rightsquigarrow$ extraction channels!

Analytical bound of [Bardyn et al.] in 2 steps

[1] Solve the problem for 2 qbits

(local measurements determine a local unitary correction)

[2] Use Jordan's lemma to argue that it holds in arbitrary dimension

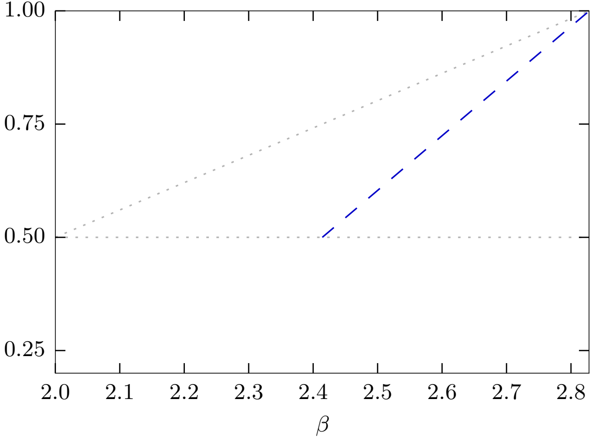
Self-testing from operator inequalities

Idea: measurement operators $\rightsquigarrow$ extraction channels!

Analytical bound of [Bardyn et al.] in 2 steps

[1] Solve the problem for 2 qbits
(local measurements determine a local unitary correction)

[2] Use Jordan's lemma to argue that it holds in arbitrary dimension



[C. E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Phys. Rev. A, 80(6), 2009. arXiv:0907.2170]

Self-testing from operator inequalities

Refined approach: assume

$$\Lambda_A := \Lambda_A(\{P_a^x\}) \quad \text{and} \quad \Lambda_B := \Lambda_B(\{Q_b^y\}).$$

Self-testing from operator inequalities

Refined approach: assume

$$\Lambda_A := \Lambda_A(\{P_a^x\}) \quad \text{and} \quad \Lambda_B := \Lambda_B(\{Q_b^y\}).$$

for $\Psi_{A'B'}$ pure

$$\begin{aligned} F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big) &= \langle (\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'} \rangle \\ &= \langle \rho_{AB}, (\Lambda_A^\dagger \otimes \Lambda_B^\dagger)(\Psi_{A'B'}) \rangle = \operatorname{tr}(K \rho_{AB}) \end{aligned}$$

for

$$K = (\Lambda_A^\dagger \otimes \Lambda_B^\dagger)(\Psi_{A'B'})$$

important: K depends only on $\Psi_{A'B'}, \{P_a^x\}, \{Q_b^y\}$, not on ρ_{AB}!

Self-testing from operator inequalities

Refined approach: assume

$$\Lambda_A := \Lambda_A(\{P_a^x\}) \quad \text{and} \quad \Lambda_B := \Lambda_B(\{Q_b^y\}).$$

for $\Psi_{A'B'}$ pure

$$\begin{aligned} F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big) &= \langle (\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'} \rangle \\ &= \langle \rho_{AB}, (\Lambda_A^\dagger \otimes \Lambda_B^\dagger)(\Psi_{A'B'}) \rangle = \operatorname{tr}(K \rho_{AB}) \end{aligned}$$

for

$$K = (\Lambda_A^\dagger \otimes \Lambda_B^\dagger)(\Psi_{A'B'})$$

important: K depends only on $\Psi_{A'B'}, \{P_a^x\}, \{Q_b^y\}$, not on ρ_{AB}!
... just like the **Bell operator**

$$W = \sum_{abxy} c_{ab}^{xy} P_a^x \otimes Q_b^y.$$

Self-testing from operator inequalities

Forget the input state ρ_{AB}! Want $s, \mu \in \mathbb{R}$ such that

$$K \geq sW + \mu \mathbb{1}$$

holds for all possible measurement operators

Self-testing from operator inequalities

Forget the input state ρ_{AB}! Want $s, \mu \in \mathbb{R}$ such that

$$K \geq sW + \mu \mathbb{1}$$

holds for all possible measurement operators

Challenging!... but if works then

$$\operatorname{tr}(K\rho_{AB}) \geq s \operatorname{tr}(W\rho_{AB}) + \mu \operatorname{tr}(\rho_{AB})$$

equivalent to

$$F\big((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\big) \geq s\beta + \mu$$

precisely a (linear) **self-testing statement!**

Self-testing from operator inequalities

Main technical challenge: find channels and s, μ such that

$$K \geq sW + \mu\mathbb{1}$$

holds **for all possible measurement operators**

Self-testing from operator inequalities

Main technical challenge: find channels and s, μ such that

$$K \geq sW + \mu\mathbb{1}$$

holds **for all possible measurement operators**

Jordan's lemma: any two binary, projective measurements can be **simultaneously block-diagonalised** into 2×2 blocks (at most)

each block parametrised by an angle $a \in [0, \pi/2]$ (up to unitary)

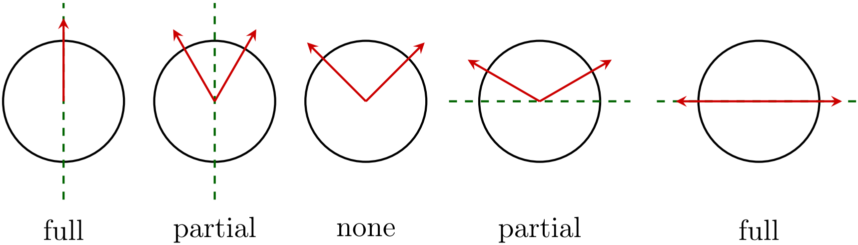
this becomes **tractable**: 1-parameter per party

Outline

- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

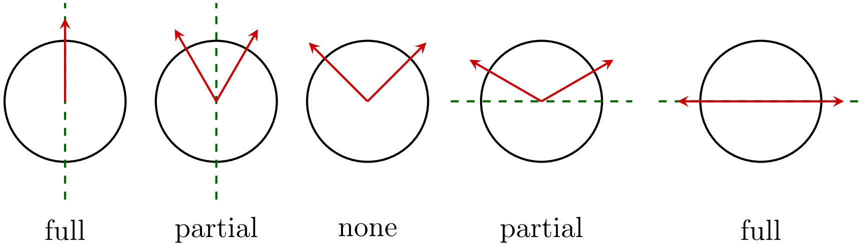
CHSH self-testing: proof in 4 steps

1. Extraction channels: **angle-dependent dephasing**



CHSH self-testing: proof in 4 steps

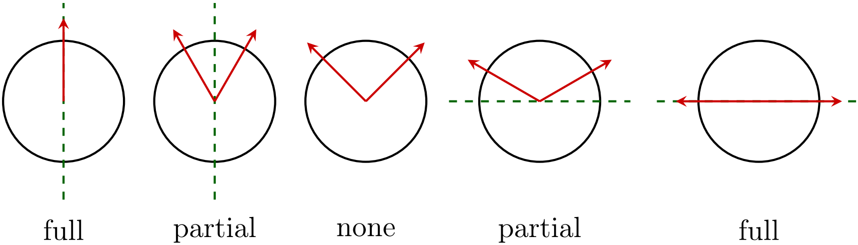
1. Extraction channels: **angle-dependent dephasing**



2. Find suitable s, μ (numerics): $s = (4 + 5\sqrt{2})/16$ and $\mu = -(1 + 2\sqrt{2})/4$

CHSH self-testing: proof in 4 steps

1. Extraction channels: **angle-dependent dephasing**



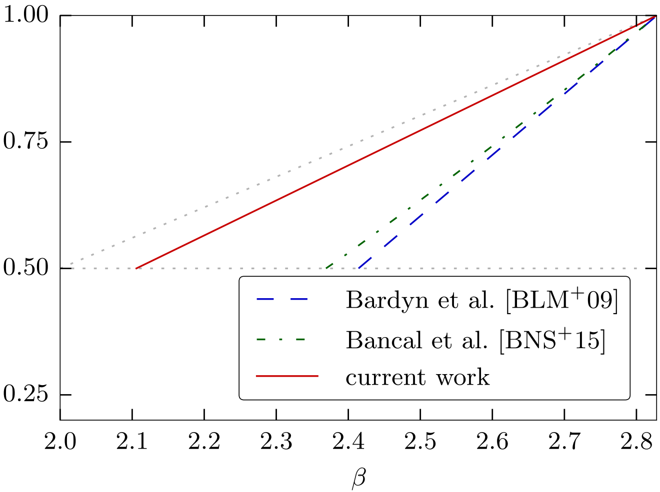
2. Find suitable s, μ (numerics): $s = (4 + 5\sqrt{2})/16$ and $\mu = -(1 + 2\sqrt{2})/4$
3. Prove

$$K(a, b) \geq sW(a, b) + \mu\mathbb{1}$$

for all $a, b \in [0, \pi/2]$
(2-parameter family of 4×4 matrices)

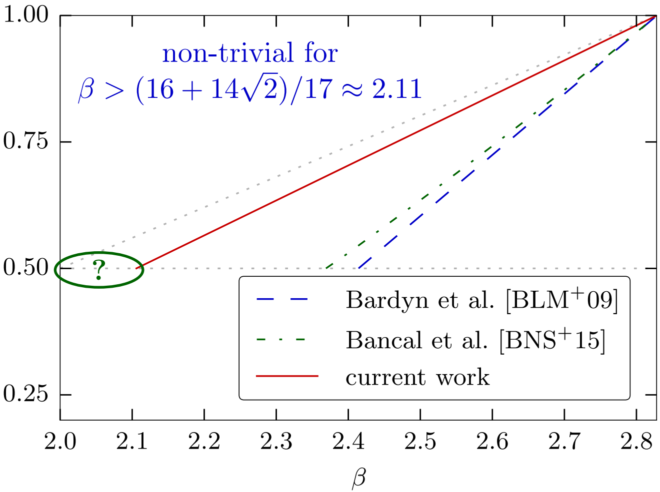
CHSH self-testing: proof in 4 steps

4. Enjoy the bound!



CHSH self-testing: proof in 4 steps

4. Enjoy the bound!



Mermin$_3$ self-testing: proof in 4 steps

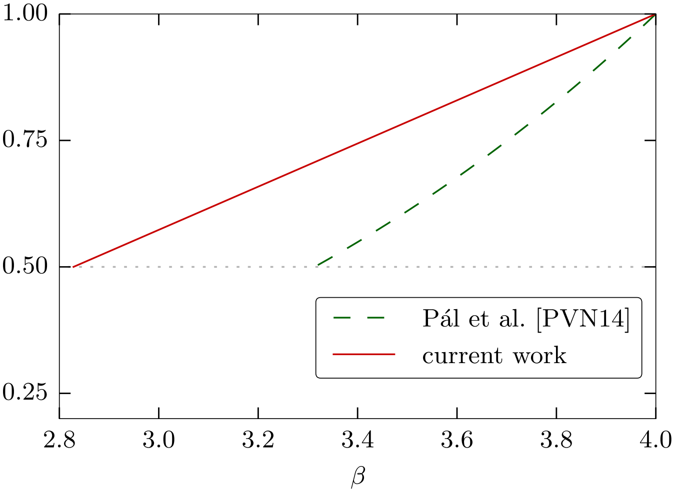
1. Same extraction channels
2. Find suitable s, μ (numerics): $s = (2+\sqrt{2})/8$ and $\mu = -1/\sqrt{2}$
3. Prove

$$K(a,b,c) \geq sW(a,b,c) + \mu \mathbb{1}$$

for all $a, b, c \in [0, \pi/2]$
(3-parameter family of 8×8 matrices)

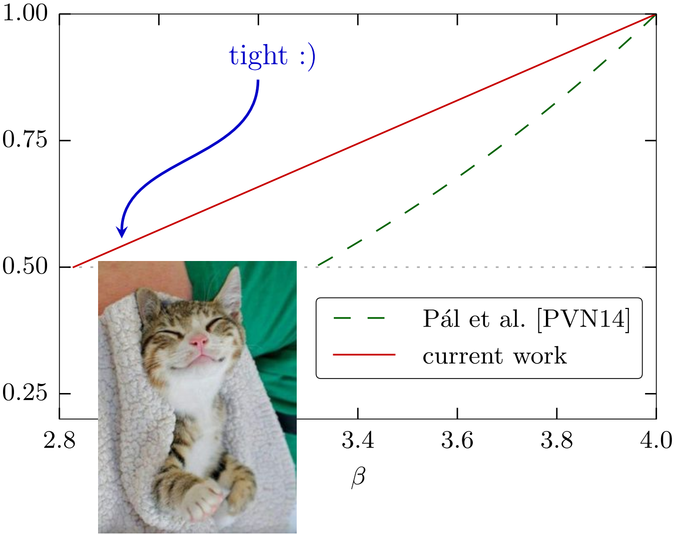
Mermin$_3$ self-testing: proof in 4 steps

4. Enjoy the bound



Mermin$_3$ self-testing: proof in 4 steps

4. Enjoy the bound



Outline

- What is self-testing?
- Previous results and new findings
- Self-testing from operator inequalities
- Two examples: the CHSH and Mermin_3 inequalities
- Summary and future work

Summary and future work

Summary

- self-testing from **operator inequalities**
- improvements for the **CHSH and Mermin$_3$ inequalities**
- first **provably tight self-testing statement**

Summary and future work

Summary

- self-testing from **operator inequalities**
- improvements for the **CHSH and Mermin$_3$ inequalities**
- first **provably tight self-testing statement**

Future work

- Mermin$_n$ $\overset{?}{\Longrightarrow}$ **GHZ$_n$ state** (preliminary numerics)
- tilted CHSH $\overset{?}{\Longrightarrow}$ **non-maximally entangled 2-qubit states** [project in progress with Tim Coopmans and Christian Schaffner]
- beyond **Jordan's lemma**?
- apply this approach to **steering**?


So you can really certify quantum states 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...
THE END