A weak form of self-testing

Jędrzej Kaniewski

Center for Theoretical Physics, Polish Academy of Sciences

(→ Faculty of Physics, University of Warsaw)

www.jkaniewski.eu

CEQIP '19

6 June 2019

National Science Centre
Poland

Outline

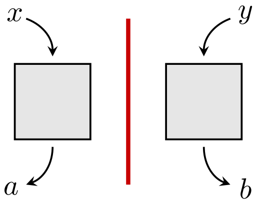
- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

Outline

- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

Bell nonlocality

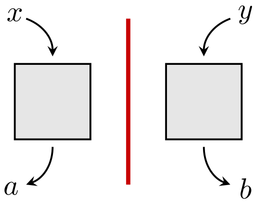
Bell scenario



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

Bell nonlocality

Bell scenario



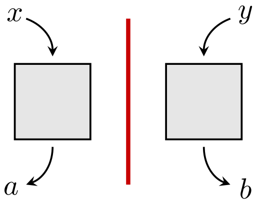
$P(a, b|x, y)$

Assume that $P \in \mathcal{Q}$ is **quantum**

$$P(a, b|x, y) = \langle F_a^x \otimes G_b^y, \rho_{AB} \rangle.$$

Bell nonlocality

Bell scenario



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

Assume that $P \in \mathcal{Q}$ is **quantum**

$$P(a, b|x, y) = \langle F_a^x \otimes G_b^y, \rho_{AB} \rangle.$$

Definition: $P \in \mathcal{L}$ is **local** if

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

Bell: $\mathcal{L} \subsetneq \mathcal{Q} \iff$ " quantum mechanics is (Bell) **nonlocal** "

Bell nonlocality

Given some $P \in \mathcal{Q}$, how to show that $P \notin \mathcal{L}$?

Bell nonlocality

Given some $P \in \mathcal{Q}$, how to show that $P \notin \mathcal{L}$?
Real vector $C = (c_{abxy})$ define

$$\langle C, P \rangle := \sum_{abxy} c_{abxy} P(a, b|x, y)$$

and

$$\beta_{\mathcal{L}} := \max_{P \in \mathcal{L}} \langle C, P \rangle \quad \text{(local value)}$$

$$\beta_{\mathcal{Q}} := \max_{P \in \mathcal{Q}} \langle C, P \rangle \quad \text{(quantum value)}$$

(suppose $\beta_{\mathcal{L}} < \beta_{\mathcal{Q}}$)

Bell nonlocality

Given some $P \in \mathcal{Q}$, how to show that $P \notin \mathcal{L}$?
Real vector $C = (c_{abxy})$ define

$$\langle C, P \rangle := \sum_{abxy} c_{abxy} P(a, b|x, y)$$

and

$$\beta_{\mathcal{L}} := \max_{P \in \mathcal{L}} \langle C, P \rangle \quad \text{(local value)}$$

$$\beta_{\mathcal{Q}} := \max_{P \in \mathcal{Q}} \langle C, P \rangle \quad \text{(quantum value)}$$

(suppose $\beta_{\mathcal{L}} < \beta_{\mathcal{Q}}$)

Bell violation: $\langle C, P \rangle > \beta_{\mathcal{L}} \implies P \notin \mathcal{L}$

Bell nonlocality

Observation: Separable states give local statistics (for all measurements)

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

Bell nonlocality

Observation: Separable states give local statistics (for all measurements)

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

$$P(a,b|x,y) = \langle F_a^x \otimes G_b^y, \rho_{AB}\rangle = \sum_\lambda p_\lambda \cdot \underbrace{\langle F_a^x, \sigma_\lambda\rangle}_{p_A(a|x,\lambda)} \cdot \underbrace{\langle G_b^y, \tau_\lambda\rangle}_{p_B(b|y,\lambda)}.$$

Nonlocality $\implies$ **entanglement**

Bell nonlocality

Observation: Separable states give local statistics (for all measurements)

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

$$P(a,b|x,y) = \langle F_a^x \otimes G_b^y, \rho_{AB}\rangle = \sum_\lambda p_\lambda \cdot \underbrace{\langle F_a^x, \sigma_\lambda\rangle}_{p_A(a|x,\lambda)} \cdot \underbrace{\langle G_b^y, \tau_\lambda\rangle}_{p_B(b|y,\lambda)}.$$

Nonlocality $\implies$ **entanglement**

Can we make this connection more explicit/quantitative?

Outline

- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

Remark 1. Bell functional vs. Bell operator

- For a Bell functional (c_{abxy}) define the Bell operator as

$$W := \sum_{abxy} c_{abxy} F_a^x \otimes G_b^y.$$

Remark 1. Bell functional vs. Bell operator

- For a Bell functional (c_{abxy}) define the Bell operator as

$$W := \sum_{abxy} c_{abxy} F_a^x \otimes G_b^y.$$

- Easy to check that

$$\langle C, P\rangle = \sum_{abxy} c_{abxy} P(a,b|x,y) = \sum_{abxy} c_{abxy} \langle F_a^x \otimes G_b^y, \rho_{AB}\rangle = \langle W, \rho_{AB}\rangle.$$

Remark 1. Bell functional vs. Bell operator

- For a Bell functional (c_{abxy}) define the Bell operator as

$$W := \sum_{abxy} c_{abxy} F_a^x \otimes G_b^y.$$

- Easy to check that

$$\langle C, P\rangle = \sum_{abxy} c_{abxy} P(a,b|x,y) = \sum_{abxy} c_{abxy} \langle F_a^x \otimes G_b^y, \rho_{AB}\rangle = \langle W, \rho_{AB}\rangle.$$

- Proving a bound on the quantum value $\beta_{\mathcal{Q}} \leq c$ is equivalent to showing that

$$W \leq c\,\mathbb{1}$$

for **all possible measurements choices**.

Remark 2. Measurements with two outcomes

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

Remark 2. Measurements with two outcomes

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

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

$$F_a = F_a^\dagger, \quad F_a \geq 0, \quad F_0 + F_1 = \mathbb{1}$$

Remark 2. Measurements with two outcomes

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

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

$$F_a = F_a^\dagger, \quad F_a \geq 0, \quad F_0 + F_1 = \mathbb{1}$$

  are conveniently written as **observables**

$$A = F_0 - F_1.$$

Remark 2. Measurements with two outcomes

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

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

$$F_a = F_a^\dagger, \quad F_a \geq 0, \quad F_0 + F_1 = \mathbb{1}$$

  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.

CHSH self-testing

- The CHSH operator reads

$$W := A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1),$$

where $-\mathbb{1} \leq A_j \leq \mathbb{1}$ and $-\mathbb{1} \leq B_k \leq \mathbb{1}$.

CHSH self-testing

- The CHSH operator reads

$$W := A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1),$$

where $-\mathbb{1} \leq A_j \leq \mathbb{1}$ and $-\mathbb{1} \leq B_k \leq \mathbb{1}$.

- Well known that $\beta_{\mathcal{L}} = 2$ and $\beta_{\mathcal{Q}} = 2\sqrt{2}$.

"The maximal violation $\beta = 2\sqrt{2}$ can be achieved in an essentially unique manner"

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

CHSH self-testing

Proof:

- Define

$$V_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}},$$

$$V_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}.$$

CHSH self-testing

Proof:

- Define

$$V_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}},$$
$$V_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}.$$

- Check

$$W = \frac{1}{\sqrt{2}}\Big[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\Big].$$

CHSH self-testing

Proof:

- Define

$$V_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}},$$
$$V_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}.$$

- Check

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\right].$$

- Conclude that $W \leq 2\sqrt{2}\,\mathbb{1} \implies \mathrm{tr}(W\rho_{AB}) \leq 2\sqrt{2} = \beta_{\mathcal{Q}}$, so the SOS decomposition is **tight**.

CHSH self-testing

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\right]$$

Observing $\mathrm{tr}(W\rho_{AB}) = 2\sqrt{2}$ implies that:

CHSH self-testing

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\right]$$

Observing $\mathrm{tr}(W\rho_{AB}) = 2\sqrt{2}$ implies that:

1. All measurements are projective on the local supports: $\mathrm{tr}(A_x^2\rho_A) = \mathrm{tr}(B_y^2\rho_B) = 1$.

CHSH self-testing

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\right]$$

Observing $\mathrm{tr}(W\rho_{AB}) = 2\sqrt{2}$ implies that:

1. All measurements are projective on the local supports: $\mathrm{tr}(A_x^2\rho_A) = \mathrm{tr}(B_y^2\rho_B) = 1$.
2. Observables of Alice and Bob satisfy $V_j\rho_{AB} = 0$, e.g.

$$(A_0 \otimes \mathbb{1})\rho_{AB} = \left(\mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}}\right)\rho_{AB}.$$

CHSH self-testing

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (V_0^\dagger V_0 + V_1^\dagger V_1)\right]$$

Observing $\mathrm{tr}(W\rho_{AB}) = 2\sqrt{2}$ implies that:

1. All measurements are projective on the local supports: $\mathrm{tr}(A_x^2\rho_A) = \mathrm{tr}(B_y^2\rho_B) = 1$.
2. Observables of Alice and Bob satisfy $V_j\rho_{AB} = 0$, e.g.

$$(A_0 \otimes \mathbb{1})\rho_{AB} = \left(\mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}}\right)\rho_{AB}.$$

If ρ_A and ρ_B are full-rank, then

$$A_0^2 = \mathbb{1} \implies \left(\frac{B_0 + B_1}{\sqrt{2}}\right)^2 = \mathbb{1} \implies \{B_0, B_1\} = 0.$$

CHSH self-testing

- These algebraic relations determine the form of observables

$$B_0^2 = B_1^2 = \mathbb{1} \quad \text{and} \quad \{B_0, B_1\} = 0 \implies \begin{array}{c} B_0 = U_B(\sigma_x \otimes \mathbb{1})U_B^\dagger \\ B_1 = U_B(\sigma_z \otimes \mathbb{1})U_B^\dagger \end{array}$$

CHSH self-testing

- These algebraic relations determine the form of observables

$$B_0^2 = B_1^2 = \mathbb{1} \quad \text{and} \quad \{B_0, B_1\} = 0 \implies \begin{aligned} B_0 &= U_B(\sigma_x \otimes \mathbb{1})U_B^\dagger \\ B_1 &= U_B(\sigma_z \otimes \mathbb{1})U_B^\dagger \end{aligned}$$

- By symmetry A_0 and A_1 have the same form.
- Construct W and determine the eigenspace corresponding to $\lambda = 2\sqrt{2}$ (essentially a two-qubit operator).

CHSH self-testing

- These algebraic relations determine the form of observables

$$B_0^2 = B_1^2 = \mathbb{1} \quad \text{and} \quad \{B_0, B_1\} = 0 \implies \begin{array}{l} B_0 = U_B(\sigma_x \otimes \mathbb{1})U_B^\dagger \\ B_1 = U_B(\sigma_z \otimes \mathbb{1})U_B^\dagger \end{array}$$

- By symmetry A_0 and A_1 have the same form.
- Construct W and determine the eigenspace corresponding to $\lambda = 2\sqrt{2}$ (essentially a two-qubit operator).

Self-testing (rigidity) statement for CHSH: if $\beta = 2\sqrt{2}$ then

$$\begin{array}{ll} A_0 = U_A(\sigma_x \otimes \mathbb{1})U_A^\dagger & \qquad B_0 = U_B(\sigma_x \otimes \mathbb{1})U_B^\dagger \\ A_1 = U_A(\sigma_z \otimes \mathbb{1})U_A^\dagger & \qquad B_1 = U_B(\sigma_z \otimes \mathbb{1})U_B^\dagger \end{array}$$

and

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

CHSH self-testing

Strategy:

1. Find tight SOS decomposition.
2. Deduce algebraic relations between local observables.
3. Deduce their exact form (up to unitaries and extra degrees of freedom).
4. Construct Bell operator and find eigenspace corresponding to $\beta_{\mathcal{Q}}$.

CHSH self-testing

Strategy:

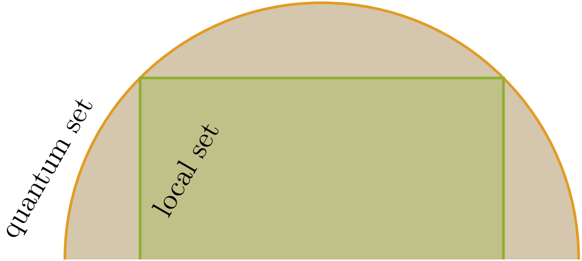
1. Find tight SOS decomposition.
2. Deduce algebraic relations between local observables.
3. Deduce their exact form (up to unitaries and extra degrees of freedom).
4. Construct Bell operator and find eigenspace corresponding to $\beta_{\mathcal{Q}}$.

Outline

- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

A weak form of self-testing

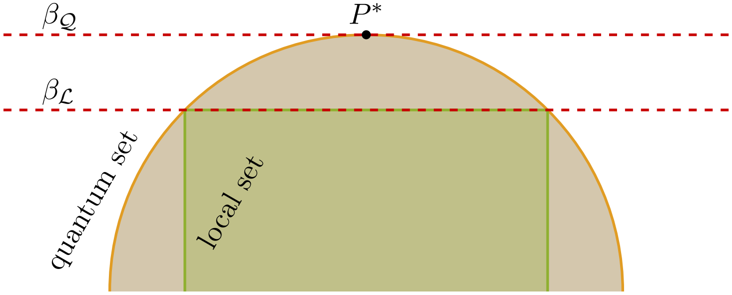
Immediate consequence of self-testing: the maximal violation is achieved by a unique probability point



What about Bell functionals that do not have a unique maximiser?

A weak form of self-testing

Immediate consequence of self-testing: the maximal violation is achieved by a unique probability point



What about Bell functionals that do not have a unique maximiser?

A weak form of self-testing

- In a scenario with 3 inputs and 2 outputs per party consider

$$W = A_0 \otimes (B_0 + B_1 + B_2) + A_1 \otimes (B_0 + B_1 - B_2) + A_2 \otimes (B_0 - B_1).$$

(the correlation part of the infamous I_{3322} functional)

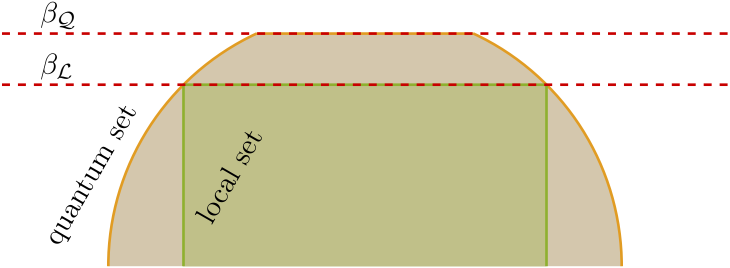
- Easy to show that $\beta_{\mathcal{L}} = 4$ and $\beta_{\mathcal{Q}} = 5$, but the maximal violation is achieved by multiple probability points.

A weak form of self-testing

- In a scenario with 3 inputs and 2 outputs per party consider

  $$W = A_0 \otimes (B_0 + B_1 + B_2) + A_1 \otimes (B_0 + B_1 - B_2) + A_2 \otimes (B_0 - B_1).$$

  (the correlation part of the infamous I_{3322} functional)
- Easy to show that $\beta_{\mathcal{L}} = 4$ and $\beta_{\mathcal{Q}} = 5$, but the maximal violation is achieved by multiple probability points.



no unique maximiser $\implies$ no rigidity statement

can we still have some **weak form of self-testing**?

A weak form of self-testing

- We already have a tight SOS decomposition

$$2W = (2A_0^2 + 2A_1^2 + A_2^2) \otimes \mathbb{1} + \mathbb{1} \otimes (2B_0^2 + 2B_1^2 + B_2^2) - \sum_{j=0}^{2} V_j^\dagger V_j,$$

where

$$\begin{aligned} V_0 &= (A_0 + A_1) \otimes \mathbb{1} - \mathbb{1} \otimes (B_0 + B_1), \\ V_1 &= (A_0 - A_1) \otimes \mathbb{1} - \mathbb{1} \otimes B_2, \\ V_2 &= A_2 \otimes \mathbb{1} - \mathbb{1} \otimes (B_0 - B_1). \end{aligned}$$

A weak form of self-testing

- We already have a tight SOS decomposition

$$2W = (2A_0^2 + 2A_1^2 + A_2^2) \otimes \mathbb{1} + \mathbb{1} \otimes (2B_0^2 + 2B_1^2 + B_2^2) - \sum_{j=0}^{2} V_j^\dagger V_j,$$

where

$$\begin{aligned} V_0 &= (A_0 + A_1) \otimes \mathbb{1} - \mathbb{1} \otimes (B_0 + B_1), \\ V_1 &= (A_0 - A_1) \otimes \mathbb{1} - \mathbb{1} \otimes B_2, \\ V_2 &= A_2 \otimes \mathbb{1} - \mathbb{1} \otimes (B_0 - B_1). \end{aligned}$$

- Observing $\beta = 5$ implies

$$\operatorname{tr}(A_j^2 \rho_A) = \operatorname{tr}(B_j^2 \rho_B) = 1,$$
$$V_j \rho_{AB} = 0$$

for $j = 0, 1, 2$.

A weak form of self-testing

- Let us derive an explicit form of the observables. Rewriting $V_1 \rho_{AB} = 0$ gives

$$\big[(A_0 - A_1) \otimes \mathbb{1}\big]\rho_{AB} = (\mathbb{1} \otimes B_2)\rho_{AB},$$

which combined with the full-rank assumption leads to

$$(A_0 - A_1)^2 = \mathbb{1}.$$

A weak form of self-testing

- Let us derive an explicit form of the observables. Rewriting $V_1 \rho_{AB} = 0$ gives

$$\big[(A_0 - A_1) \otimes \mathbb{1}\big]\rho_{AB} = (\mathbb{1} \otimes B_2)\rho_{AB},$$

which combined with the full-rank assumption leads to

$$(A_0 - A_1)^2 = \mathbb{1}.$$

- Together with projectivity this gives

$$\begin{aligned}\mathcal{H}_A &\equiv \mathbb{C}^2 \otimes \mathbb{C}^{d_A},\\ A_0 &= \Big(\cos\frac{\pi}{6}\,\mathsf{X} + \sin\frac{\pi}{6}\,\mathsf{Z}\Big) \otimes \mathbb{1},\\ A_1 &= \Big(\cos\frac{\pi}{6}\,\mathsf{X} - \sin\frac{\pi}{6}\,\mathsf{Z}\Big) \otimes \mathbb{1}.\end{aligned}$$

(up to a choice of basis)

A weak form of self-testing

- Combining $V_0\rho_{AB} = 0$ and $V_2\rho_{AB} = 0$ gives
$$\frac{1}{2}\big[(A_0 + A_1 + A_2) \otimes \mathbb{1}\big]\rho_{AB} = (\mathbb{1} \otimes B_2)\rho_{AB}$$
and finally
$$(A_0 + A_1 + A_2)^2 = 4\,\mathbb{1}.$$

A weak form of self-testing

- Combining $V_0\rho_{AB} = 0$ and $V_2\rho_{AB} = 0$ gives
$$\frac{1}{2}\big[(A_0 + A_1 + A_2) \otimes \mathbb{1}\big]\rho_{AB} = (\mathbb{1} \otimes B_2)\rho_{AB}$$
and finally
$$(A_0 + A_1 + A_2)^2 = 4\,\mathbb{1}.$$

- Plugging in the previously derived characterisation of A_0, A_1 gives
$$(2\cos\frac{\pi}{6}\,\mathsf{X} \otimes \mathbb{1} + A_2)^2 = 4\,\mathbb{1}.$$

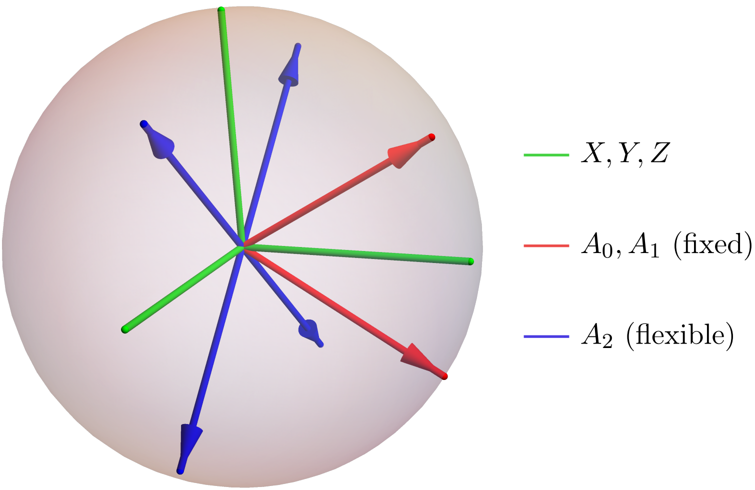
A weak form of self-testing

- Combining $V_0 \rho_{AB} = 0$ and $V_2 \rho_{AB} = 0$ gives
$$\frac{1}{2}\big[(A_0 + A_1 + A_2) \otimes \mathbb{1}\big]\rho_{AB} = (\mathbb{1} \otimes B_2)\rho_{AB}$$
and finally
$$(A_0 + A_1 + A_2)^2 = 4\,\mathbb{1}.$$

- Plugging in the previously derived characterisation of A_0, A_1 gives
$$(2\cos\frac{\pi}{6}\,\mathsf{X} \otimes \mathbb{1} + A_2)^2 = 4\,\mathbb{1}.$$

- Simple algebra yields
$$A_2 = \sum_{j=1}^{d_A} \big(\cos u_j\,\mathsf{Y} + \sin u_j\,\mathsf{Z}\big) \otimes |e_j\rangle\langle e_j|,$$
where $u_j \in [0, 2\pi)$ and $\{|e_j\rangle\}_{j=1}^{d_A}$ is an orthonormal basis on $\mathbb{C}^{d_A}$.

A weak form of self-testing



A weak form of self-testing

- By symmetry the same characterisation holds for the observables of Bob. The Bell operator reads

$$W = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} R(u_j, v_k) \otimes |e_j\rangle\langle e_j| \otimes |f_k\rangle\langle f_k|,$$

where $R(u_j, v_k)$ is a two-qubit operator.

A weak form of self-testing

- By symmetry the same characterisation holds for the observables of Bob. The Bell operator reads

$$W = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} R(u_j, v_k) \otimes |e_j\rangle\langle e_j| \otimes |f_k\rangle\langle f_k|,$$

  where $R(u_j, v_k)$ is a two-qubit operator.
- Diagonalising $R(u_j, v_k)$ shows that $\lambda = 5$ belong to the spectrum iff $u_j = v_k$.

A weak form of self-testing

- By symmetry the same characterisation holds for the observables of Bob. The Bell operator reads

$$W = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} R(u_j, v_k) \otimes |e_j\rangle\langle e_j| \otimes |f_k\rangle\langle f_k|,$$

  where $R(u_j, v_k)$ is a two-qubit operator.
- Diagonalising $R(u_j, v_k)$ shows that $\lambda = 5$ belong to the spectrum iff $u_j = v_k$.
- The corresponding eigenvector is the standard maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (**smart** parameterisation)

A weak form of self-testing

- By symmetry the same characterisation holds for the observables of Bob. The Bell operator reads

$$W = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} R(u_j, v_k) \otimes |e_j\rangle\langle e_j| \otimes |f_k\rangle\langle f_k|,$$

  where $R(u_j, v_k)$ is a two-qubit operator.
- Diagonalising $R(u_j, v_k)$ shows that $\lambda = 5$ belong to the spectrum iff $u_j = v_k$.
- The corresponding eigenvector is the standard maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (**smart** parameterisation)
- Finally, the global state must be of the form

$$\rho_{AB} = \Phi^+_{A'B'} \otimes \sigma_{A''B''},$$

  where $\sigma_{A''B''}$ is a normalised state satisfying

$$\mathrm{tr}\left(\sigma_{A''B''} |e_j\rangle\langle e_j| \otimes |f_k\rangle\langle f_k|\right) = 0 \quad \text{if} \quad u_j \neq v_k.$$

A weak form of self-testing

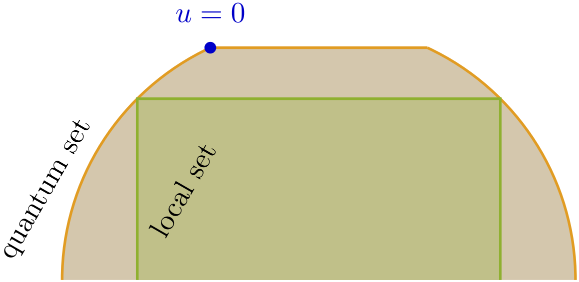
Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

What happens in the space of correlations?

A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

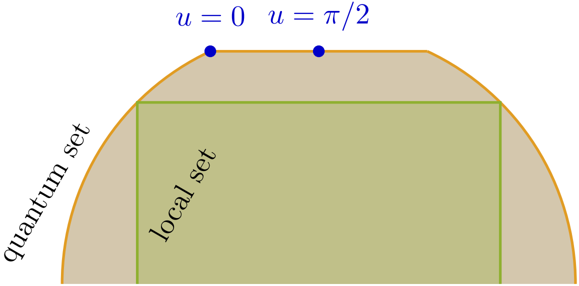
What happens in the space of correlations?



A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

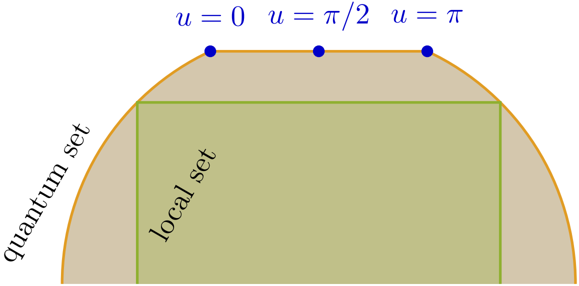
What happens in the space of correlations?



A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

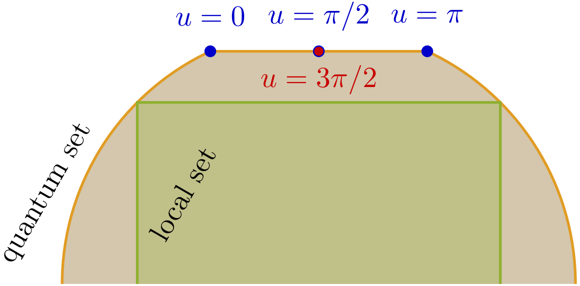
What happens in the space of correlations?



A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

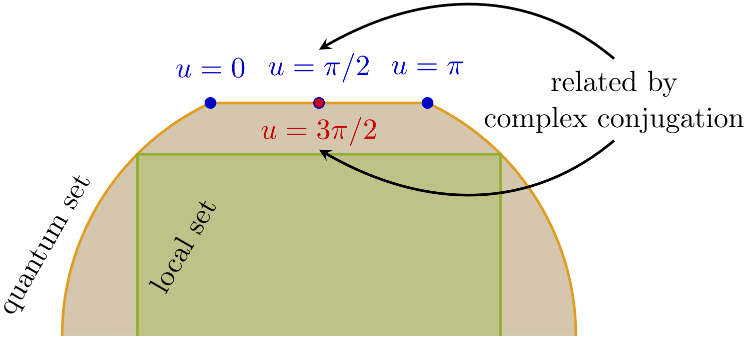
What happens in the space of correlations?



A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

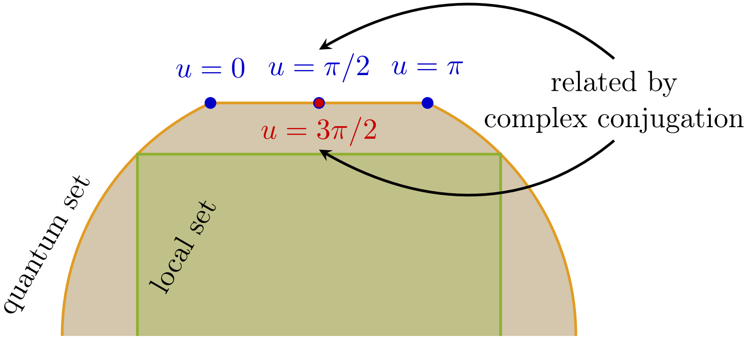
What happens in the space of correlations?



A weak form of self-testing

Conclusion: there is a family of optimal strategies parametrised by $u \in [0, 2\pi)$ and **every optimal strategy is just a convex combination** of those.

What happens in the space of correlations?



1. The face is a line segment.
2. The endpoints are self-tests in the usual strong sense.

Outline

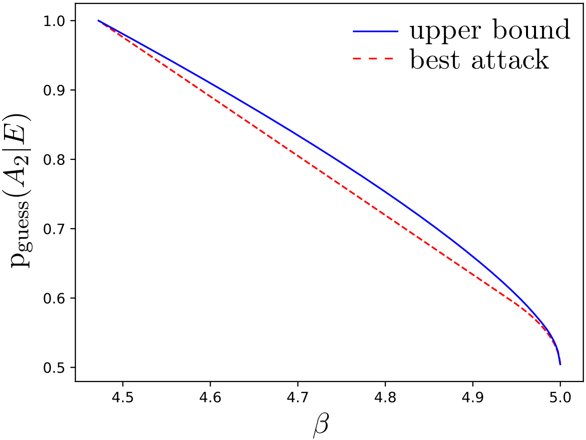
- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

Certifying randomness

Setup: Alice and Bob observe Bell violation, Eve is trying to guess the outcome of Alice for a specific setting. We start with A_2:

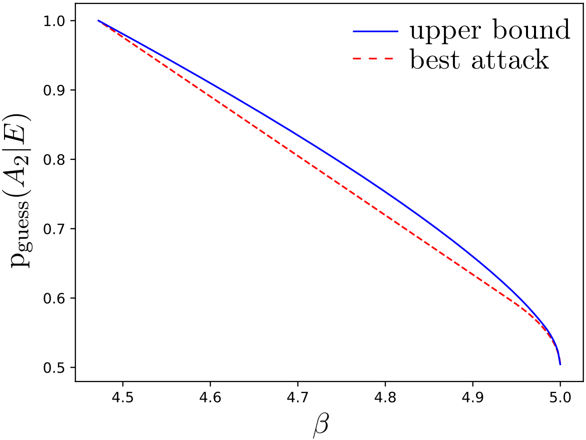
Certifying randomness

Setup: Alice and Bob observe Bell violation, Eve is trying to guess the outcome of Alice for a specific setting. We start with A_2:



Certifying randomness

Setup: Alice and Bob observe Bell violation, Eve is trying to guess the outcome of Alice for a specific setting. We start with A_2:



randomness guaranteed only when $\beta > 4.5$

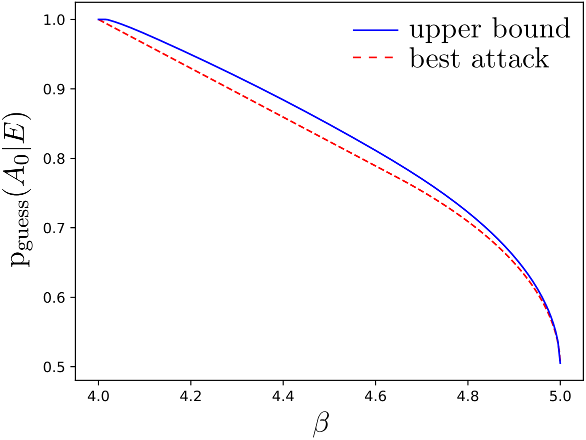
$(\beta_{\mathcal{L}} = 4)$

Certifying randomness

Luckily A_0 and A_1 are **much better**!

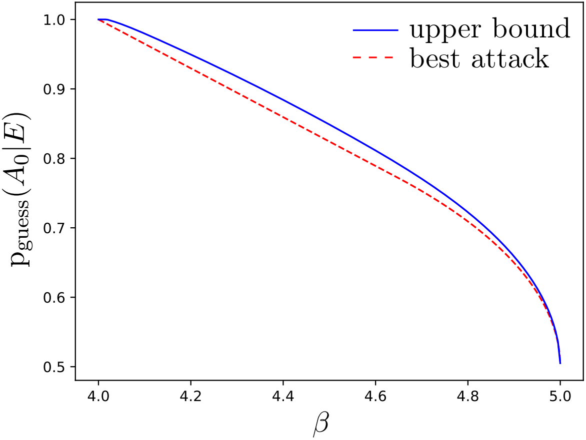
Certifying randomness

Luckily A_0 and A_1 are **much better**!



Certifying randomness

Luckily A_0 and A_1 are **much better**!



randomness guaranteed for all $\beta > 4$

randomness profile similar to CHSH

Outline

- Bell nonlocality
- Strong self-testing (CHSH)
- Weak self-testing
- Certifying randomness
- Conclusions and open questions

Conclusions:

- A new weak form of self-testing: the maximal violation certifies the state, but not the measurements.
- Nevertheless, the randomness certification power is not significantly affected.

Conclusions:

- A new weak form of self-testing: the maximal violation certifies the state, but not the measurements.
- Nevertheless, the randomness certification power is not significantly affected.

Open questions:

- Is the self-testing robust? How to construct an extraction channel which depends on 3 observables (instead of the usual 2)?
- Can we find a scenario in which the non-rigidty has a significant impact, e.g. for randomness certification?
- Can we find a bipartite Bell inequality which can be maximally violated by distinct states? (exists for 3 parties)

Conclusions:

- A new weak form of self-testing: the maximal violation certifies the state, but not the measurements.
- Nevertheless, the randomness certification power is not significantly affected.

Open questions:

- Is the self-testing robust? How to construct an extraction channel which depends on 3 observables (instead of the usual 2)?
- Can we find a scenario in which the non-rigidty has a significant impact, e.g. for randomness certification?
- Can we find a bipartite Bell inequality which can be maximally violated by distinct states? (exists for 3 parties)

see also related independent work by Jebarathinam et al. `arXiv:1905.09867` (based on lifting)

Conclusions:

- A new weak form of self-testing: the maximal violation certifies the state, but not the measurements.
- Nevertheless, the randomness certification power is not significantly affected.

Open questions:

- Is the self-testing robust? How to construct an extraction channel which depends on 3 observables (instead of the usual 2)?
- Can we find a scenario in which the non-rigidty has a significant impact, e.g. for randomness certification?
- Can we find a bipartite Bell inequality which can be maximally violated by distinct states? (exists for 3 parties)

see also related independent work by Jebarathinam et al. `arXiv:1905.09867` (based on lifting)

Thank you for your attention!