Self-testing of qutrit systems

Jędrzej Kaniewski

QMATH, Department of Mathematical Sciences

University of Copenhagen, Denmark

joint work with

Antonio Acín, Remigiusz Augusiak, Flavio Baccari, Alexia Salavrakos, Ivan Šupić, Jordi Tura

CEQIP '18

15 June 2018

QMATH Centre for the Mathematics of Quantum Theory

Outline

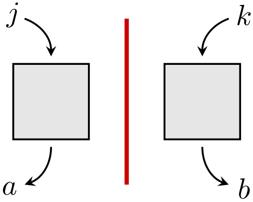
- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Outline

- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Bell nonlocality

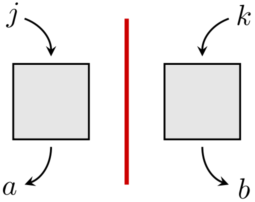
Bell scenario



$P(a, b|j, k)$

Bell nonlocality

Bell scenario



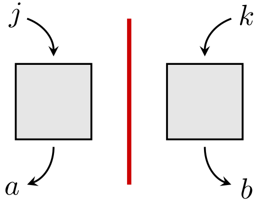
$P(a, b|j, k)$

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

$$P(a, b|j, k) = \text{tr}\left[(F_a^j \otimes G_b^k)\rho_{AB}\right].$$

Bell nonlocality

Bell scenario



$P(a,b|j,k)$

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

$$P(a,b|j,k) = \mathrm{tr}\left[(F_a^j \otimes G_b^k)\rho_{AB}\right].$$

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

$$P(a,b|j,k) = \sum_\lambda p(\lambda)\, p_A(a|j,\lambda)\, p_B(b|k,\lambda).$$

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 $C = (c_{abjk})$ define

$$\langle C, P \rangle := \sum_{abjk} c_{abjk} P(a, b|j, k)$$

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 $C = (c_{abjk})$ define

$$\langle C, P \rangle := \sum_{abjk} c_{abjk} P(a, b|j, k)$$

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

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

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

Bell nonlocality

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

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

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

Nonlocality $\implies$ **entanglement**

Bell nonlocality

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

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

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

Nonlocality $\implies$ **entanglement**

can we make this connection more explicit/rigorous?

Outline

- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Self-testing

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

deduce properties of ρ_{AB}, $\{F_a^j\}$, $\{G_b^k\}$

Self-testing

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

deduce properties of ρ_{AB}, $\{F_a^j\}$, $\{G_b^k\}$

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

Self-testing

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

deduce properties of ρ_{AB}, $\{F_a^j\}$, $\{G_b^k\}$

(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

$$\langle C, P \rangle = \beta$$

Self-testing

Given $P(a,b|j,k) = \text{tr}\left[(F_a^j \otimes G_b^k)\rho_{AB}\right]$

deduce properties of ρ_{AB}, $\{F_a^j\}$, $\{G_b^k\}$

(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

$$\langle C, P \rangle = \beta$$

might seem like a hopeless task...

...but often can deduce **essentially everything**!

Outline

- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Sum-of-squares decomposition

Given a Bell functional C, how to compute $\beta_{\mathcal{Q}} = \max_{P \in \mathcal{Q}} \langle C, P \rangle$?
Easy to provide **lower** bounds, what about **upper** bounds?

Sum-of-squares decomposition

Given a Bell functional C, how to compute $\beta_{\mathcal{Q}} = \max_{P \in \mathcal{Q}} \langle C, P \rangle$?
Easy to provide **lower** bounds, what about **upper** bounds?

1. Construct **Bell operator**

$$W := \sum_{abjk} c_{abjk} F_a^j \otimes G_b^k$$

Sum-of-squares decomposition

Given a Bell functional C, how to compute $\beta_{\mathcal{Q}} = \max_{P \in \mathcal{Q}} \langle C, P \rangle$?
Easy to provide **lower** bounds, what about **upper** bounds?

1. Construct **Bell operator**

$$W := \sum_{abjk} c_{abjk} F_a^j \otimes G_b^k$$

2. Prove that for all measurements

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

for $c \in \mathbb{R}$

Sum-of-squares decomposition

Given a Bell functional C, how to compute $\beta_{\mathcal{Q}} = \max_{P \in \mathcal{Q}} \langle C, P \rangle$?
Easy to provide **lower** bounds, what about **upper** bounds?

1. Construct **Bell operator**

$$W := \sum_{abjk} c_{abjk} F_a^j \otimes G_b^k$$

2. Prove that for all measurements

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

   for $c \in \mathbb{R}$

3. Then $\beta_Q \leq c$ because for all quantum realisations

$$\langle C, P \rangle = \mathrm{tr}(W \rho_{AB}) \leq c\, \mathrm{tr}(\rho_{AB}) = c$$

Sum-of-squares decomposition

Q: How to show that $W \leq c\,\mathbb{1}$ for all measurements?

Sum-of-squares decomposition

Q: How to show that $W \leq c\,\mathbb{1}$ for all measurements?

A: Write difference as sum of squares

$$c\,\mathbb{1} - W \geq \sum_j L_j^\dagger L_j .$$

(operators L_j depend on measurement operators)

- if $\beta_Q = c \implies$ sum-of-squares (SOS) decomposition is **tight**

Outline

- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Example: the CHSH inequality

- the CHSH operator

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

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

Example: the CHSH inequality

- the CHSH operator

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

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

$$L_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}}$$

$$L_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}$$

Example: the CHSH inequality

- the CHSH operator

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

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

$$L_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}}$$
$$L_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}$$

- check

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

Example: the CHSH inequality

- the CHSH operator

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

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

$$L_0 = A_0 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 + B_1}{\sqrt{2}}$$
$$L_1 = A_1 \otimes \mathbb{1} - \mathbb{1} \otimes \frac{B_0 - B_1}{\sqrt{2}}$$

- check

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

- $W \leq 2\sqrt{2}\,\mathbb{1}$ and $\beta_{\mathcal{Q}} = 2\sqrt{2}$, so the SOS decomposition is **tight**

Example: the CHSH inequality

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

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

Example: the CHSH inequality

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

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

1. all measurements are projective on the local supports: $\mathrm{tr}(A_j^2\rho_A) = \mathrm{tr}(B_k^2\rho_B) = 1$

Example: the CHSH inequality

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

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

1. all measurements are projective on the local supports: $\mathrm{tr}(A_j^2\rho_A) = \mathrm{tr}(B_k^2\rho_B) = 1$
2. observables of Alice and Bob satisfy $L_j\rho_{AB} = 0$

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

Example: the CHSH inequality

$$W = \frac{1}{\sqrt{2}}\left[(A_0^2 + A_1^2) \otimes \mathbb{1} + \mathbb{1} \otimes (B_0^2 + B_1^2) - (L_0^\dagger L_0 + L_1^\dagger L_1)\right]$$

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

1. all measurements are projective on the local supports: $\mathrm{tr}(A_j^2\rho_A) = \mathrm{tr}(B_k^2\rho_B) = 1$
2. observables of Alice and Bob satisfy $L_j\rho_{AB} = 0$

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

if ρ_A and ρ_B are full-rank, then

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

Example: the CHSH inequality

- the relation determines form of observables

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

Example: the CHSH inequality

- the relation determines form of observables

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

- the inequality is symmetric, so A_0 and A_1 have the same form
- construct W and determine the eigenspace corresponding to $2\sqrt{2}$

Example: the CHSH inequality

- the relation determines form of observables

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

- the inequality is symmetric, so A_0 and A_1 have the same form
- construct W and determine the eigenspace corresponding to $2\sqrt{2}$

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

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

and

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

Example: the CHSH inequality

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 $\beta_{\mathcal{Q}}$

Example: the CHSH inequality

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
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Result 1: SATWAP inequality

- maximally violated by **maximally entangled state** and **CGLMP measurements** (Remik's talk)
- CGLMP measurement in dimension d for $\phi \in [0, 2\pi]$

$$|e_j^\phi\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(j-\phi)k} |k\rangle \quad \text{for} \quad \omega := \exp(2\pi i/d)$$

Result 1: SATWAP inequality

- maximally violated by **maximally entangled state** and **CGLMP measurements** (Remik's talk)
- CGLMP measurement in dimension d for $\phi \in [0, 2\pi]$

$$|e_j^{\phi}\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(j-\phi)k} |k\rangle \quad \text{for} \quad \omega := \exp(2\pi i/d)$$

- we look at **2** inputs and **3** outputs, optimal angles $\phi_0 = 0$, $\phi_1 = 1/2$; computing $|\langle e_{j'}^{1/2}|e_j^0\rangle|$ gives

$j \backslash j'$	0	1	2
0	2/3	2/3	1/3
1	1/3	2/3	2/3
2	2/3	1/3	2/3

not mutually unbiased

Result 1: SATWAP inequality

- SOS written in terms of observables (unitary for projective measurements)

$$A_j = \sum_a \omega^a F_a^j$$

$$B_k = \sum_b \omega^b G_b^k$$

Result 1: SATWAP inequality

- SOS written in terms of observables (unitary for projective measurements)

$$A_j = \sum_a \omega^a F_a^j$$
$$B_k = \sum_b \omega^b G_b^k$$

- SOS decomposition and some algebra $\implies$ **projectivity** and

$$\omega^2 B_0^\dagger + \omega B_1^\dagger = -\{B_0, B_1\}$$

Result 1: SATWAP inequality

- SOS written in terms of observables (unitary for projective measurements)

$$A_j = \sum_a \omega^a F_a^j$$
$$B_k = \sum_b \omega^b G_b^k$$

- SOS decomposition and some algebra $\implies$ **projectivity** and

$$\omega^2 B_0^\dagger + \omega B_1^\dagger = -\{B_0, B_1\}$$

- more algebra... $\implies$ B_0, B_1 are the CGLMP measurements acting on a qutrit (up to usual equivalences)

Result 1: SATWAP inequality

- SOS written in terms of observables (unitary for projective measurements)

$$A_j = \sum_a \omega^a F_a^j$$
$$B_k = \sum_b \omega^b G_b^k$$

- SOS decomposition and some algebra $\implies$ **projectivity** and

$$\omega^2 B_0^\dagger + \omega B_1^\dagger = -\{B_0, B_1\}$$

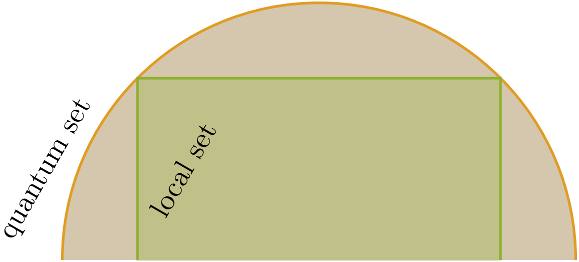
- more algebra... $\implies$ B_0, B_1 are the CGLMP measurements acting on a qutrit (up to usual equivalences)
- construct Bell operator $\implies$ ...

Result 1: SATWAP inequality

Result: Self-testing statement for SATWAP for $d = 3$

Result 1: SATWAP inequality

Result: Self-testing statement for SATWAP for $d = 3$
Cor. 1: SATWAP functional has a unique maximiser

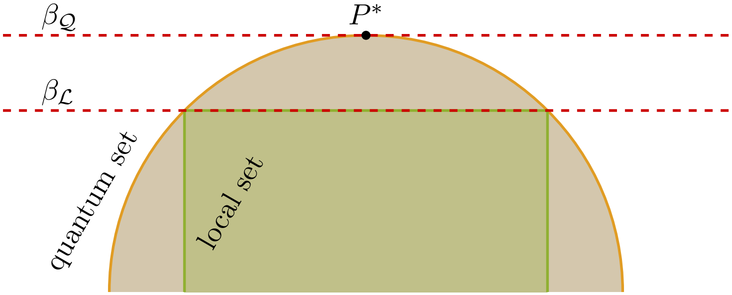


Cor. 2: The maximal violation certifies $\log 3$ bits of local randomness
$\Longrightarrow$ could use for cryptography

Result 1: SATWAP inequality

Result: Self-testing statement for SATWAP for $d = 3$

Cor. 1: SATWAP functional has a unique maximiser

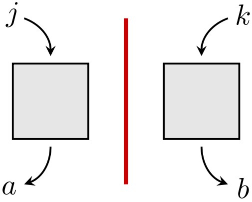


Cor. 2: The maximal violation certifies $\log 3$ bits of local randomness $\implies$ could use for cryptography

Outline

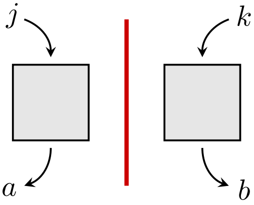
- Bell nonlocality
- Self-testing
- Sum-of-squares decomposition
- Example: CHSH inequality
- Result 1: SATWAP inequality
- Result 2: generalised CHSH inequality

Result 2: generalised CHSH inequality



$$P(a, b|j, k)$$

Result 2: generalised CHSH inequality

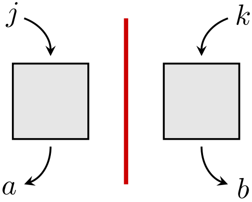


$P(a, b|j, k)$

CHSH: $a, b, j, k \in \{0, 1\}$

win $\iff a \oplus b \oplus jk = 0$

Result 2: generalised CHSH inequality



$P(a, b|j, k)$

CHSH: $a, b, j, k \in \{0, 1\}$

win $\iff a \oplus b \oplus jk = 0$

CHSH$_d$: $a, b, j, k \in \{0, 1, \ldots, d-1\}$

win $\iff a + b + jk \equiv 0 \mod d$

Result 2: generalised CHSH inequality

- Buhrman and Massar ('05) proposed and studied $d = 3$
- Ji et al. ('08) and Liang et al. ('09) studied higher d (mainly prime)

Result 2: generalised CHSH inequality

- Buhrman and Massar ('05) proposed and studied $d = 3$
- Ji et al. ('08) and Liang et al. ('09) studied higher d (mainly prime)
- **inconclusive!** classical value, quantum value, optimal realisation: **not understood**

Result 2: generalised CHSH inequality

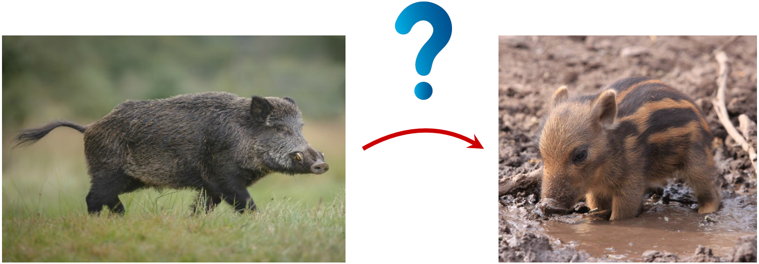
- Buhrman and Massar ('05) proposed and studied $d = 3$
- Ji et al. ('08) and Liang et al. ('09) studied higher d (mainly prime)
- **inconclusive!** classical value, quantum value, optimal realisation: **not understood**
- **conclusion:** this Bell functional seems natural, but turns out to be ill-behaved

Result 2: generalised CHSH inequality

- Buhrman and Massar ('05) proposed and studied $d = 3$
- Ji et al. ('08) and Liang et al. ('09) studied higher d (mainly prime)
- **inconclusive!** classical value, quantum value, optimal realisation: **not understood**
- **conclusion:** this Bell functional seems natural, but turns out to be ill-behaved

Result 2: generalised CHSH inequality

- Buhrman and Massar ('05) proposed and studied $d = 3$
- Ji et al. ('08) and Liang et al. ('09) studied higher d (mainly prime)
- **inconclusive!** classical value, quantum value, optimal realisation: **not understood**
- **conclusion:** this Bell functional seems natural, but turns out to be ill-behaved



Result 2: generalised CHSH inequality

- Bell operator reads

$$W_d := \frac{1}{d^3} \sum_{n=0}^{d-1} \sum_{j,k=0}^{d-1} \omega^{njk} A_j^n \otimes B_k^n$$

Result 2: generalised CHSH inequality

- Bell operator reads

$$W_d := \frac{1}{d^3} \sum_{n=0}^{d-1} \sum_{j,k=0}^{d-1} \omega^{njk} A_j^n \otimes B_k^n$$

- we consider prime d and

$$W_d' := \frac{1}{d^3} \sum_{n=0}^{d-1} \lambda_{n,d} \sum_{j,k=0}^{d-1} \omega^{njk} A_j^n \otimes B_k^n$$

for $\lambda_{n,d} \in \mathbb{C}$, $|\lambda_{n,d}| = 1$

Result 2: generalised CHSH inequality

- Bell operator reads

$$W_d := \frac{1}{d^3} \sum_{n=0}^{d-1} \sum_{j,k=0}^{d-1} \omega^{njk} A_j^n \otimes B_k^n$$

- we consider prime d and

$$W_d' := \frac{1}{d^3} \sum_{n=0}^{d-1} \lambda_{n,d} \sum_{j,k=0}^{d-1} \omega^{njk} A_j^n \otimes B_k^n$$

  for $\lambda_{n,d} \in \mathbb{C}$, $|\lambda_{n,d}| = 1$

- for the right choice of $\lambda_{n,d}$ the quantum value can be computed **analytically** (tight SOS decomposition)!

Result 2: generalised CHSH inequality

- quantum realisation achieving the quantum value

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle$$

$$B_k = \omega^{k(k+1)} X Z^k$$

$$A_j = \dots$$

- the observables correspond to d distinct bases which are pairwise mutually unbiased
- for $d = 3$ SOS relations allow us to prove self-testing!

Result 2: generalised CHSH inequality

For $d = 3$ the phases are:

$$\lambda_{0,d} = 1, \quad \lambda_{1,d} = e^{-i\pi/18}, \quad \lambda_{2,d} = e^{+i\pi/18}$$
$$(e^{-i\pi/18} \approx 0.9849 - 0.1737i \approx 1)$$

- SOS + algebra $\implies$ **projectivity** and
$$B_0^\dagger = -\omega\{B_1, B_2\} \quad \text{(and perm.)}$$
- this is sufficient to deduce the form of observables...

Result 2: generalised CHSH inequality

For $d = 3$ the phases are:

$$\lambda_{0,d} = 1, \quad \lambda_{1,d} = e^{-i\pi/18}, \quad \lambda_{2,d} = e^{+i\pi/18}$$
$$(e^{-i\pi/18} \approx 0.9849 - 0.1737i \approx 1)$$

- SOS + algebra $\implies$ **projectivity** and

$$B_0^\dagger = -\omega\{B_1, B_2\} \quad \text{(and perm.)}$$

- this is sufficient to deduce the form of observables...
  ...except that now there are two inequivalent solutions

$$(B_0, B_1, B_2) \not\equiv (B_0^{\mathrm{T}}, B_1^{\mathrm{T}}, B_2^{\mathrm{T}}) \quad \textbf{not unitarily equivalent}$$
$$(\sigma_x, \sigma_y, \sigma_z) \not\equiv (\sigma_x, -\sigma_y, \sigma_z)$$

- local Hilbert spaces decompose into the "right-" and "left-handed" subspace and maximal violation possible only if Alice and Bob use opposite types!

Result 2: generalised CHSH inequality

Maximal violation certifies:

- $|\Phi\rangle = \frac{1}{\sqrt{3}} \sum_{j=0}^{2} |j\rangle|j\rangle$
- specific MUB measurements for each party
- the two measurements must be of the opposite type

Result 2: generalised CHSH inequality

Maximal violation certifies:

- $|\Phi\rangle = \frac{1}{\sqrt{3}} \sum_{j=0}^{2} |j\rangle|j\rangle$
- specific MUB measurements for each party
- the two measurements must be of the opposite type

Corollaries:

- has unique maximiser in $\mathcal{Q}$
- certifies $\log 3$ bits of local randomness

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test
- proposed a family of Bell inequalities maximally violated by the maximally entangled state and MUB measurements

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test
- proposed a family of Bell inequalities maximally violated by the maximally entangled state and MUB measurements
- for $d = 3$ this a self-test (right/left-handed twist!)

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test
- proposed a family of Bell inequalities maximally violated by the maximally entangled state and MUB measurements
- for $d = 3$ this a self-test (right/left-handed twist!)
- self-testing results **not relying** on self-testing of qubit subspaces

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test
- proposed a family of Bell inequalities maximally violated by the maximally entangled state and MUB measurements
- for $d = 3$ this a self-test (right/left-handed twist!)
- self-testing results **not relying** on self-testing of qubit subspaces

Open questions:

- extend SATWAP self-testing to arbitrary d
- extend generalised CHSH self-testing to arbitrary prime d

Conclusions and open questions

Conclusions:

- SATWAP inequality for $d = 3$ is a self-test
- proposed a family of Bell inequalities maximally violated by the maximally entangled state and MUB measurements
- for $d = 3$ this a self-test (right/left-handed twist!)
- self-testing results **not relying** on self-testing of qubit subspaces

Open questions:

- extend SATWAP self-testing to arbitrary d
- extend generalised CHSH self-testing to arbitrary prime d
- **robustness!**


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