Title: Self-testing Bell inequalities from the stabiliser formalism and their applications

Speakers: Flavio Baccari

Series: Quantum Foundations

Date: December 11, 2020 - 12:00 PM

URL: http://pirsa.org/20120017

Abstract: I will introduce a tool to construct self-testing Bell inequalities from the stabiliser formalism and present two applications in the framework of device-independent certification protocols. Firstly, I will show how the method allows to derive Bell inequalities maximally violated by the family of multi-qubit graph states and suited for their robust self-testing. Secondly, I will present how the same method allows to introduce the first examples of subspace self-testing, a form of certification that the measured quantum state belongs to a given quantum error correction code subspace, which remarkably includes also mixed states.

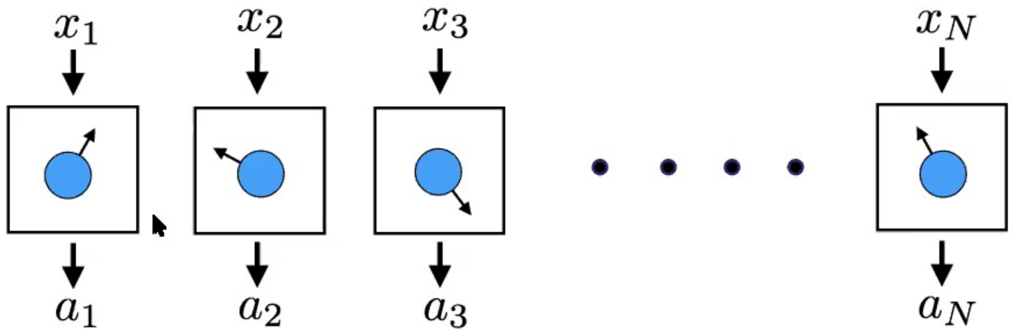
Self-testing Bell inequalities from the stabiliser formalism and their applications

Flavio Baccari, Remigiusz Augusiak, Ivan Šupić,
Jordi Tura and Antonio Acín

The framework

Device-independent protocols

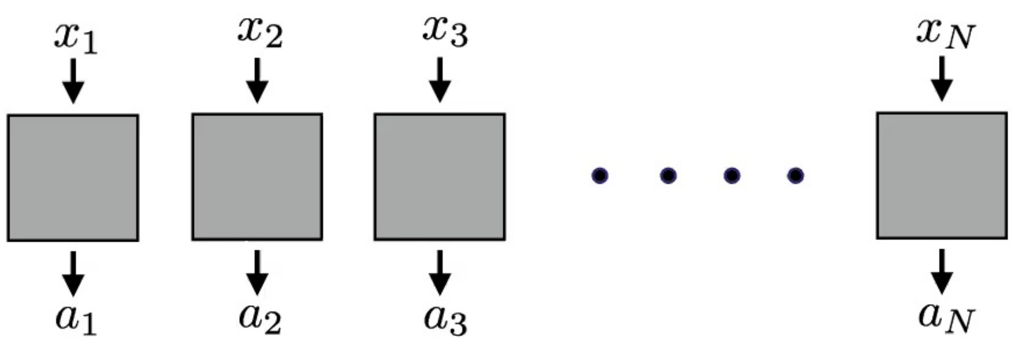
measurements choices



measurements outcomes

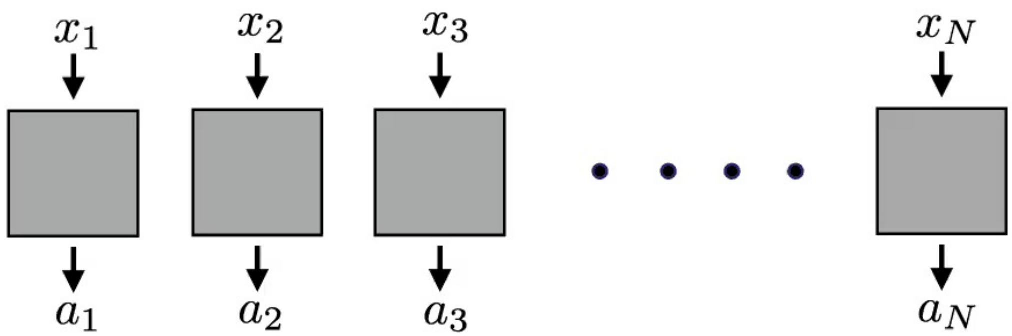
$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) = \langle \psi | M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N} | \psi \rangle$$

Device-independent protocols



$$p(a_1, \ldots, a_N | x_1, \ldots, x_N)$$

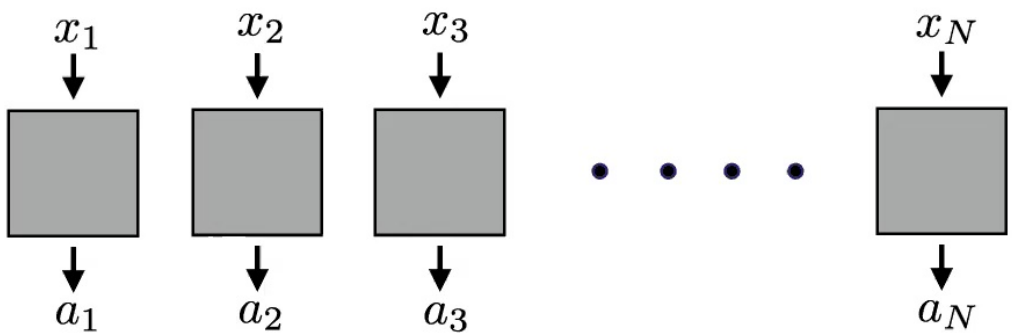
Device-independent protocols



$$p(a_1, \ldots, a_N | x_1, \ldots, x_N)$$

→ **Infer properties on the underlying state and measurements**

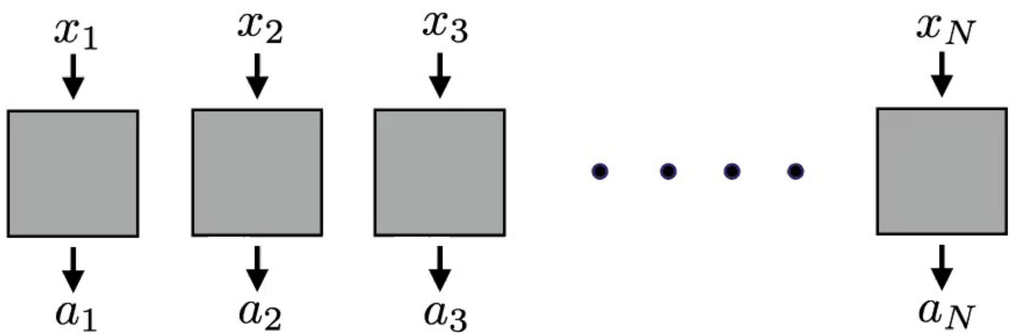
Device-independent protocols



Local correlations = what can be achieved classically

$$p(a_1,\dots,a_N|x_1,\dots,x_N) \;=\int d\lambda p(\lambda)p(a_1|x_1,\lambda)\dots p(a_N|x_N,\lambda)$$

Device-independent protocols



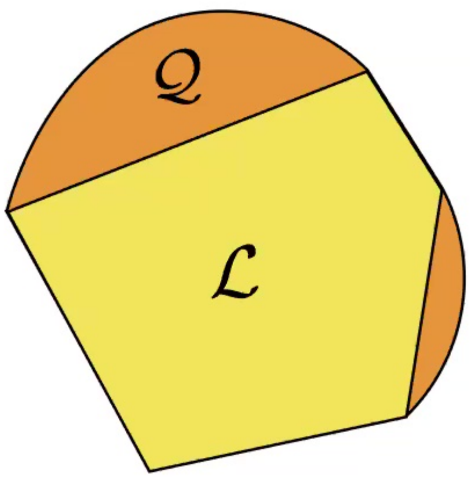
Nonlocal correlations = Resource

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) \neq \int d\lambda p(\lambda) p(a_1|x_1, \lambda) \ldots p(a_N|x_N, \lambda)$$

The geometrical picture

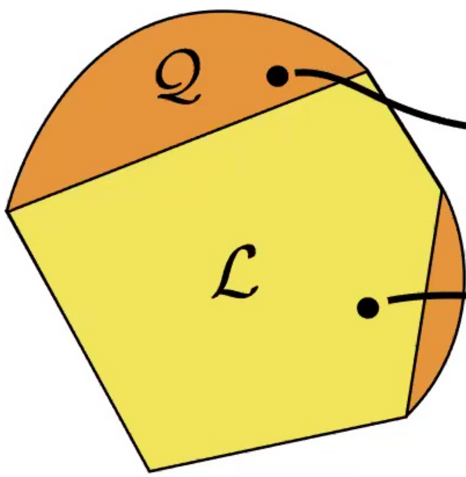
Sets of correlations

$$\vec{p} = (\{p(a_1, \ldots, a_N | x_1, \ldots, x_N)\})$$



The geometrical picture

Sets of correlations $\vec{p} = (\{p(a_1, \ldots, a_N | x_1, \ldots, x_N)\})$



Quantum

$$\langle \psi | M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N} | \psi \rangle$$

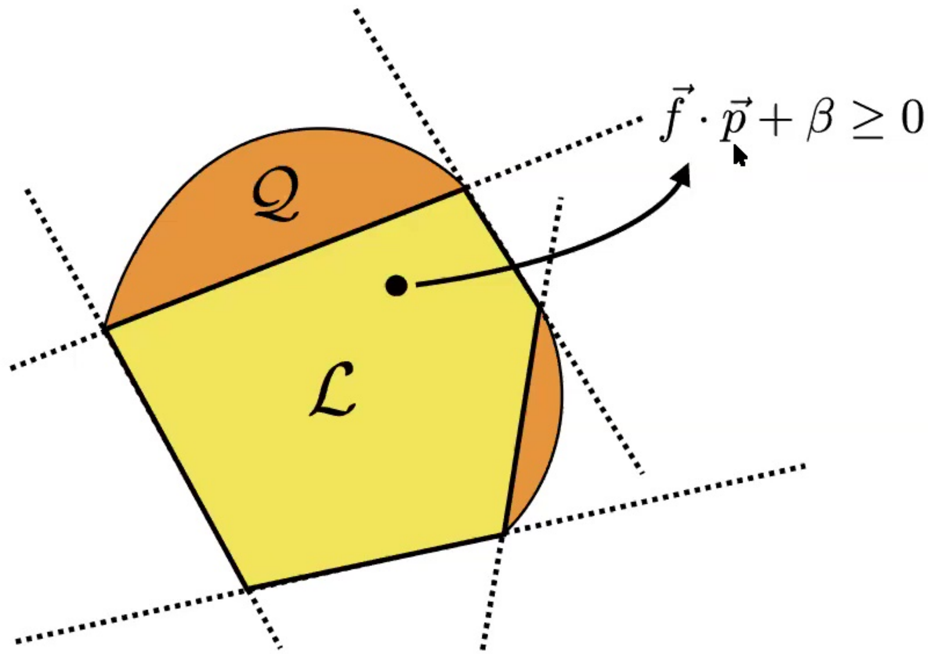
Local

$$\int d\lambda p(\lambda) p(a_1 | x_1, \lambda) \ldots p(a_N | x_N, \lambda)$$

The geometrical picture

Sets of correlations $\vec{p} = (\{p(a_1, \ldots, a_N | x_1, \ldots, x_N)\})$

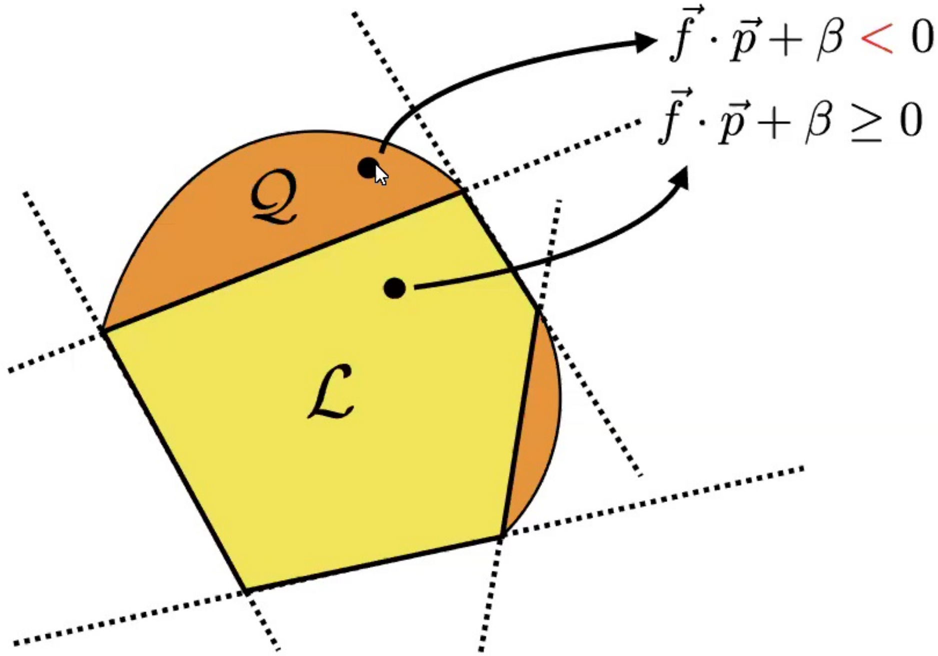
A fundamental tool for DI protocols: **Bell inequalities**

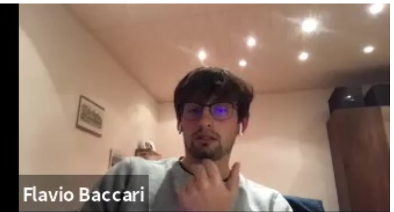


The geometrical picture

Sets of correlations $\vec{p} = (\{p(a_1, \ldots, a_N | x_1, \ldots, x_N)\})$

A fundamental tool for DI protocols: **Bell inequalities**





Self-testing of states

$$p(a_1, \ldots, a_N | x_1, \ldots, x_N) \longrightarrow |\psi\rangle$$

Inferring directly the state from the correlations

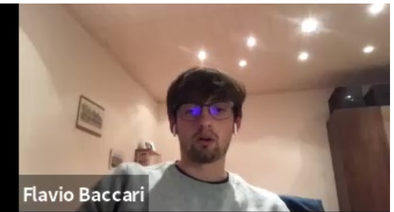
Possible up to undetectable symmetries = **local isometries**

Formal self-testing statement

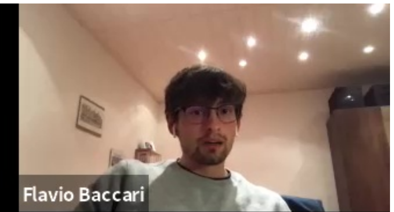
$$U_1 \otimes \ldots \otimes U_N (|\phi\rangle \otimes |+\rangle^{\otimes N}) \quad = \quad |\psi\rangle \otimes |\text{junk}\rangle$$

State producing the observed correlations

Uncorrelated degrees of freedom



An example



CHSH and the maximally entangled two-qubit state

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

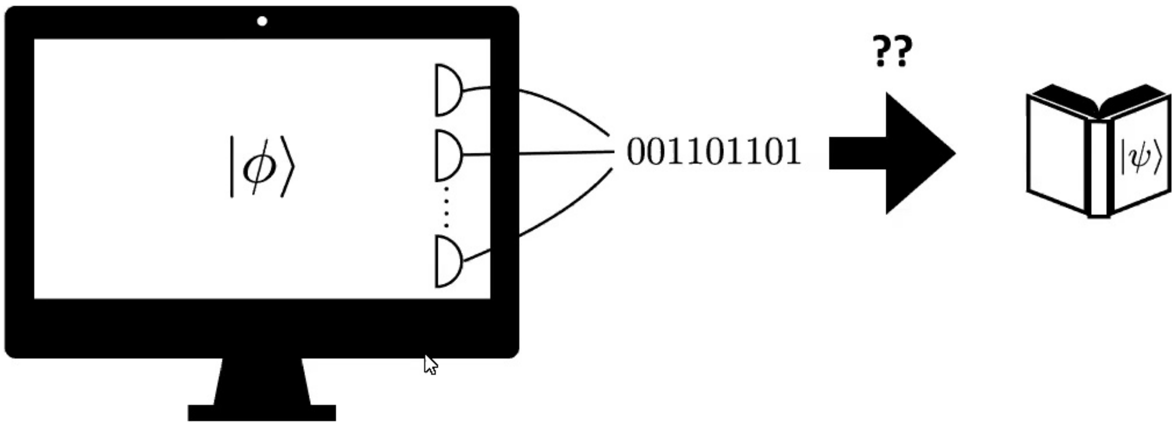
$\beta_Q = 2\sqrt{2}$ Maximal quantum violation

↓ Local isometry

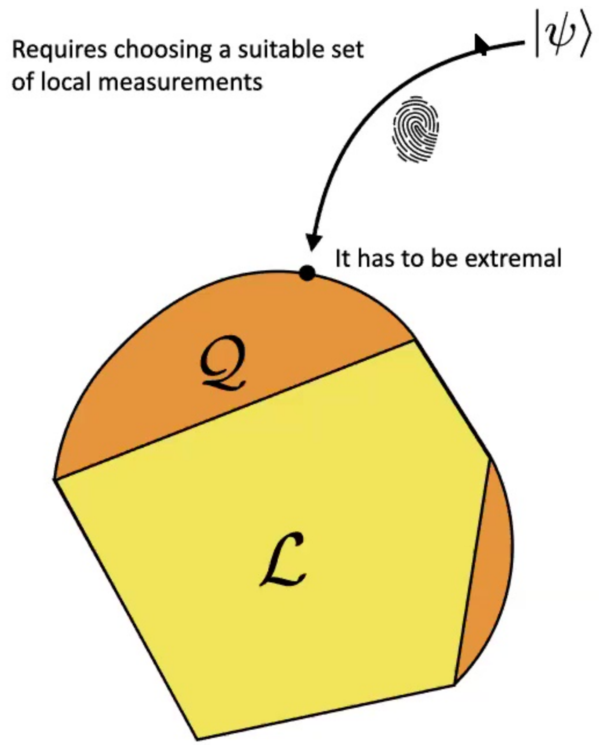
$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$$

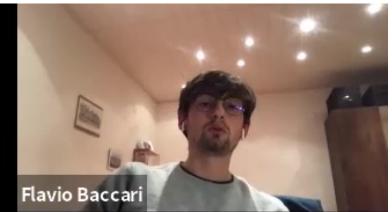
A hard challenge

Verifying the output of some computation



How to tailor a self-testing scheme to a state?



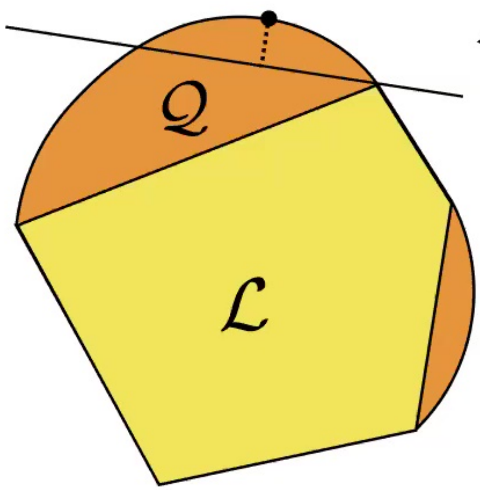


How to tailor a self-testing scheme to a state?

Requires choosing a suitable set of local measurements

$|\psi\rangle$

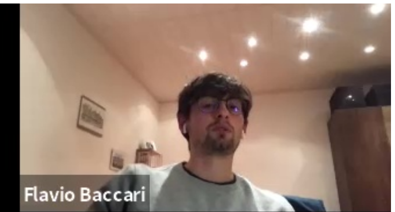
Finding a maximally violated Bell inequality

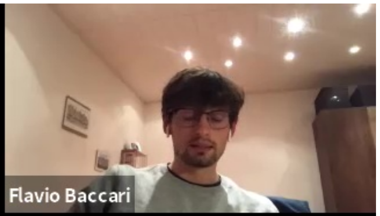


$$\vec{f} \cdot \vec{p} + \beta \geq 0$$

Better for experimental implementation

More promising for robustness to errors





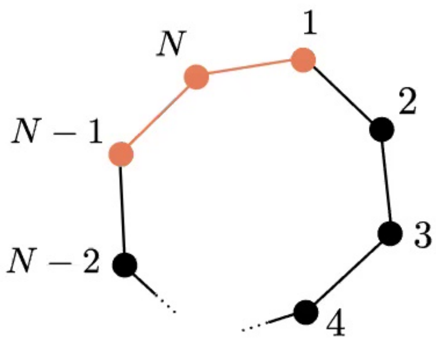
Solving the problem for graph states

Making use of the stabiliser formalism

$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \ldots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

The stabilising operators are defined by a connectivity graph



$$S_1 = X_1 Z_2 Z_N$$
$$S_2 = Z_1 X_2 Z_3$$
$$\vdots$$
$$S_N = X_N Z_1 Z_{N-1}$$

Associating a Bell inequality to each graph state

$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \ldots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

Step 1

$$\tilde{X}_1 \to \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \to \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

$$\tilde{X}_i \to M_0^{(i)} \qquad \tilde{Z}_i \to M_1^{(i)} \qquad i \neq 1$$

Associating a Bell inequality to each graph state

$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \ldots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

Step 1

$$\tilde{X}_1 \rightarrow \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \rightarrow \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

$$\tilde{X}_i \rightarrow M_0^{(i)} \qquad \tilde{Z}_i \rightarrow M_1^{(i)} \qquad i \neq 1$$

Step 2

$$\tilde{S}_i = \tilde{X}_i \otimes \bigotimes_{j \in n(i)} \tilde{Z}_j$$

Associating a Bell inequality to each graph state

$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \ldots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

Step 1

$$\tilde{X}_1 \to \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \to \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

$$\tilde{X}_i \to M_0^{(i)} \qquad \tilde{Z}_i \to M_1^{(i)} \qquad i \neq 1$$

Step 2

$$\tilde{S}_i = \tilde{X}_i \otimes \bigotimes_{j \in n(i)} \tilde{Z}_j$$

Step 3

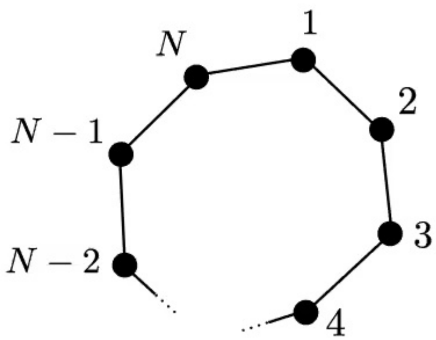
$$\mathcal{I}_G = \sqrt{2}|n(1)|\langle \tilde{S}_1 \rangle + \sqrt{2} \sum_{j \in n(1)} \langle \tilde{S}_j \rangle + \sum_{j \notin n(1)} \langle \tilde{S}_j \rangle$$

Associating a Bell inequality to each graph state

$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \dots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

Example



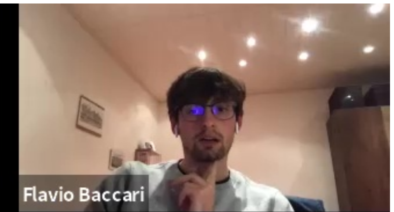
$$\tilde{S}_1 = \frac{M_0^{(1)} + M_1^{(1)}}{\sqrt{2}} M_1^{(2)} M_1^{(N)}$$

$$\tilde{S}_2 = \frac{M_0^{(1)} - M_1^{(1)}}{\sqrt{2}} M_0^{(2)} M_1^{(3)}$$

$$\vdots$$

$$\tilde{S}_N = M_0^{(N)} \frac{M_0^{(1)} - M_1^{(1)}}{\sqrt{2}} M_1^{(2)}$$

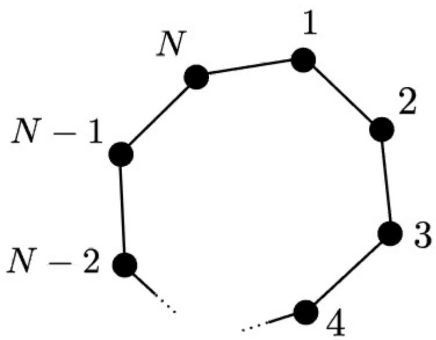
Associating a Bell inequality to each graph state



$$S_i|\psi_G\rangle = |\psi_G\rangle \qquad i = 1, \ldots, N$$

$$S_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j$$

Example



$$\begin{aligned}\mathcal{I}_{\text{ring}} = \; & 2\langle M_1^{(N)}(M_0^{(1)} + M_1^{(1)})M_1^{(2)}\rangle \\ & +\langle (M_0^{(1)} - M_1^{(1)})M_0^{(2)} M_1^{(3)}\rangle \\ & +\langle M_1^{(N-1)} M_0^{(N)} (M_0^{(1)} - M_1^{(1)})\rangle \\ & + \sum_{i=3}^{N-1} \langle M_1^{(i-1)} M_0^{(i)} M_1^{(i+1)}\rangle\end{aligned}$$

From the maximal quantum violation to self-testing

Maximal quantum violation = stabilising conditions

$$X_1 \leftarrow \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad Z_1 \leftarrow \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

$$X_i \leftarrow M_0^{(i)} \qquad Z_i \leftarrow M_1^{(i)}$$

Choosing the right measurements

$$\mathcal{I}_G = \sqrt{2}|n(1)|\langle S_1 \rangle + \sqrt{2} \sum_{j \in n(1)} \langle S_j \rangle + \sum_{j \notin n(1)} \langle S_j \rangle$$

$$\beta_G^Q = (2\sqrt{2} - 1)|n(1)| + N - 1$$

Achieved by the corresponding graph state

From the maximal quantum violation to self-testing

Proving that the violation is maximal

$$\mathcal{I}_G = \langle \mathcal{B}_G \rangle$$

Deriving a sum of squares for the Bell operator

$$(\beta_Q \mathbb{1} - \mathcal{B}_G) = \frac{|n(1)|}{\sqrt{2}}(\mathbb{1} - \tilde{S}_1)^2 + \frac{1}{\sqrt{2}} \sum_{j \in n(1)} (\mathbb{1} - \tilde{S}_j)^2 + \sum_{j \notin n(1)} (\mathbb{1} - \tilde{S}_j)^2$$

From the maximal quantum violation to self-testing

Proving that the violation is maximal

$$\mathcal{I}_G = \langle \mathcal{B}_G \rangle$$

Deriving a sum of squares for the Bell operator

$$(\beta_Q \mathbb{1} - \mathcal{B}_G) = \frac{|n(1)|}{\sqrt{2}}(\mathbb{1} - \tilde{S}_1)^2 + \frac{1}{\sqrt{2}} \sum_{j \in n(1)} (\mathbb{1} - \tilde{S}_j)^2 + \sum_{j \notin n(1)} (\mathbb{1} - \tilde{S}_j)^2 \succeq 0$$

$$tr(\rho \mathcal{B}_G) \leq \beta_Q$$

From the maximal quantum violation to self-testing

From the sum of squares to a self-testing statement

If $|\phi\rangle$ achieves β_Q ➡ $\tilde{S}_i|\phi\rangle = |\phi\rangle$ for all

for all i

$$\{\tilde{X}_i, \tilde{Z}_i\} = 0$$
$$\tilde{X}_i^2 = \mathbb{1}$$
$$\tilde{Z}_i^2 = \mathbb{1}$$

From the maximal quantum violation to self-testing

From the sum of squares to a self-testing statement

If $|\phi\rangle$ achieves β_Q ➡ $\tilde{S}_i|\phi\rangle = |\phi\rangle$ for all i

for all i

$$\{\tilde{X}_i, \tilde{Z}_i\} = 0$$
$$\tilde{X}_i^2 = \mathbb{1}$$
$$\tilde{Z}_i^2 = \mathbb{1}$$

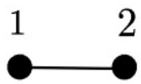
Local isometry →

Pauli X_i, Z_i

$$S_i|\psi\rangle = |\psi\rangle$$

Graph state!

We recover the CHSH self-testing



Maximally entangled 2-qubit state

Step 1

$$\tilde{X}_A = \frac{A_0 + A_1}{\sqrt{2}} \qquad \tilde{Z}_A = \frac{A_0 - A_1}{\sqrt{2}}$$

$$\tilde{X}_B = B_0 \qquad \tilde{Z}_B = B_1$$

Step 2

$$\tilde{S}_1 = \tilde{X}_A \tilde{Z}_B$$

$$\tilde{S}_2 = \tilde{X}_B \tilde{Z}_A$$

Step 3

$$\mathcal{I}_G = \sqrt{2}\langle \tilde{S}_1 \rangle + \sqrt{2}\langle \tilde{S}_2 \rangle = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$$

Quick comparison with other schemes

IMPORTANT DISCLAIMER: We are not the first

Quick comparison with other schemes

	Our method
Self-testing	✓
Bell inequality	✓
Efficiently Measurable	✓
Potentially robust	✓

Quick comparison with other schemes

	Our method
Self-testing	✓
Bell inequality	✓
Efficiently Measurable	✓
Potentially robust	✓

Bonus:

Precise strategy that could be exported to other states

Quick comparison with other schemes

Our method

	Our method
Self-testing	✓
Bell inequality	✓
Efficiently Measurable	✓
Potentially robust	✓

Bonus:

Precise strategy that could be exported to other states

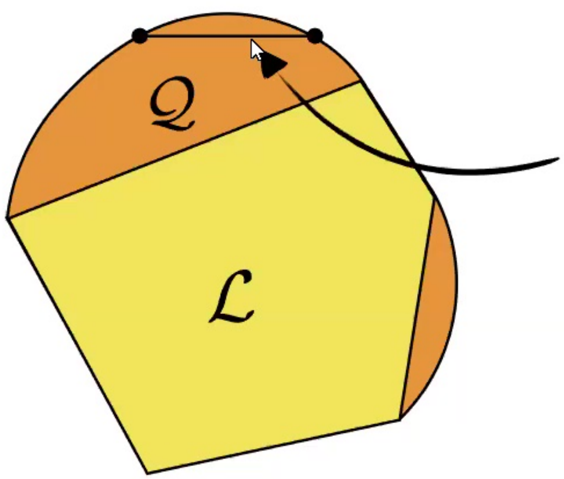
And more: see next

A novel notion of self-testing

A common belief: no self-testing of mixed states

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \quad \longrightarrow \quad \vec{p} = \sum_i p_i \, \vec{p}_i$$

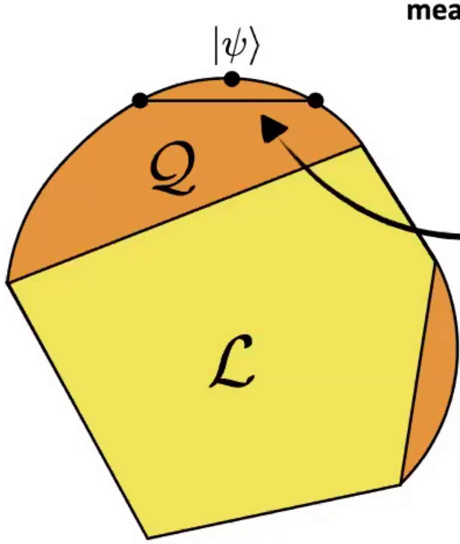
Local measurements



Problem: not extremal in the middle

A common belief: no self-testing of mixed states

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \quad \xrightarrow{\text{Local measurements}} \quad \vec{p} = \sum_i p_i \, \vec{p}_i$$



Problem: not extremal in the middle

No way to distinguish between

ρ

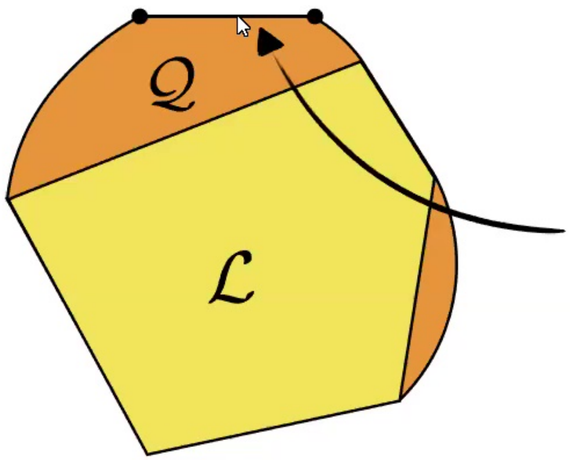
and

$(1-p)|\psi\rangle\langle\psi| + p\mathbb{1}$

A common belief: no self-testing of mixed states

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \quad \longrightarrow \quad \vec{p} = \sum_i p_i \, \vec{p}_i$$

Local measurements



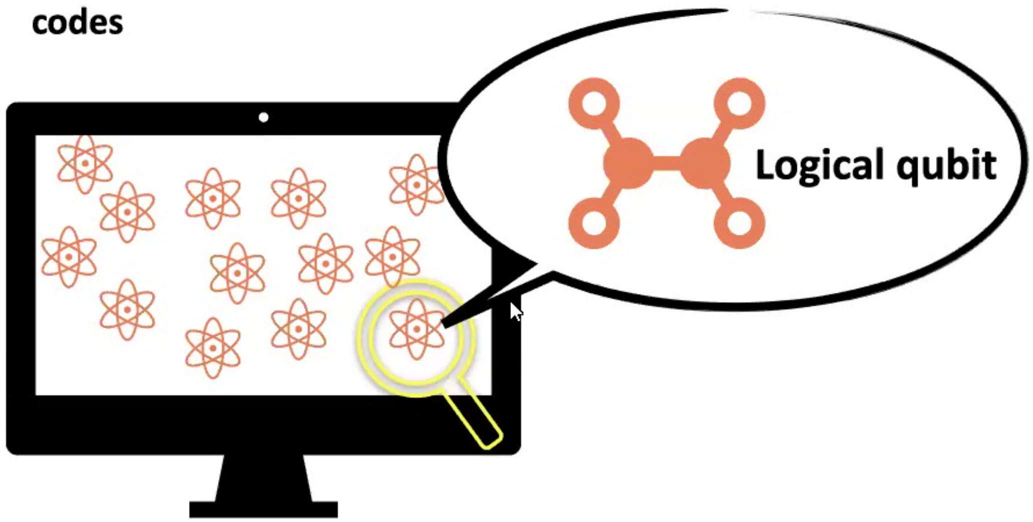
Problem: not extremal in the middle

Solution: the whole line is extremal

Stabilzers: from single states to genuinely entangled subspaces

Finding good candidates: genuinely entangled subspaces

Quantum error correction codes



Stabilzers: from single states to genuinely entangled subspaces

Finding good candidates: genuinely entangled subspaces

↓

Quantum error correction codes

↓

Stabilizer codes

$$S_i|\psi\rangle = |\psi\rangle \qquad i = 1, \dots, N - k$$

Defines a subspace of dimension 2^k

Example: the 5-qubit code

$$\left.\begin{aligned} S_1 &= X_1 Z_2 Z_3 X_4 \\ S_2 &= X_2 Z_3 Z_4 X_5 \\ S_3 &= X_1 X_3 Z_4 Z_5 \\ S_4 &= Z_1 X_2 X_4 Z_5 \end{aligned}\right\} \qquad \begin{aligned} &|\psi_0\rangle \\ &|\psi_1\rangle \end{aligned}$$

Encodes 1 logical qubit

Example: the 5-qubit code

$$\left.\begin{aligned} S_1 &= X_1 Z_2 Z_3 X_4 \\ S_2 &= X_2 Z_3 Z_4 X_5 \\ S_3 &= X_1 X_3 Z_4 Z_5 \\ S_4 &= Z_1 X_2 X_4 Z_5 \end{aligned}\right\} \quad \begin{aligned} &|\psi_0\rangle \\ &|\psi_1\rangle \end{aligned}$$

Encodes 1 logical qubit

Make the substitution and define the Bell inequality

$$\tilde{X}_1 \to \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \to \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

$$\tilde{X}_i \to M_0^{(i)} \qquad \tilde{Z}_i \to M_1^{(i)} \qquad i \neq 1$$

$$I_5 = \langle (M_0^{(1)} + M_1^{(1)}) M_1^{(2)} M_1^{(3)} M_0^{(4)} \rangle + \langle M_0^{(2)} M_1^{(3)} M_1^{(4)} M_0^{(5)} \rangle$$
$$+ \langle (M_0^{(1)} + M_1^{(1)}) M_0^{(3)} M_1^{(4)} M_1^{(5)} \rangle + 2 \langle (M_0^{(1)} - M_1^{(1)}) M_0^{(2)} M_0^{(4)} M_1^{(5)} \rangle \leq 5$$

Example: the 5-qubit code

$$\left.\begin{aligned} S_1 &= X_1 Z_2 Z_3 X_4 \\ S_2 &= X_2 Z_3 Z_4 X_5 \\ S_3 &= X_1 X_3 Z_4 Z_5 \\ S_4 &= Z_1 X_2 X_4 Z_5 \end{aligned}\right\} \quad \begin{matrix} |\psi_0\rangle \\ |\psi_1\rangle \end{matrix}$$

Encodes 1 logical qubit

Make the substitution and define the Bell inequality

$$\tilde{X}_1 \to \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \to \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

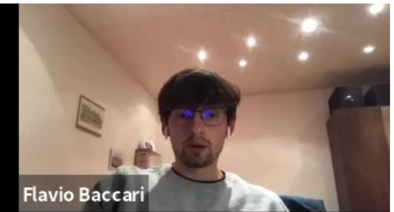
$$\tilde{X}_i \to M_0^{(i)} \qquad \tilde{Z}_i \to M_1^{(i)} \qquad i \neq 1$$

$$I_5 = \langle (M_0^{(1)} + M_1^{(1)}) M_1^{(2)} M_1^{(3)} M_0^{(4)} \rangle + \langle M_0^{(2)} M_1^{(3)} M_1^{(4)} M_0^{(5)} \rangle + \langle (M_0^{(1)} + M_1^{(1)}) M_0^{(3)} M_1^{(4)} M_1^{(5)} \rangle + 2\langle (M_0^{(1)} - M_1^{(1)}) M_0^{(2)} M_0^{(4)} M_1^{(5)} \rangle \leq 5$$

Prove the maximal quantum violation

$$\beta_q \mathbb{1} - \mathcal{B}_5 = \frac{1}{\sqrt{2}}\left(\mathbb{1} - \tilde{S}_1\right)^2 + \frac{1}{2}\left(\mathbb{1} - \tilde{S}_2\right)^2 + \frac{1}{\sqrt{2}}\left(\mathbb{1} - \tilde{S}_3\right)^2 + \sqrt{2}\left(\mathbb{1} - \tilde{S}_4\right)^2$$

achieved by every state in the subspace!



Example: the 5-qubit code

$$\left.\begin{aligned} S_1 &= X_1 Z_2 Z_3 X_4 \\ S_2 &= X_2 Z_3 Z_4 X_5 \\ S_3 &= X_1 X_3 Z_4 Z_5 \\ S_4 &= Z_1 X_2 X_4 Z_5 \end{aligned}\right\}$$

$|\psi_0\rangle$
$|\psi_1\rangle$

Encodes 1 logical qubit

Make the substitution and define the Bell inequality

$$\tilde{X}_1 \to \frac{(M_0^{(1)} + M_1^{(1)})}{\sqrt{2}} \qquad \tilde{Z}_1 \to \frac{(M_0^{(1)} - M_1^{(1)})}{\sqrt{2}}$$

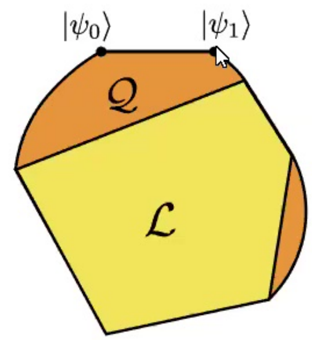
$$\tilde{X}_i \to M_0^{(i)} \qquad \tilde{Z}_i \to M_1^{(i)} \qquad i \neq 1$$

$$I_5 = \langle (M_0^{(1)} + M_1^{(1)}) M_1^{(2)} M_1^{(3)} M_0^{(4)} \rangle + \langle M_0^{(2)} M_1^{(3)} M_1^{(4)} M_0^{(5)} \rangle$$
$$+ \langle (M_0^{(1)} + M_1^{(1)}) M_0^{(3)} M_1^{(4)} M_1^{(5)} \rangle + 2 \langle (M_0^{(1)} - M_1^{(1)}) M_0^{(2)} M_0^{(4)} M_1^{(5)} \rangle \leq 5$$

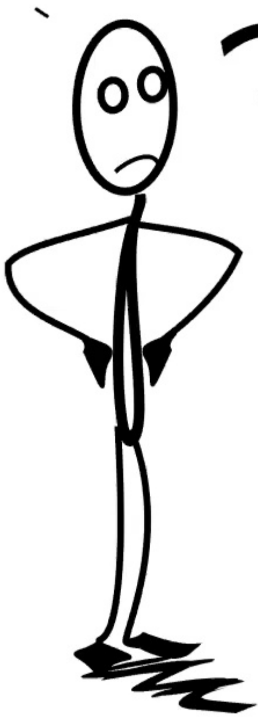
Prove the maximal quantum violation

$$\beta_q \mathbb{1} - \mathcal{B}_5 = \frac{1}{\sqrt{2}}\left(\mathbb{1} - \tilde{S}_1\right)^2 + \frac{1}{2}\left(\mathbb{1} - \tilde{S}_2\right)^2 + \frac{1}{\sqrt{2}}\left(\mathbb{1} - \tilde{S}_3\right)^2 + \sqrt{2}\left(\mathbb{1} - \tilde{S}_4\right)^2$$

achieved by every state in the subspace!



Notion of self-testing of genuinely entangled subspaces



How do
we define
self-testing here?

Notion of self-testing of genuinely entangled subspaces

$$\text{Local isometry}\left(|\phi\rangle \right) = |\psi\rangle \otimes |\text{junk}\rangle$$

State producing the observed correlations

Uncorrelated degrees of freedom

Notion of self-testing of genuinely entangled subspaces

$$\text{Local isometry}\left(\ |\phi\rangle\ \right) = \sqrt{p}\,|\psi_0\rangle|j_0\rangle + \sqrt{1-p}\,|\psi_1\rangle|j_1\rangle$$

State producing the observed correlations

Partially correlated additional degrees of freedom

Additional symmetry that does not change the observed correlations

Notion of self-testing of genuinely entangled subspaces

$$\text{Local isometry}\left(\ |\phi\rangle\ \right) = \sqrt{p}\,|\psi_0\rangle|j_0\rangle + \sqrt{1-p}\,|\psi_1\rangle|j_1\rangle$$

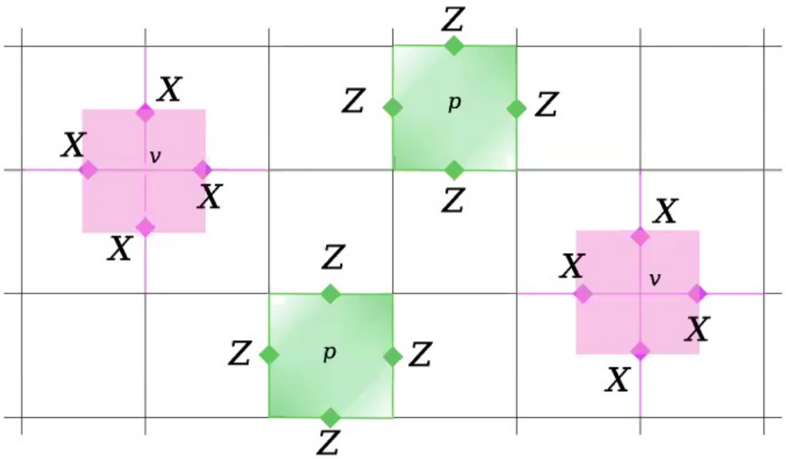
State producing the observed correlations

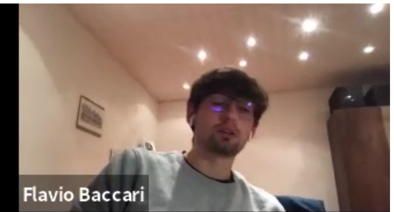
Partially correlated additional degrees of freedom

Additional symmetry that does not change the observed correlations

We include mixed states!

The toric code



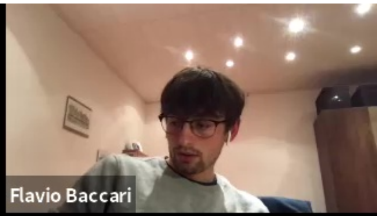


Self-testing of a subspaces spanned by 4 orthogonal states

Example of subspaces self-testing for any N

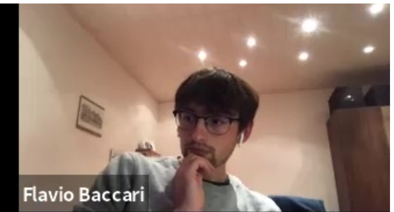
Flat structures at the boundary of the quantum set for any N

Outlook



Many open questions

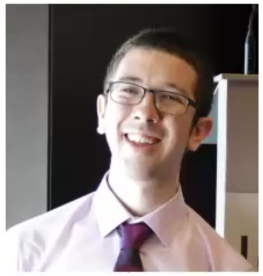
1) Robustness to noise
2) Does it apply to other stabilizers? Maybe hyper-graph states?
3) Can one self-test fault tolerant quantum computation?



Many thanks

To my collaborators

Ivan Šupić



Jordi Tura

Remigiusz Augusiak

Antonio Acín

And to all of you for your attention