



# Self-testing within the stabiliser formalism

## Remigiusz Augusiak

## Center for Theoretical Physics, Polish Academy of Sciences, Warsaw, Poland

F. Baccari, R.A., I. Šupić, J. Tura, A. Acín PRL **124**, 020402 (2020) F. Baccari, R.A., I. Šupić, A. Acín PRL **125**, 260507 (2020)







European Union European Regional Development Fund



## Preliminaries

**Bell scenario:** *N* observers performing measurements on their shares of the state



measurements outcomes

$$p(\vec{a}|\vec{x}) := p(a_1, \dots, a_N | x_1, \dots, x_N) = \langle \psi | M_{x_1}^{a_1} \otimes \dots \otimes M_{x_N}^{a_N} | \psi \rangle$$

correlations

measurement operators

[J. S. Bell, Physics 1, 195 (1964)]



$$p(\vec{a}|\vec{x}) = \sum_{\lambda} p(\lambda)p(a_1|x_1,\lambda) \cdot \ldots \cdot p(a_N|x_N,\lambda)$$

$$\forall_{a_i, x_i, \lambda} \qquad p(a_i | x_i, \lambda) \in \{0, 1\}$$

 $\lambda~$  – hidden variable



Otherwise they are called **nonlocal nonlocality** 

$$\mathcal{P}_{m,d} \subsetneq \mathcal{Q}_{m,d}$$

### Preliminaries Nonlocality and Bell inequalities

**Bell inequalities**: *Hyperplanes constraining the local set* 

**Bell inequalities** 

$$I := \sum_{\vec{a}, \vec{x}} \alpha_{\vec{a}, \vec{x}} p(\vec{a} | \vec{x}) \le \beta_C$$

$$\beta_C = \max_{\mathcal{P}_{m, d}} I \quad \text{(classical bound)}$$

$$\beta_Q = \sup_{\mathcal{Q}_{m, d}} I \quad \text{(quantum bound)}$$

$$Local polytope$$

#### Examples

Clauser, Horne, Shimony, Holt (1969); Collins *et al.* (CGLMP) (2002); Barrett, Kent, Pironio (BKP) (2006);

$$I := \sum_{\vec{a}, \vec{x}} \alpha_{\vec{a}, \vec{x}} p(\vec{a} | \vec{x}) > \beta_{C}$$

$$\Downarrow$$
nonlocality

**Example**: Clauser-Horne-Shimony-Holt (CHSH) Bell inequality



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

**Example**: Clauser-Horne-Shimony-Holt (CHSH) Bell inequality

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



## Non-locality

Non-locality is a resource for device-independent applications

Quantum key distribution [Ekert, PRL (1991); A. Acín et al., PRL (2007)]

Randomness certification/amplification
[Pironio et al., Nature (2010); Colbeck, Renner, Nat. Phys. (2012)]

Device-independent entanglement certification [J.-D. Bancal et al., PRL (2011)]

Self-testing
 [Mayers, Yao, QIC (2004)]

## Self-testing

► The idea of device-independent certification



## Self-testing

► The idea of device-independent certification



- Given  $\{p(\vec{a}|\vec{x})\}$
- or violation of some Bell inequality

 $\sum_{\vec{a},\vec{x}} \alpha_{\vec{a},\vec{x}} \, p(\vec{a}|\vec{x}) = \beta > \beta_C$ 

 $\blacktriangleright$  deduce properties of the state  $|\psi\rangle$  and the underlying measurements

• Self-testing:  $\exists_{U_1,...,U_N}$   $(U_1 \otimes \ldots \otimes U_N) |\psi\rangle = |\phi\rangle \otimes |aux\rangle$ Iocal isometries
the state we want to certify

## Self-testing

► The idea of device-independent certification



- Given  $\{p(\vec{a}|\vec{x})\}$
- or violation of some Bell inequality

 $\sum_{\vec{a},\vec{x}} \alpha_{\vec{a},\vec{x}} \, p(\vec{a}|\vec{x}) = \beta > \beta_C$ 

 $\blacktriangleright$  deduce properties of the state  $|\psi\rangle$  and the underlying measurements

Self-testing:  $\exists_{U_1,...,U_N}$   $(U_1 \otimes \ldots \otimes U_N) |\psi\rangle = |\phi\rangle \otimes |aux\rangle$ 

#### Seems like a hopeless task!

but

often one can deduce everything!



**Example**: Self-testing from violation of the CHSH Bell inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \le 2\sqrt{2}$$

 $\exists U_A, U_B \qquad U_A \otimes U_B |\psi_{AB}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \otimes |aux\rangle$ 

$$U_{A} A_{0} U_{A}^{\dagger} = X \otimes \mathbb{1} \qquad U_{B} B_{0} U_{B}^{\dagger} = \frac{1}{\sqrt{2}} (X + Z) \otimes \mathbb{1}$$
$$U_{A} A_{1} U_{A}^{\dagger} = Z \otimes \mathbb{1} \qquad U_{B} B_{1} U_{B}^{\dagger} = \frac{1}{\sqrt{2}} (X - Z) \otimes \mathbb{1}$$
$$P^{*} \qquad \beta_{Q} = 2\sqrt{2}$$
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{unique maximiser } \int_{\mathbb{R}^{3}}^{\mathbb{R}^{3}} \int_{$$

## Scalable Bell inequalities for graph states

F. Baccari, R.A., I. Šupić, J. Tura, A. Acín PRL **124**, 020402 (2020)

## Stabilizer formalism

N-qubit Pauli group

$$\mathbb{G}_N = \{\lambda g_1 \otimes \ldots \otimes g_N \mid g_i \in \{\mathbb{1}, X, Y, Z\}; \lambda \in \{\pm 1, \pm i\}\}\$$

*N*-fold tensor products of the Pauli matrices

- Consider a subgroup
  - $\mathbb{S}_N = \langle G_1, \dots, G_k \rangle \qquad \qquad G_i \in \mathbb{G}_N \quad \text{ generators}$ (independent elements of the group)

Stabilizer if it stabilizes a nontrivial subspace V in  $\mathcal{H}_N = (\mathbb{C}^2)^{\otimes N}$ 

$$\bigvee_{|\psi\rangle \in V} \quad \mathbb{S}_N |\psi\rangle = |\psi\rangle \qquad \text{dim } V = 2^{N-k}$$

## Stabilizer formalism

Necessary and sufficient condition

- Applications:
  - Quantum computing
  - Quantum error correction
- Useful description of a class of multipartite systems



Graph states

[Hein et al. (2004)]

 $\blacktriangleright$  Multiqubit graph states ~G=(V,E)

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

► Graph state associated to a graph *G*:

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



Graph states

[Hein *et al.* (2004)]

 $\blacktriangleright$  Multiqubit graph states ~G=(V,E)

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

▶ Graph state associated to a graph *G*:

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



$$X = \left(\begin{array}{cc} 0 & 1\\ 1 & 0 \end{array}\right) \ Z = \left(\begin{array}{cc} 1 & 0\\ 0 & -1 \end{array}\right)$$

A representative class of multiqubit entangled states

- GHZ states multipartite cryptography
- Cluster states quantum computing
- Absolutely maximally entangled states
- All stabilizer states are LU equivalent to graph states

$$\frac{1}{\sqrt{2}} \left( |0\rangle^{\otimes N} + |1\rangle^{\otimes N} \right)$$

## CHSH-like Bell inequalities for graph states

**Step 1:** Take a graph and the generators G = (V, E)

$$G_i = X_i \otimes \bigotimes_{j \in n(i)} Z_j \qquad \qquad n(1) = \max_{i=1,\dots,N} n(i)$$



**Step 2:** *Make a substitution* 

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

 $\widetilde{X}_{1} = A_{0}^{(1)} + A_{1}^{(1)} \qquad \widetilde{X}_{i} = A_{0}^{(i)}$  $\widetilde{Z}_{1} = A_{0}^{(1)} - A_{1}^{(1)} \qquad \widetilde{Z}_{i} \to A_{1}^{(i)} \qquad i = 2, \dots, N$ 



**Step 3:** Construct Bell expression

$$I_G := \sqrt{2} |n(1)| \langle \widetilde{G}_1 \rangle + \sqrt{2} \sum_{j \in n(1)} \langle \widetilde{G}_j \rangle + \sum_{j \notin n(1)} \langle \widetilde{G}_j \rangle$$

## Bell inequalities for graph states – example

**Example:** *the simplest graph* 

#### Step 2

Step 3

$$I_G = \langle \widetilde{G}_1 \rangle + \langle \widetilde{G}_1 \rangle = \langle (A_0 + A_1) B_0 \rangle + \langle (A_0 - A_1) B_1 \rangle \le 2$$

The CHSH Bell inequality

## Bell inequalities for graph states

### Properties

- ✓ Number of expectation values linear in N
- Analytical expressions for maximal classical and quantum values

$$\beta_G^C = N + n_{\max} - 1$$
  
 $\beta_G^Q = N + (2\sqrt{2} - 1)n_{\max} - 1$ 

• sum-of-squares decomposition

$$\beta_G^Q > \beta_G^C$$
 for any connected graph

previous constructions

- exponential scaling

O. Gühne *et al.*, PRL (2005)

$$\beta_G^Q \mathbb{1} - \mathcal{B}_G = \frac{|n(1)|}{\sqrt{2}} (\mathbb{1} - \widetilde{G}_1)^2 + \frac{1}{\sqrt{2}} \sum_{j \in n(1)} (\mathbb{1} - \widetilde{G}_j)^2 + \sum_{j \neq n(1)} (\mathbb{1} - \widetilde{G}_j)^2 \quad \left| \int \operatorname{Tr}(\mathcal{B}_G \rho) \leq \beta_Q \right|$$

• optimal quantum realisation

$$A_{0/1}^{(1)} = (X \pm Z)/\sqrt{2}$$
  
 $A_{0/1}^{(i)} = X/Z$   $(i = 2, ..., N)$ 

$$\langle \psi_G | \mathcal{B}_G | \psi_G \rangle = \beta_G^Q$$

## Bell inequalities for graph states



## Bell inequalities for graph states

We are not the first to provide Bell inequalities and self-testing methods for graph states

O. Gühne *et al.,* Phys. Rev. Lett. (2005) G. Tóth *et al.,* Phys. Rev. A (2006) M.McKague, Lecture Notes in Computer Science (2014)

#### But:

- Scalable Bell inequalities minimal information?
- Maximal classical and quantum values direct to determine
- Self-testing
- Potentially robust
- Possible generalization to entangled subspaces

Recent experiment: D. Wu *et al.,* arXiv:2105.10298

 $\beta_C^Q > \beta_C^C$ 

# Self-testing of genuinely entangled subspaces

F. Baccari, R.A., I. Šupić, A. Acín PRL **125**, 260507 (2020)

What about stabilizer subspaces of higher dimension?

$$\mathbb{S}_N = \langle G_1, \dots, G_k \rangle \qquad \mathbb{S}_N V = V$$

 $\dim V = 2^{N-k}$ 

Can we construct Bell inequalities maximally violated by whole subspace?

$$I_{\mathbb{S}}(|\psi\rangle) = \beta^Q \qquad |\psi\rangle \in V$$

#### genuinely entangled subspaces

$$egin{aligned} & |\psi
angle - ext{genuinely entangled} \ & |\psi
angle 
eq |\psi_1
angle \otimes |\psi_2
angle \end{aligned}$$

M. Demianowicz, RA, Phys. Rev. A (2020)

**Example:** five-qubit code  $\mathcal{H} = (\mathbb{C}^2)^{\otimes 5}$ 

 $S_{5} = \langle G_{1}, G_{2}, G_{3}, G_{4} \rangle$   $G_{1} = X_{1}Z_{2}Z_{3}X_{4}$   $G_{2} = X_{2}Z_{3}Z_{4}X_{5}$   $G_{3} = X_{1}X_{3}Z_{4}Z_{5}$   $G_{4} = Z_{1}X_{2}X_{4}Z_{5}$ 

(allows for encoding 1 logical qubit)

$$V = \operatorname{span}\{|\psi_0\rangle, |\psi_1\rangle\}$$

genuinely entangled subspace

**Example:** five-qubit code  $\mathcal{H} = (\mathbb{C}^2)^{\otimes 5}$ 

 $S_{5} = \langle G_{1}, G_{2}, G_{3}, G_{4} \rangle$   $G_{1} = X_{1}Z_{2}Z_{3}X_{4}$   $G_{2} = X_{2}Z_{3}Z_{4}X_{5}$   $G_{3} = X_{1}X_{3}Z_{4}Z_{5}$   $G_{4} = Z_{1}X_{2}X_{4}Z_{5}$ 

(allows for encoding 1 logical qubit)

$$V = \operatorname{span}\{|\psi_0\rangle, |\psi_1\rangle\}$$

genuinely entangled subspace

Constructing a Bell inequality

$$X_{1} \to A_{0}^{(1)} + A_{1}^{(1)} \qquad X_{i} \to A_{0}^{(i)}$$
$$i = 2, \dots, 5$$
$$Z_{1} \to A_{0}^{(1)} - A_{1}^{(1)} \qquad Z_{i} \to A_{1}^{(i)}$$

 $I_{5} = \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{1}^{(2)}A_{1}^{(3)}A_{0}^{(4)} \rangle + \langle A_{0}^{(2)}A_{1}^{(3)}A_{1}^{(4)}A_{0}^{(5)} \rangle$  $+ \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{0}^{(3)}A_{1}^{(4)}A_{1}^{(5)} \rangle + 2\langle (A_{0}^{(1)} - A_{1}^{(1)})A_{0}^{(2)}A_{0}^{(4)}A_{1}^{(5)} \rangle \le 5$ 

$$I_{5} = \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{1}^{(2)}A_{1}^{(3)}A_{0}^{(4)}\rangle + \langle A_{0}^{(2)}A_{1}^{(3)}A_{1}^{(4)}A_{0}^{(5)}\rangle + \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{0}^{(3)}A_{1}^{(4)}A_{1}^{(5)}\rangle + 2\langle (A_{0}^{(1)} - A_{1}^{(1)})A_{0}^{(2)}A_{0}^{(4)}A_{1}^{(5)}\rangle \le 5$$

### Quantum violations

$$A_{0/1}^{(1)} = (X \pm Z)/\sqrt{2}$$
  

$$B_5 = \sqrt{2}(G_1 + G_2 + 2G_3) + G_4$$
  

$$A_{0/1}^{(i)} = X/Z \quad (i = 2, \dots, 5)$$
  

$$\langle \psi | \mathcal{B}_5 | \psi \rangle = 4\sqrt{2} + 1 > 5 \quad \forall | \psi \rangle \in V$$

Sum-of-squares decomposition

$$(4\sqrt{2}+1)\mathbb{1} - \mathcal{B}_5 = \frac{1}{\sqrt{2}}(\mathbb{1} - \tilde{G}_1)^2 + \frac{1}{2}(\mathbb{1} - \tilde{G}_2)^2 + \frac{1}{\sqrt{2}}(\mathbb{1} - \tilde{G}_3)^2 + \sqrt{2}(\mathbb{1} - \tilde{G}_4)^2$$

any vector from the subspace violates this inequality maximally

Geometric picture



Our Bell inequality identifies a nontrivial face structure in the set of quantum correlations

Maximal violation by mixed states

 $\rho = p|\psi_0\rangle\!\langle\psi_0| + (1-p)p|\psi_1\rangle\!\langle\psi_1|$ 

Can we self-test this entangled subspace?

But how one defines self-testing of a subspace?

State self-testing  $\vec{p} \implies \exists_{U_1,...,U_N}$  such that

 $U_1 \otimes \ldots \otimes U_N |\psi\rangle = |\phi\rangle \otimes |\mathrm{aux}\rangle$ 



But how one defines self-testing of a subspace?





## Subspaces

consider a subspace  $V = \operatorname{span}\{|\phi_1\rangle, \dots, |\phi_k\rangle\}$ 



**Example:** *five-qubit code* 

$$S_{5} = \langle G_{1}, G_{2}, G_{3}, G_{4} \rangle$$

$$G_{1} = X_{1}Z_{2}Z_{3}X_{4}$$

$$G_{2} = X_{2}Z_{3}Z_{4}X_{5}$$

$$G_{3} = X_{1}X_{3}Z_{4}Z_{5}$$

$$G_{4} = Z_{1}X_{2}X_{4}Z_{5}$$

$$V = \operatorname{span}\{|\psi_0\rangle, |\psi_1\rangle\}$$

genuinely entangled subspace

$$I_{5} = \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{1}^{(2)}A_{1}^{(3)}A_{0}^{(4)} \rangle + \langle A_{0}^{(2)}A_{1}^{(3)}A_{1}^{(4)}A_{0}^{(5)} \rangle + \langle (A_{0}^{(1)} + A_{1}^{(1)})A_{0}^{(3)}A_{1}^{(4)}A_{1}^{(5)} \rangle + 2\langle (A_{0}^{(1)} - A_{1}^{(1)})A_{0}^{(2)}A_{0}^{(4)}A_{1}^{(5)} \rangle \leq 2$$

 $I_5(|\psi
angle)=4\sqrt{2}+1$  maximal violation

 $U_1 \otimes \ldots \otimes U_5 |\psi\rangle = p |\psi_1\rangle \otimes |\operatorname{aux}_1\rangle + \sqrt{1-p} |\psi_2\rangle \otimes |\operatorname{aux}_2\rangle$ 

## Generalizations

• Graph states of local dimension d prime G = (V, E)

 $G_i = X_i \otimes \bigotimes_{j \in n(i)} Z^{r_{ij}}$ 

 $G_i |\psi_G\rangle = |\psi_G\rangle$ 

$$\begin{split} X|i\rangle &= |i+1\rangle \\ Z|i\rangle &= \omega^i |i\rangle \end{split} \qquad \forall |i\rangle \end{split}$$

generalizations of Pauli matrices

Naive approach to constructing Bell inequalities

$$egin{aligned} X_1 & o A_0^{(1)} + A_1^{(1)} & X_i & o A_0^{(i)} & A_j^{(i)} \ && Z_1 & o A_0^{(1)} - A_1^{(1)} & Z_i & o A_1^{(i)} & d ext{-outcome unitary observables} \end{aligned}$$

#### But

$$\nexists \quad \alpha X + \beta Z - \text{unitary} \qquad \blacksquare \\ \alpha, \beta \in \mathbb{C}$$

how to determine maximal quantum violation?

A possible solution

$$\omega^{k(k+1)} X Z^k \qquad k = 0, \dots, d-1$$

mutually unbiased bases
 in prime d

 $|\psi_{AME(3,4)}\rangle$ 

 certain combinations of these give proper observables

**Example**: *AME*(4,3) *state*  $\mathcal{H} = (\mathbb{C}^3)^{\otimes 4}$ 

$$G_1 = X_1 Z_2 Z_3$$
  $G_3 = Z_1 X_3 Z_4^2$   
 $G_2 = Z_1 X_2 Z_4$   $G_4 = Z_2 Z_3^2 X_4$ 



Constructing a Bell inequality

 $G_1 = X_1 Z_2 Z_3$   $G_1 G_2 = (XZ)_1 (ZX)_2 Z_3 Z_4$  $G_1 G_2^2 = (XZ^2)_1 (ZX^2)_2 Z_3 Z_4^2$   $G_1G_3 = (XZ)_1Z_2(ZX)_3Z_4^2$  $G_4 = Z_2Z_3^2X_4$ 

## Generalizations

Substitution

$$\begin{split} X_1 &\to \frac{1}{\sqrt{3\lambda}} (A_0^{(1)} + A_1^{(1)} + A_2^{(1)}) & Z_2 \to A_0^{(2)} \\ (\omega XZ)_1 &\to \frac{1}{\sqrt{3\lambda}} (A_0^{(1)} + \omega A_1^{(1)} + \omega^2 A_2^{(1)}) & (ZX)_2 \to A_1^{(2)} \\ (XZ^2)_1 &\to \frac{1}{\sqrt{3\lambda}} (A_0^{(1)} + \omega^2 A_1^{(1)} + \omega A_2^{(1)}) & (ZX^2)_2 \to A_2^{(2)} \\ & \lambda \in \mathbb{C} \\ \omega &= \exp(2\pi i/3) \end{split}$$

#### ► Bell inequality

$$\begin{split} I_{\text{AME}} &= \frac{1}{\sqrt{3}\lambda} \langle (A_0^{(1)} + A_1^{(1)} + A_2^{(1)}) B_0 C_0 \rangle + \frac{1}{\sqrt{3}\lambda\omega} \langle (A_0^{(1)} + \omega A_1^{(1)} + \omega^2 A_2^{(1)}) B_1 C_0 D_0 \rangle \\ &+ \frac{1}{\sqrt{3}\lambda} \langle (A_0^{(1)} + \omega^2 A_1^{(1)} + \omega A_2^{(1)}) B_2 C_0 D_0^2 \rangle \\ &+ \frac{1}{\sqrt{3}\lambda\omega} \langle (A_0^{(1)} + \omega A_1^{(1)} + \omega^2 A_2^{(1)}) B_0 C_1 D_0^2 \rangle + \langle B_0 C_0^2 D_1 \rangle + \text{c.c.} \leq \beta_C \end{split}$$

maximally violated by the AME(4,3) state

## Conclusion/Outlook



- Further questions
  - Self-testing of multipartite states from minimal information
  - Are all genuinely entangled subspaces self-testable?

are all multipartite genuinely entangled states self-testable?