Certification of local quantum systems: Self-testing and dimension witnessing

Maharshi Ray

Mie University, Japan
CQT, Singapore

Based On

arXiv:1812.07265 (Phys. Rev. Lett. 122, 250403)
&
arXiv:1911.09448
&
arXiv: 2007.10746 (New Journal of Physics, 2020)

Joint works with

Kishor Bharti Antonios Varvitsiotis Naresh Boddu
Naqueeb A. Warsi Adan Cabello Leong-Chuan Kwek

About me

- Name : Maharshi Ray

- 2010-15 : IIIT-Hyderabad (B. Tech+MS)
- Supervisors :
    - Indranil Chakrabarty
    - Harjinder Singh

- 2015-20 : Centre for Quantum Technologies (CQT), National University of Singapore (PhD).
- Supervisors :
    - Miklos Santha, CQT, CNRS France.
    - Troy Lee, UTS Australia.

- 2020-present : Mie University, Japan (QLEAP Project Assist. Prof)

- Areas of interest:
    - Quantum computing
    - Optimisation theory
    - Game theory
    - Quantum foundations

Talk outline

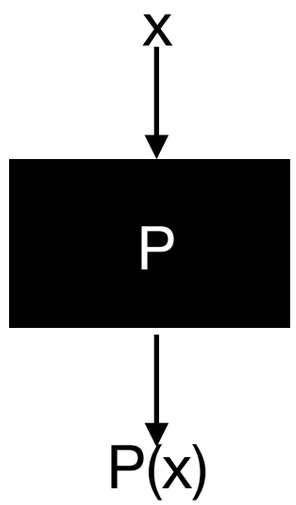
1. **Background**
    - **Device certification**
    - **Cabello-Severini-Winter (CSW) framework**

2. **Self-testing**
    - **Definitions**
    - **Odd-cycle self tests**
    - **Anti-odd cycle self tests**

3. **Dimension witnessing (DW)**
    - **Formalism**
    - **Tools - a rank constrained SDP**
    - **A family of DW of arbitrary high dimensions**

Device certification

- **Classical analogy:** A computer program P is written to compute some function f. How do we know if the program is "buggy", i.e.,$P(x) \neq f(x)$ for some input instance x?



- **Quantum world:** We have quantum states and measurements prepared by untrusted sources and goal is to verify them.

- **General set up:** Perform some measurements on some quantum state(s) and collect the experimental statistics. Deduce some properties of the underlying quantum systems from these data.

Device certification in non-local scenario

Data : $\{P(a,b \mid x,y)\}_{a,b,x,y}$

Bell inequalities : $\sum_{a,b,x,y} s_{xy}^{ab} P(a,b \mid x,y) \leq S_C$

In quantum theory $P(a,b \mid x,y) = \left\langle \psi_{AB} \left| M_{a|x} \otimes M_{b|y} \right| \psi_{AB} \right\rangle$

For example, in CHSH experiment, $x,y,a,b \in \{0,1\}$ and

$$s_{xy}^{ab} = \begin{cases} 1 & \textbf{if } a \oplus b = x \cdot y \\ 0 & \textbf{otherwise} \end{cases}$$

Question: From this data, what can we say about the underlying quantum system?

Cabello-Severini-Winter (CSW) framework

- Measurement events: $e_1, e_2, \cdots, e_n$
- Exclusive event-pairs cannot happen simultaneously

Exclusivity graph $\mathcal{G}_{ex}$:

- Vertices : $1, \cdots, n$
- Edges : $i \sim j,$ when e_i, e_j exclusive

- Consider theories assigning probabilities to events

$$p : [n] \to [0,1] \textbf{ where } p_i + p_j \leq 1 \, \forall i \sim j$$

behaviour

Non-contextual theories

Deterministic non-contextual theories:

- All events have pre-determined values that do not depend on the occurrence of other events

$$p : [n] \to \{0,1\} \textbf{ where } p_i + p_j \leq 1 \, \forall i \sim j$$

- Characteristic vectors of stable sets of $\mathcal{G}_{ex}$

Non-contextual theories: Convex hull of deterministic non-contextual behaviours.

[CSW, Phys Rev Lett'14]:

- The polytope of NC behaviours is STAB($\mathcal{G}_{ex}$)

Quantum Theory

A behaviour $p : [n] \to [0,1]$ is quantum if $\exists$ quantum state $|\psi\rangle$ and projectors $\Pi_1, \Pi_2, \ldots, \Pi_n$, such that

- $p_i = \langle\psi|\Pi_i|\psi\rangle, \forall i \in [n]$
- $\mathbf{Tr}(\Pi_i\Pi_j) = 0, \forall\ i \sim j$

Theta body of graph G : $x \in \mathbf{TH}(G)$ iff $\exists$ PSD matrix X of size $n+1$ such that :

- $X_{00} = 1$
- $x_i = X_{ii}, \forall i \in [n]$
- $X_{0i} = X_{ii}, \forall i \in [n]$
- $X_{ij} = 0, \forall i \sim j$

[CSW'14]:

- The set of quantum behaviours is $\mathrm{TH}(\mathcal{G}_{ex})$

Some graph invariants

Independence number : Size of the largest stable set. Denoted by α.

Lovász theta number :

$$\vartheta = \max \|x\|_1 : x \in \mathbf{TH}(G)$$

$$= \max \sum_{i=1}^{n} X_{ii}$$

$$\textbf{subject to } X_{ii} = X_{0i}, \quad 1 \leq i \leq n$$

$$X_{ij} = 0, \quad i \sim j$$

$$X_{00} = 1,$$

$$X \in \mathcal{S}_{+}^{1+n}$$

Chromatic number : Minimum number of colours needed to colour the vertices such that no two vertices sharing an edge have the same colour. Denoted by χ.

Sandwich Theorem : $\alpha(G) \leq \vartheta(G) \leq \chi(\overline{G})$

NP-hard to compute

NC-inequalities

Facet of the NC-polytope

$$\sum_{i\in[n]} w_i p_i \leq \alpha(\mathcal{G}_{ex}, w), \forall p \in \text{STAB}(\mathcal{G}_{ex})$$

weighted independence number

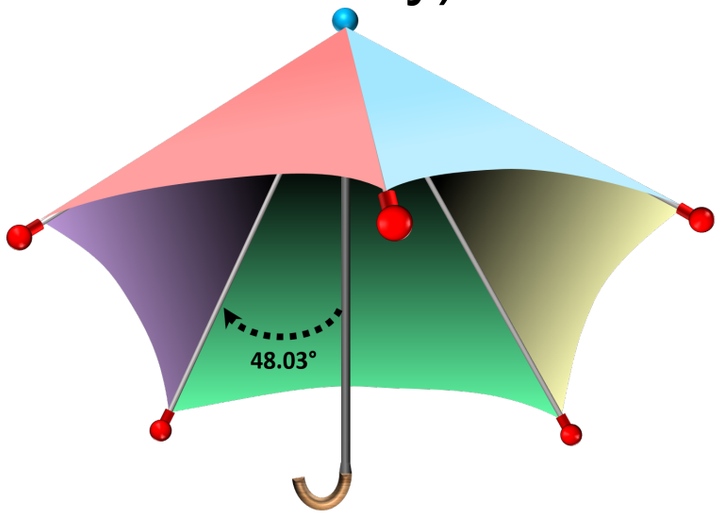
Quantum value of a NC inequality:

$$\vartheta(\mathcal{G}_{ex}, w) = \max\{ \sum_{i\in[n]} w_i p_i : p \in \text{TH}(\mathcal{G}_{ex})\}$$

weighted Lovasz theta number

$KCBS_n$ inequalities (Klyachko-Can-Binicioğlu-Shumovsky)

- For odd $n \geq 5$, $KCBS_n$ corresponds to the NC inequalities for C_n
- Maximum value attained by quantum realisations = $\frac{n}{1 + sec(\pi/n)}$



Lovasz's umbrella configuration for $n = 5$ [Lovasz, 1979], $\vartheta(C_5) = \sqrt{5}$

Self-testing

- Scheme to certify the underlying quantum state and measurements from the measurement statistics
- Have been well studied in the non-local setting.
- *CHSH* is a self-test for the two qubit maximally entangled states.

Perform the *CHSH* test and achieve the Tsirelson bound $2\sqrt{2}$

Underlying state must be Bell-states upto local isometry

$$(V_1 \otimes V_2)\,|\psi\rangle_{AB} = |junk\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Applications :

- Crypto - Random number generation, Delegated computing.
- Verifying computation [Reichardt, Unger, Vazirani, Nature'13][Natarajan, Vidick, STOC'17]
- Crucial ingredients in complexity theory proofs (e.g. MIP* = RE)

Self-testing NC-inequalities

The NC-inequality $\sum_{i\in[n]} w_i p_i \leq \alpha(G,w)$ self-tests the system $\{\,|u_i\rangle\langle u_i|\,\}_{i=0}^{n}$ if :

- $\{\,|u_i\rangle\langle u_i|\,\}_{i=0}^{n}$ achieves the quantum value = $\vartheta(G,w)$

- For any other ensemble $\{\,|u_i'\rangle\langle u_i'|\,\}_{i=0}^{n}$ that achieves the quantum value, $\exists$ isometry V such that

$$V|u_i\rangle\langle u_i|V^\dagger = |u_i'\rangle\langle u_i'|, \quad 0 \leq i \leq n$$

Robustness

The NC-inequality $\sum_{i\in[n]} w_i p_i \leq \alpha(G,w)$ is an (ϵ, r) robust self-test if

- It self-tests $\{\,|u_i\rangle\langle u_i|\,\}_{i=0}^{n}$
- For any other realisation $\{\,|u_i'\rangle\langle u_i'|\,\}_{i=0}^{n}$ satisfying:

$$\sum_{i=1}^{n} w_i \left|\langle u_i' \,|\, u_0'\rangle\right|^2 \geq \vartheta(G,w) - \epsilon$$

$\exists$ isometry V such that:

$$\|V\,|u_i\rangle\langle u_i|\,V^\dagger - |u_i'\rangle\langle u_i'|\| \leq \mathcal{O}\left(\epsilon^r\right), \quad 0 \leq i \leq n$$

Result 1

Theorem: For any odd n, the $KCBS_n$ inequality is an $\left(\epsilon, \frac{1}{2}\right)$ robust *self-test* for the canonical ensemble.

[Phys. Rev. Lett. 122, 250403]

Proof strategy

Roadmap to a robust self-testing result :

- The Lovász theta SDP has unique solution X^*
- $\sum_i w_i \tilde{X}_{ii} \geq \vartheta\left(\mathcal{G}_{ex}\right) - \epsilon \Longrightarrow \left\| \tilde{X} - X^* \right\|_{\mathrm{F}} \leq \mathcal{O}(\epsilon)$
- Two PSD matrices ϵ-close in Frobenius distance, their Gram decompositions are $\mathcal{O}(\sqrt{\epsilon})$ close in ℓ_2-norm.

Uniqueness of SDP solutions

Primal SDP

$$\max \quad \langle C, X \rangle$$

$$\langle A_i, X \rangle = b_i, \quad \forall i \in [m]$$

$$X \in \mathcal{S}_+^n$$

Dual SDP

$$\min \quad \sum_{i=1}^{m} b_i y_i$$

$$\sum_{i=1}^{m} y_i A_i - C = Z \in \mathcal{S}_+^n$$

Theorem [Alizadeh, Haeberly, Overton, 1997]

Let Z be dual optimal, for which the linear system $MZ = 0, \langle M, A_1 \rangle = 0, \cdots, \langle M, A_m \rangle = 0,$ only admits the trivial solution $M = 0$.

Then, the primal SDP has a unique optimal solution.

→ Z is a called a dual *non-degenerate* optimal solution

Dual opt solution

Dual of the Lovasz theta SDP is given as follows :

$$\min t : tE_{00} + \sum_i E_{ii}(\lambda_i - 1) - \sum_i \lambda_i E_{0i} + \sum_{(i,j):i\sim j} \mu_{ij} E_{ij} \equiv Z \succeq 0.$$

Claim : $Z_n = \left[\begin{array}{c|c} \vartheta_n & -e^T \\ \hline -e & I_n + \frac{n-\vartheta_n}{2\vartheta_n} A_{C_n} \end{array}\right]$ is an optimal dual solution

Proof Sketch :

- Take $t = \vartheta_n$, $\lambda_i = 2, \mu_{ij} = \frac{n-\vartheta_n}{2\vartheta_n}$
- Taking Schur complement w.r.t top left entry : $Z_n \succeq 0 \iff I_n + \frac{n-\vartheta_n}{2\vartheta_n} A_{C_n} - \frac{1}{\vartheta_n} ee^T \succeq 0.$
- e is an eigenvector of A_{C_n}

  $\implies Eig\left(I_n + \frac{n-\vartheta_n}{2\vartheta_n} A_{C_n} - \frac{1}{\vartheta_n} ee^T\right) = \left\{1 + \frac{n-\vartheta_n}{\vartheta_n} \cos\frac{2\pi k}{n},\ 1 \le k \le n-1\right\} \cup 0.$

which follow from the fact A_{C_n} is circulant and it's eigenvalues are given by $\omega^k + \omega^{-k}, \forall$ $0 \le k \le n-1$, where $\omega = \mathbf{exp}(2\pi\iota/n)$

Non-degeneracy of dual opt

E.g for n = 5 :

$$\underbrace{\left(\begin{array}{c|ccccc} 0 & m_1 & m_2 & m_3 & m_4 & m_5 \\ \hline m_1 & m_1 & 0 & m_6 & m_9 & 0 \\ m_2 & 0 & m_2 & 0 & m_7 & m_{10} \\ m_3 & m_6 & 0 & m_3 & 0 & m_8 \\ m_4 & m_9 & m_7 & 0 & m_4 & 0 \\ m_5 & 0 & m_{10} & m_8 & 0 & m_5 \end{array}\right)}_{M_5} \Downarrow \underbrace{\left(\begin{array}{c|ccccc} \sqrt{5} & -1 & -1 & -1 & -1 & -1 \\ \hline -1 & 1 & c & 0 & 0 & c \\ -1 & c & 1 & c & 0 & 0 \\ -1 & 0 & c & 1 & c & 0 \\ -1 & 0 & 0 & c & 1 & c \\ -1 & c & 0 & 0 & c & 1 \end{array}\right)}_{Z_5} = 0$$

where $c = \dfrac{5-\sqrt{5}}{2\sqrt{5}}$

$$\alpha = \frac{1-c}{c}$$

$$(0,0) \Longrightarrow Tr(M_5) = 0,$$

$$\begin{aligned} (1,2) &\Longrightarrow m_6 = \alpha m_1, & (1,5) &\Longrightarrow m_9 = \alpha m_1, \\ (2,3) &\Longrightarrow m_7 = \alpha m_2, & (2,1) &\Longrightarrow m_{10} = \alpha m_2, \\ (3,4) &\Longrightarrow m_8 = \alpha m_3, & (3,2) &\Longrightarrow m_6 = \alpha m_3, \\ (4,5) &\Longrightarrow m_9 = \alpha m_4, & (4,3) &\Longrightarrow m_7 = \alpha m_4, \\ (5,1) &\Longrightarrow m_{10} = \alpha m_5, & (5,4) &\Longrightarrow m_8 = \alpha m_5 . \end{aligned}$$

$$\Longrightarrow \quad M_5 = 0$$

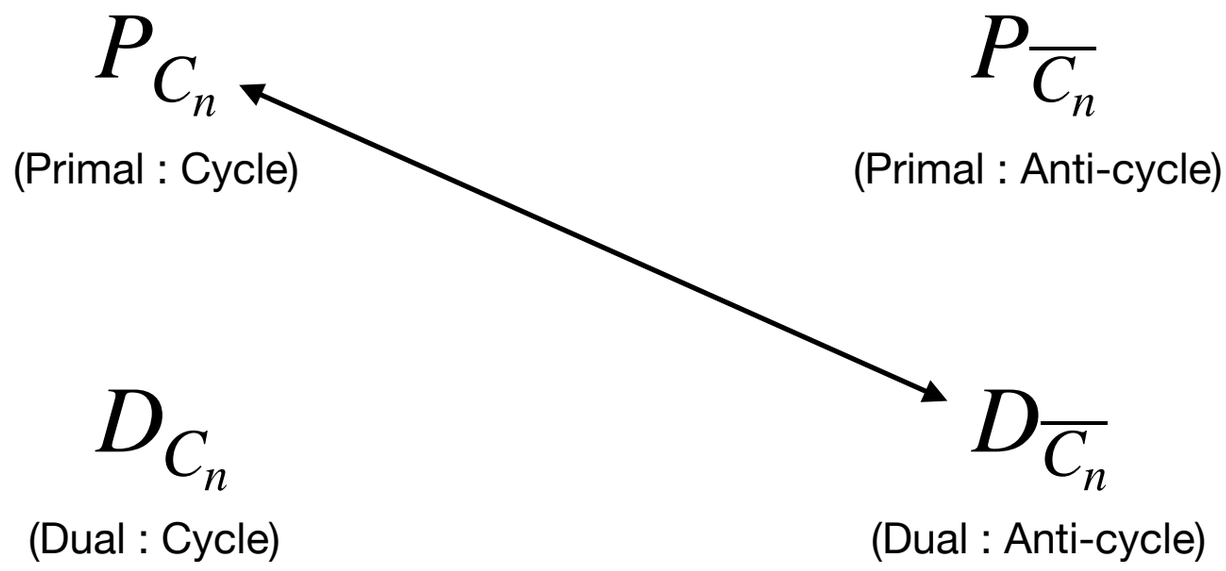
→ Can be generalised to all odd *n*

Result 2

Theorem: For any odd n, the non-contextuality inequality corresponding to the **anti-n-cycle** graph admits $\left(\epsilon, \frac{1}{2}\right)$-robust *self-test.* [arXiv:1911.09448]

Strategy

Idea : Relate primal solution of cycles to dual solution of anti-cycles.



Theorem : Let $X^* = \textbf{Gram}(v_0, v_1, \cdots, v_n)$ be the unique optimal solution for P_{C_n}. Then, $Z^* = \vartheta(\overline{C_n})\textbf{Gram}(-v_0, v_1, \cdots, v_n)$ is a dual optimal solution for $D_{\overline{C_n}}$.

Z^* can also be expressed as : $Z^* = \left[\begin{array}{c|c} \vartheta(\overline{C_n}) & -e^T \\ \hline -e & circ(u) \end{array}\right]$

where $u = (1, \vartheta(\overline{C_n})\langle v_1 \,|\, v_2\rangle, \cdots, \vartheta(\overline{C_n})\langle v_1 \,|\, v_n\rangle)$

Application - Certify high dim

Claim : For all odd *n,* the dimension in which the quantum realisations corresponding to the anti-*n*-cycle graph achieves the maximum (Lovasz theta) is *n-2*.

Idea :

$$X^* = \left[\begin{array}{c|c} 1 & \frac{\bar{\vartheta}_n}{n} e^T \\ \hline \frac{\bar{\vartheta}_n}{n} e & circ(u) \end{array}\right] \quad \text{with} \quad u = \left(\frac{\vartheta(\overline{C}_n)}{n}, \frac{n-\vartheta(C_n)}{2\vartheta(C_n)^2}, 0, 0, \cdots, 0, 0, \frac{n-\vartheta(C_n)}{2\vartheta(C_n)^2} \right)$$

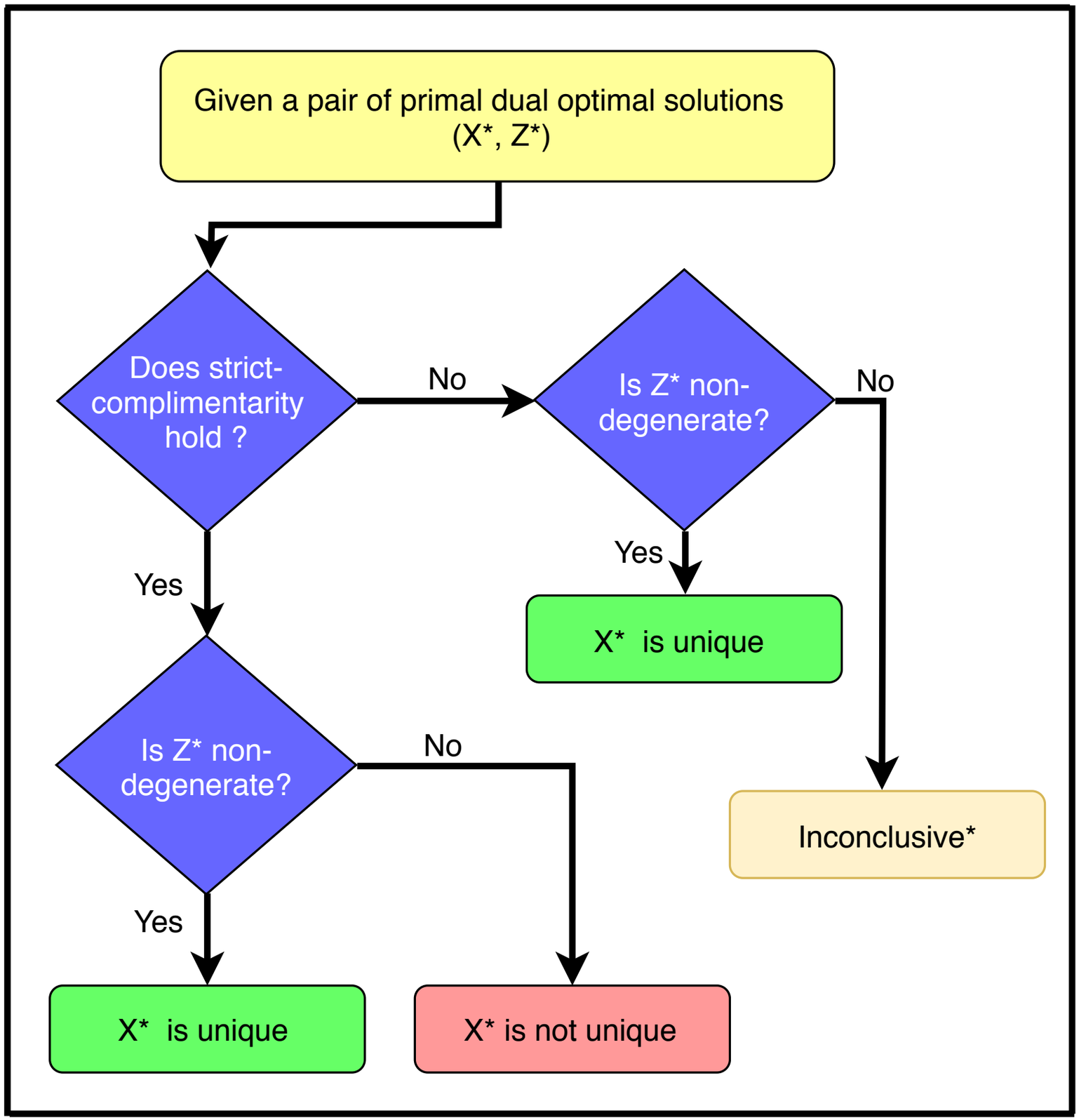
is the unique primal optimal.

$$Eig(circ(u)) = \left\{ \frac{1}{\vartheta_n} + \frac{n-\vartheta_n}{\vartheta_n} \cos\left(\frac{2\pi j}{n}\right) : j \in [n] \right\} \neq 0 \quad unless \quad j = \frac{n-1}{2} \quad or \quad \frac{n+1}{2}$$

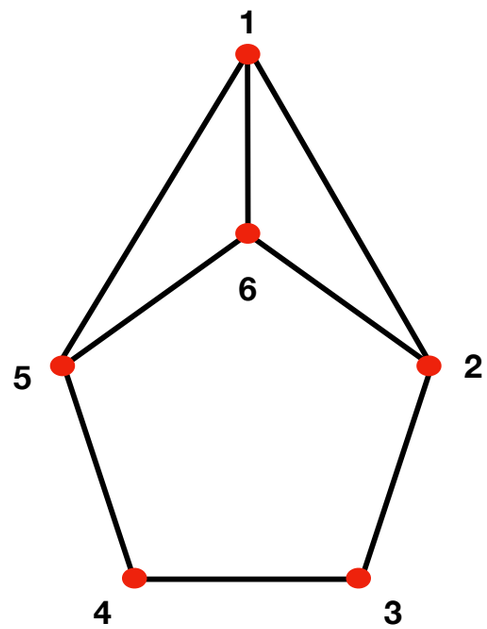
$$Rank(X^*) \geq n-2$$

Explicit construction exists for dim = *n-2*

For general graphs



- Not all graphs can be self-tested.



Open problems

- A complete characterisation of all self-testable graphs ?
  - Easier problem 1: G self-testable imply $\overline{G}$ too?
  - Easier problem 2: Can vertex transitivity help ?
- Explicit robustness bounds.
- Large gaps between $\vartheta(G)\, and\, \alpha(G)$?
- Results on verifying quantum computation by classical verifier leverages self-testing results. Can local self-testing schemes help ?

Quantum dimension witnesses

Bell inequalities in d-dimensional space : $\sum_{a,b,x,y} s_{xy}^{ab} P^d(a,b \mid x,y) \leq S_Q^d$

where $P^d(a,b \mid x,y) = \left\langle \psi_{AB} \right| M_{a|x} \otimes M_{b|y} \left| \psi_{AB} \right\rangle$ and $\left| \psi_{AB} \right\rangle \in \mathbb{C}^d, M_{a|x} \otimes M_{b|y} \in \mathbb{C}^{d \times d}$

Violation of the inequality $\Longrightarrow$ underlying quantum system has dimensions $\geq d+1$

References :

- DW in prepare and measure scenarios [Brunner et. al, PRL ’08]
- DW in Bell-nonlocal scenarios [Brunner et. al, PRL ’13] [Navascues et. al, PRL ’15]
- DW for high dimensional entanglement testing [Chao, Reichardt, Sutherland, Vidick, Quantum ’18] [Coladangelo, Quantum 2020]
- DW in contextuality framework [Guhne et. al, PRA ‘14]

Quantum correlations with dimensional restrictions

For an exclusivity graph $\mathcal{G}_{ex}$, behaviour $p : [n] \to [0,1]$ is d-quantum if $\exists$ d-dimensional quantum state $|\psi\rangle$ and projectors $\Pi_1, \Pi_2, \ldots, \Pi_n$, such that

- $p_i = \langle\psi|\Pi_i|\psi\rangle, \forall i \in [n]$
- $\mathbf{Tr}(\Pi_i\Pi_j) = 0, \forall\ i \sim j$

$\Pi_1, \Pi_2, \ldots, \Pi_n$ **is a d-dimensional orthonormal representation of $\mathcal{G}_{ex}$**

The **orthogonal rank** $R_o(\mathcal{G}_{ex})$, is the minimum d such that there exists a d-dimensional orthonormal representation for $\mathcal{G}_{ex}$.

The Lovász rank $R_L(\mathcal{G}_{ex})$, is the minimum d for which $\vartheta(\mathcal{G}_{ex}) = \vartheta^d(\mathcal{G}_{ex})$.

$$\vartheta^d\left(\mathcal{G}_{\mathrm{ex}}\right) = \max \sum_{i=1}^{n} X_{ii}$$

subject to $X_{ii} = X_{0i}, \forall i = 1,\ldots,n$

$$X_{ij} = 0\,\forall\, i \sim j, X_{00} = 1, X \in \mathcal{S}_{+}^{1+n}$$

$$\mathrm{rank}(X) \leq d$$

Quantum correlations with dimensional restrictions

$$\vartheta^{R_o(\mathcal{G}_{\mathrm{ex}})}\left(\mathcal{G}_{\mathrm{ex}}\right) \leq \vartheta^{R_o(\mathcal{G}_{\mathrm{ex}})+1}\left(\mathcal{G}_{\mathrm{ex}}\right) \leq \cdots \leq \vartheta^{R_L(\mathcal{G}_{\mathrm{ex}})}\left(\mathcal{G}_{\mathrm{ex}}\right) = \vartheta\left(\mathcal{G}_{\mathrm{ex}}\right)$$

A violation of the inequality $\sum_{i\in[n]} p_i \leq \vartheta^d(G), p \in \mathrm{TH}(\mathcal{G}_{ex})$ implies - underlying quantum system must have dimension $\geq d+1$.

Result 3: Identify a class of graphs which allows us to certify arbitrarily high quantum dimensions.

[arXiv:2007.10746, New Journal of Physics,2020]

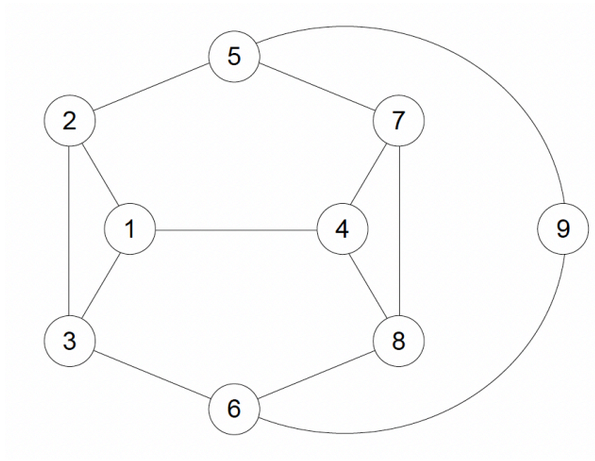
Low rank solutions

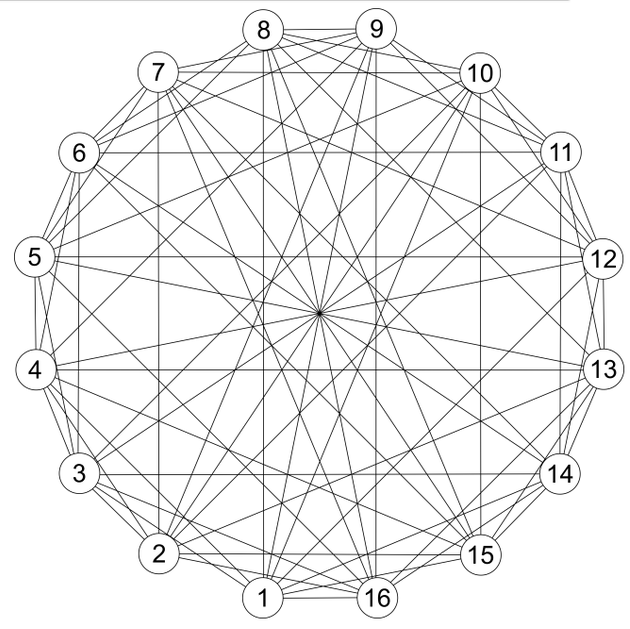
Algorithm 1: Heuristics using SDPs.

input : Graph G having n nodes, dimension d, number of iterations $\mathtt{k}$
output: A lower bound to $\vartheta^d(G)$

Generate a random matrix $W \in \mathbb{R}^{(n+1)\times(n+1)}$;
iter = 1;
while *iter* $< k$ **do**
    Minimise $\mathrm{tr}((W - I_{n+1})X)$, subject to $X \succeq 0$, $X_{00} = 1$, $X_{ii} = X_{0i}$ for all i and $X_{ij} = 0$ for all $i \sim j$;
    Obtain optimal X for the above SDP;
    Minimise $\mathrm{tr}(XW)$, subject to $I_{n+1} \succeq W \succeq 0$, $\mathrm{tr}(W) = n + 1 - d$;
    Obtain optimal W from the above SDP ;
    iter = *iter* + 1;
end

Examples :





$d =$	3	4
$\vartheta^d(G_1) \geq$	3.333	$3.4706 = \vartheta(G_1)$

$d =$	4	5	6	7
$\vartheta^d(G_2) \geq$	3.414	3.436	3.6514	$4 = \vartheta(G_2)$

Family of Qites: Definition

A k-Qite graph has $2k+1$ vertices, $v_1, v_2, \ldots, v_{2k+1}$, with the first k vertices forming a fully connected graph. Vertex v_i is connected to vertex v_{i+k}, for all $1 \leq i \leq k$. Vertex v_{2k+1} is connected to vertices v_{k+i}, for all $1 \leq i \leq k$.

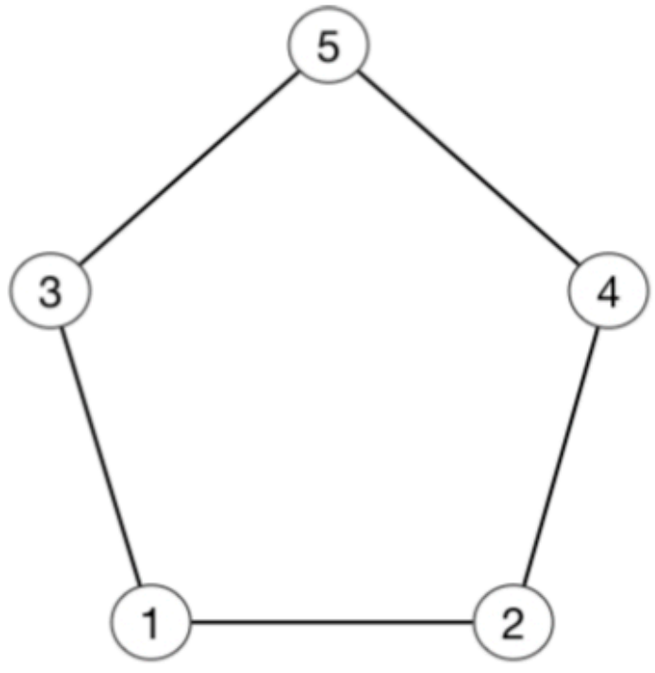


Figure 5: 2-Qite $\equiv C_5$, where $\alpha(C_5) = 2, \vartheta(C_5) = \sqrt{5} \approx 2.2361$

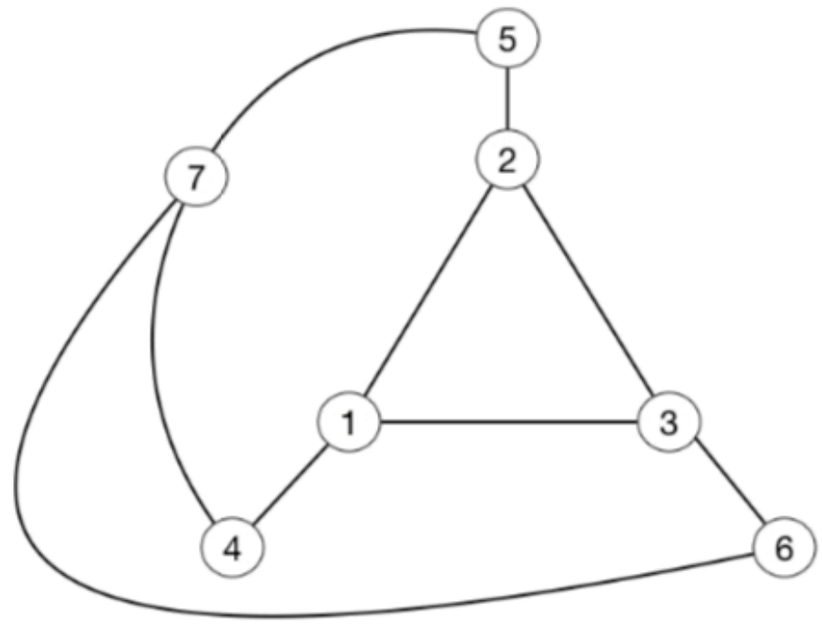


Figure 6: 3-Qite, where $\alpha(\text{3-Qite}) = 3, \vartheta(\text{3-Qite}) \approx 3.0642$

Fact: $\vartheta(\text{k-}Qite) > k$, for all $k \geq 3$.

Family of Qites: Results

Lemma: The independence number of the k-Qite graph is k.

Lemma: $R_o(\text{k-}Qite) = k$, for all $k \geq 3$.

Theorem: $\vartheta^k(\text{k-}Qite) \leq k$, for all $k \geq 3$.

Corollary: Violating the non-contextuality inequality

$$\sum_i p_i \leq k, \text{ where } p \in \text{TH}(\text{k-}Qite),$$

implies that the underlying quantum realisation must have dimension at least $k + 1$.

Conclusions

Main application: Certify dimensions of local quantum systems for arbitrary high dimensions

Open problems:

- Find generic analytical (upper) bounds on $\vartheta^d(\mathcal{G}_{ex})$.
- Find noise-robust DW.
- Developing a general graph-theoretic framework to analyse and unify different approaches to dimension witnessing.

Thanks! Questions ?