Constant-sized robust self-tests for states and measurements of unbounded dimension

Jitendra Prakash
University of Copenhagen

(Jointly with Laura Mančinska and Christopher Schafhauser)

February 1, 2021

Introduction

- **Self-testing**: Techniques in QIT to infer the quantum-mechanical description of a device from classical observations

Introduction

- **Self-testing**: Techniques in QIT to infer the quantum-mechanical description of a device from classical observations
- **Applications**: device-independent quantum cryptography, entanglement detection, investigating the structure of the quantum correlation set, quantum complexity theory

Introduction

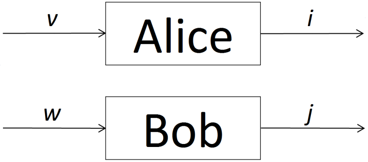
- **Self-testing**: Techniques in QIT to infer the quantum-mechanical description of a device from classical observations
- **Applications**: device-independent quantum cryptography, entanglement detection, investigating the structure of the quantum correlation set, quantum complexity theory
- Has been used in the recent breakthrough: $\mathrm{MIP}^* = \mathrm{RE}$ [JNV+20]. Implication: Negative resolution of the Connes' embedding problem – open since 70s

General scenario

Suppose Alice and Bob (spatially separated) share a quantum state and each of them has a quantum device.

Suppose Alice and Bob (spatially separated) share a quantum state and each of them has a quantum device.

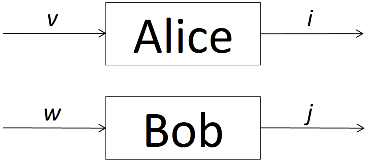
Quantum device: n measurement settings $\{1, \ldots, n\}$, each setting has k outcomes $\{1, \ldots, k\}$.



General scenario

Suppose Alice and Bob (spatially separated) share a quantum state and each of them has a quantum device.

Quantum device: n measurement settings $\{1, \ldots, n\}$, each setting has k outcomes $\{1, \ldots, k\}$.

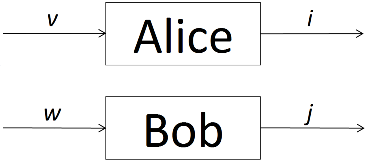


$p(i, j|v, w)$ - joint conditional probability that Alice gets outcome i and Bob gets j, provided that they performed measurements v and w, respectively.

General scenario

Suppose Alice and Bob (spatially separated) share a quantum state and each of them has a quantum device.

Quantum device: n measurement settings $\{1, \ldots, n\}$, each setting has k outcomes $\{1, \ldots, k\}$.



$p(i, j|v, w)$ - joint conditional probability that Alice gets outcome i and Bob gets j, provided that they performed measurements v and w, respectively.

In certain cases, self-testing allows one to infer what the quantum state and quantum measurements must have been from the statistics $p(i, j|v, w)$.

A quantum strategy is given by a triple

$$\mathscr{S} = \left(\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}, \{E_{v,i} : 1 \le v \le n, 1 \le i \le k\}, \{F_{w,j} : 1 \le w \le n, 1 \le j \le k\}\right),$$

where

Quantum strategy and quantum correlation

A quantum strategy is given by a triple

$$\mathscr{S} = \left(\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}, \{E_{v,i} : 1 \leq v \leq n, 1 \leq i \leq k\}, \{F_{w,j} : 1 \leq w \leq n, 1 \leq j \leq k\}\right),$$

where

- ψ is a unit vector (called a quantum state),
- $E_{v,i} \geq 0$ and $\sum_i E_{v,i} = I_{d_A}$ for each v,
- $F_{w,j} \geq 0$ and $\sum_j F_{w,j} = I_{d_B}$ for each w.

Quantum strategy and quantum correlation

A quantum strategy is given by a triple

$$\mathscr{S} = \left(\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}, \{E_{v,i} : 1 \le v \le n, 1 \le i \le k\}, \{F_{w,j} : 1 \le w \le n, 1 \le j \le k\}\right),$$

where

- ψ is a unit vector (called a quantum state),
- $E_{v,i} \ge 0$ and $\sum_i E_{v,i} = I_{d_A}$ for each v,
- $F_{w,j} \ge 0$ and $\sum_j F_{w,j} = I_{d_B}$ for each w.

The induced **quantum correlation** is given by

$$p(i,j|v,w) = \langle (E_{v,i} \otimes F_{w,j})\psi, \psi \rangle .$$

An example: CHSH game

CHSH game: 2-input, 2-output non-local game

An example: CHSH game

CHSH game: 2-input, 2-output non-local game

Quantum value $\omega_q(CHSH) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.85$ (Maximum winning probability using quantum strategies).

Using the (canonical) strategy:

$$(\varphi_2 \in \mathbb{C}^2 \otimes \mathbb{C}^2, \{\widetilde{A}_0 = Z, \widetilde{A}_1 = X\}, \{\widetilde{B}_0 = \frac{Z+X}{\sqrt{2}}, \widetilde{B}_1 = \frac{Z-X}{\sqrt{2}}\}).$$

An example: CHSH game

CHSH game: 2-input, 2-output non-local game

Quantum value $\omega_q(CHSH) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.85$ (Maximum winning probability using quantum strategies).

Using the (canonical) strategy:

$$(\varphi_2 \in \mathbb{C}^2 \otimes \mathbb{C}^2, \{\widetilde{A}_0 = Z, \widetilde{A}_1 = X\}, \{\widetilde{B}_0 = \frac{Z + X}{\sqrt{2}}, \widetilde{B}_1 = \frac{Z - X}{\sqrt{2}}\}).$$

In general, if $\mathscr{S} = (\psi \in \mathbb{C}^d \otimes \mathbb{C}^d, \{A_0, A_1\}, \{B_0, B_1\})$ is any other strategy which achieves the quantum value then there exist isometries $V_A : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathcal{K}_A$ and $V_B : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathcal{K}_B$ and some junk state $\psi_{junk} \in \mathcal{K}_A \otimes \mathcal{K}_B$ such that

$$(V_A \otimes V_B)(A_i \otimes B_j)\psi = (\widetilde{A}_i \otimes \widetilde{B}_j)\varphi_2 \otimes \psi_{junk}.$$

This is an example of “self-testing”.

An example: CHSH game

CHSH game: 2-input, 2-output non-local game

Quantum value $\omega_q(CHSH) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.85$ (Maximum winning probability using quantum strategies).

Using the (canonical) strategy:

$$(\varphi_2 \in \mathbb{C}^2 \otimes \mathbb{C}^2, \{\widetilde{A}_0 = Z, \widetilde{A}_1 = X\}, \{\widetilde{B}_0 = \frac{Z + X}{\sqrt{2}}, \widetilde{B}_1 = \frac{Z - X}{\sqrt{2}}\}).$$

In general, if $\mathscr{S} = (\psi \in \mathbb{C}^d \otimes \mathbb{C}^d, \{A_0, A_1\}, \{B_0, B_1\})$ is any other strategy which achieves the quantum value then there exist isometries $V_A : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathcal{K}_A$ and $V_B : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathcal{K}_B$ and some junk state $\psi_{junk} \in \mathcal{K}_A \otimes \mathcal{K}_B$ such that

$$(V_A \otimes V_B)(A_i \otimes B_j)\psi = (\widetilde{A}_i \otimes \widetilde{B}_j)\varphi_2 \otimes \psi_{junk}.$$

This is an example of "self-testing". Robust self-testing: when $\omega_q(\mathscr{S}) \approx_\epsilon \omega_q(CHSH)$, then

$$(V_A \otimes V_B)(A_i \otimes B_j)\psi \approx_{f(\epsilon)} (\widetilde{A}_i \otimes \widetilde{B}_j)\varphi_2 \otimes \psi_{junk}.$$

An example: CHSH game

Proof technique:

1. Associate a group (the dihedral group of order 8) with the CHSH game.

An example: CHSH game

Proof technique:

1. Associate a group (the dihedral group of order 8) with the CHSH game.
2. Show that perfect strategies lead to a representation of the group; and approximately perfect strategies lead to "approximate" representations of the group.

An example: CHSH game

Proof technique:

1. Associate a group (the dihedral group of order 8) with the CHSH game.
2. Show that perfect strategies lead to a representation of the group; and approximately perfect strategies lead to “approximate” representations of the group.
3. Use Gowers-Hatami Theorem to find the isometry relating the approximate representation to the canonical one.

Projections summing up to scalar times the identity

We consider $d \times d$ projections $\widetilde{P}_1, \ldots, \widetilde{P}_n$ ($n \geq 3$) with

$$\widetilde{P}_1 + \cdots + \widetilde{P}_n = xI_d = \frac{b}{d} I_d,$$

where $\gcd(b, d) = 1$.

Projections summing up to scalar times the identity

We consider $d \times d$ projections $\widetilde{P}_1, \dots, \widetilde{P}_n$ ($n \geq 3$) with

$$\widetilde{P}_1 + \cdots + \widetilde{P}_n = xI_d = \frac{b}{d} I_d,$$

where $\gcd(b, d) = 1$.

The scalar x and the projections $\widetilde{P}_1, \dots, \widetilde{P}_n$ have the property that whenever $P_1, \dots, P_n$ are any other projections such that $P_1 + \cdots + P_n = xI$, then $P_i = I \otimes \widetilde{P}_i$ for all $1 \leq i \leq n$ in some basis. Λ_n - the set of such scalars x.

Projections summing up to scalar times the identity

We consider $d \times d$ projections $\widetilde{P}_1, \ldots, \widetilde{P}_n$ ($n \geq 3$) with

$$\widetilde{P}_1 + \cdots + \widetilde{P}_n = xI_d = \frac{b}{d} I_d,$$

where $\gcd(b, d) = 1$.

The scalar x and the projections $\widetilde{P}_1, \ldots, \widetilde{P}_n$ have the property that whenever $P_1, \ldots, P_n$ are any other projections such that $P_1 + \cdots + P_n = xI$, then $P_i = I \otimes \widetilde{P}_i$ for all $1 \leq i \leq n$ in some basis. Λ_n - the set of such scalars x.

Example

Take any $n \geq 3$ and consider n unit vectors $\xi_1, \ldots, \xi_n$ in $\mathbb{R}^{n-1}$ which form the vertices of a regular n-simplex centered at the origin. Then their corresponding projections $\widetilde{P}_i = \xi_i \xi_i^*$ form an irreducible representation of the relation $P_1 + \cdots + P_n = \frac{n}{n-1} I$.

More in the paper [KRS02].

Quantum strategy from projections summing up to scalar times the identity

For $n \geq 3$ and $x \in \Lambda_n$, and $\widetilde{P}_1, \ldots, \widetilde{P}_n$ as above, we define a quantum strategy

$$\widetilde{\mathscr{S}}_{n,x} = (\varphi_d \in \mathbb{C}^d \otimes \mathbb{C}^d, \{\widetilde{P}_v, I_d - \widetilde{P}_v\}_{v=1}^n, \{\widetilde{P}_w^T, I_d - \widetilde{P}_w^T\}_{w=1}^n),$$

where $\varphi_d = \frac{1}{\sqrt{d}} \sum_i e_i \otimes e_i$ is the maximally entangled state.

Let $\widetilde{p}_{n,x}$ denote the quantum correlation induced by $\widetilde{\mathscr{S}}_{n,x}$.

Main result

If we have a a quantum strategy $\mathscr{S}$ which induces a quantum correlation p close to the ideal correlation $\widetilde{p}_{n,x}$, then the strategy $\mathscr{S}$ must be close to the ideal quantum strategy $\widetilde{\mathscr{S}}_{n,x}$.

Main result

If we have a a quantum strategy $\mathscr{S}$ which induces a quantum correlation p close to the ideal correlation $\widetilde{p}_{n,x}$, then the strategy $\mathscr{S}$ must be close to the ideal quantum strategy $\widetilde{\mathscr{S}}_{n,x}$.

Theorem

Let $n \geq 3, x \in \Lambda_n$ and let $\widetilde{P}_1, \ldots, \widetilde{P}_n$ be projections as above. For any $\epsilon \geq 0$, there exists a $\delta \geq 0$ such that the following holds. Let p be a quantum correlation induced from an arbitrary quantum strategy

$$\mathscr{S} = (\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}, \{E_v, I_{d_A} - E_v\}_{v=1}^{n}, \{F_w, I_{d_B} - F_w\}_{w=1}^{n}),$$

such that $\|\widetilde{p}_{n,x} - p\| \leq \delta$. Then $\mathscr{S}$ is approximately related to $\widetilde{\mathscr{S}}_{n,x}$ via a local isometry, that is, there exist isometries $V_A \colon \mathbb{C}^{d_A} \to \mathbb{C}^{d} \otimes \mathbb{C}^{r_A}$ and $V_B \colon \mathbb{C}^{d_B} \to \mathbb{C}^{d} \otimes \mathbb{C}^{r_B}$ for some $r_A, r_B \in \mathbb{N}$ and a quantum state $\psi_{\text{junk}} \in \mathbb{C}^{r_A} \otimes \mathbb{C}^{r_B}$ such that for all $1 \leq v, w \leq n$,

$$(V_A \otimes V_B)(E_v \otimes F_w)\psi \approx_\epsilon (\widetilde{P}_v \otimes \widetilde{P}_w^T)\varphi_d \otimes \psi_{\text{junk}},$$
$$(V_A \otimes V_B)\psi \approx_\epsilon \varphi_d \otimes \psi_{\text{junk}}.$$

Proof outline

- Associate a C*-algebra with the relation $p_1 + \cdots + p_n = x1$.
- Show that "approximate" strategies lead to "approximate" representations of the C*-algebra
- Use the following analogue of Gowers-Hatami Theorem:

Theorem

(Informal) Suppose positive semi-definite matrices $E_1, \ldots, E_n \in \mathbb{M}_{d_A}$ are "approximate" projections and form an "approximate" representation (with respect to ρ_A) of the relation $p_1 + \cdots + p_n = xI$. Then, there exists an isometry $V : \mathbb{C}^{d_A} \to \mathbb{C}^d \otimes \mathbb{C}^{r_A}$ such that for all $1 \leq v \leq n$, we have $\left\| E_v - V^*(\widetilde{P}_v \otimes I_s)V \right\|_{\rho_A} \approx 0$.

Corollaries

Example ($n = 4$)

For any $k \in \mathbb{N}$, there exists four rank k projections $\widetilde{P}_{k,1}, \widetilde{P}_{k,2}, \widetilde{P}_{k,3}, \widetilde{P}_{k,4}$ in $\mathbb{M}_{2k+1}$ such that $\widetilde{P}_{k,1} + \widetilde{P}_{k,2} + \widetilde{P}_{k,3} + \widetilde{P}_{k,4} = \frac{4k}{2k+1} I_{2k+1}$. We can robustly self-test each of the strategies

$$\widetilde{\mathscr{S}_k} = (\varphi_{2k+1}, \{\widetilde{P}_{k,v}, I_{2k+1} - \widetilde{P}_{k,v}\}_{v=1}^{4}, \{\widetilde{P}_{k,w}^{T}, I_{2k+1} - \widetilde{P}_{k,w}^{T}\}_{w=1}^{4}),$$

from the correlations $\widetilde{p}_{4,k}$ that each strategy induces.

Corollaries (cotd.)

Self-testing of quantum states is relatively well understood:

Corollaries (cotd.)

Self-testing of quantum states is relatively well understood:

1. Any (pure) bipartite entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be self-tested from a correlation with 3 inputs and d outputs [CGS17].

Corollaries (cotd.)

Self-testing of quantum states is relatively well understood:

1. Any (pure) bipartite entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be self-tested from a correlation with 3 inputs and d outputs [CGS17].
2. For each $d \in \mathscr{D}$, where $\mathscr{D}$ is an infinite subset of the primes, the maximally entangled state $\varphi_{4(d-1)}$ can be robustly self-tested from correlations with roughly 100 inputs per party [Fu19].

Corollaries (cotd.)

Self-testing of quantum states is relatively well understood:

1. Any (pure) bipartite entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be self-tested from a correlation with 3 inputs and d outputs [CGS17].
2. For each $d \in \mathscr{D}$, where $\mathscr{D}$ is an infinite subset of the primes, the maximally entangled state $\varphi_{4(d-1)}$ can be robustly self-tested from correlations with roughly 100 inputs per party [Fu19].

Corollary

For each odd dimension $d \geq 3$, the maximally entangled state φ_d can be robustly self-tested by quantum correlations with four inputs and two outputs.

Corollaries (cotd.)

Self-testing of quantum states is relatively well understood:

1. Any (pure) bipartite entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be self-tested from a correlation with 3 inputs and d outputs [CGS17].
2. For each $d \in \mathscr{D}$, where $\mathscr{D}$ is an infinite subset of the primes, the maximally entangled state $\varphi_{4(d-1)}$ can be robustly self-tested from correlations with roughly 100 inputs per party [Fu19].

Corollary

For each odd dimension $d \geq 3$, the maximally entangled state φ_d can be robustly self-tested by quantum correlations with four inputs and two outputs.

Corollary

Given any natural number k there exist four projections of rank k which can be robustly self-tested by quantum correlations with four inputs and two outputs.

References

A. Coladangelo, K. T. Goh, and V. Scarani.
All pure bipartite entangled states can be self-tested.
Nature Communications, 8(1), May 2017.

H. Fu.
Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension.
arXiv e-prints, page arXiv:1911.01494, November 2019.

Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen.
MIP*=RE.
arXiv e-prints, page arXiv:2001.04383, January 2020.

S. A. Kruglyak, V. I. Rabanovich, and Yu. S. Samoĭlenko.
On sums of projections.
Funktsional. Anal. i Prilozhen., 36(3):20–35, 96, 2002.