The Navascués–Pironio–Acín hierarchy

Guillaume Aubrun

Université Lyon 1, France

April 9, 2020

Reference : `arXiv:0803.4290`, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations.

Recall from lecture 1: Connes' embedding problem $\iff$ Kirchberg conjecture $\iff$ Tsirelson problem.

Tsirelson problem asks whether the equality $\mathsf{C}_{\mathrm{qc}}^{m,d} = \overline{\mathsf{C}_{\mathrm{q}\otimes}^{m,d}}$ holds for every m, d (definition in next slides). A negative answer is announced in the $\mathsf{MIP}^* = \mathsf{RE}$ paper.

qc = quantum commuting, $\mathrm{q}\otimes$ = quantum tensor product

Recall from lecture 1: Connes' embedding problem $\iff$ Kirchberg conjecture $\iff$ Tsirelson problem.

Tsirelson problem asks whether the equality $\mathrm{C}_{\mathrm{qc}}^{m,d} = \overline{\mathrm{C}_{\mathrm{q}\otimes}^{m,d}}$ holds for every m, d (definition in next slides). A negative answer is announced in the $\mathrm{MIP}^* = \mathrm{RE}$ paper.

qc = quantum commuting, $\mathrm{q}\otimes$ = quantum tensor product

Both $\mathrm{C}_{\mathrm{qc}}^{m,d}$ and $\mathrm{C}_{\mathrm{q}\otimes}^{m,d}$ are sets of correlation matrices, of the form

$$p(ab|xy)_{a,b\in[m];x,y\in[d]},$$

such that, at fixed x, y, $p(ab|xy)_{a,b}$ is a probability distribution on $[m]^2$.

We now drop the superscripts m and d.

The set of quantum correlation matrices with commuting measurements C_{qc} is the set of correlation matrices $p(ab|xy)$ of the form

$$p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in a Hilbert space $\mathcal{H}$,
- for every $x \in [d]$, $(P_x^a)_{a \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $y \in [d]$, $(Q_y^b)_{b \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $x, y \in [d]$, and $a, b \in [m]$, we have $[P_x^a, Q_y^b] = 0$.

PVM (projector-valued measure) $=$ finite family of orthogonal projections summing to Id.

The set of quantum correlation matrices with commuting measurements C_{qc} is the set of correlation matrices $p(ab|xy)$ of the form

$$p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in a Hilbert space $\mathcal{H}$,
- for every $x \in [d]$, $(P_x^a)_{a \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $y \in [d]$, $(Q_y^b)_{b \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $x, y \in [d]$, and $a, b \in [m]$, we have $[P_x^a, Q_y^b] = 0$.

PVM (projector-valued measure) = finite family of orthogonal projections summing to Id.

$\mathsf{C}_{\mathrm{qc}} \subset [0,1]^{m^2 d^2}$;

The set of quantum correlation matrices with commuting measurements C_{qc} is the set of correlation matrices $p(ab|xy)$ of the form

$$p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in a Hilbert space $\mathcal{H}$,
- for every $x \in [d]$, $(P_x^a)_{a \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $y \in [d]$, $(Q_y^b)_{b \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $x, y \in [d]$, and $a, b \in [m]$, we have $[P_x^a, Q_y^b] = 0$.

PVM (projector-valued measure) = finite family of orthogonal projections summing to Id.

$\mathsf{C}_{\mathrm{qc}} \subset [0,1]^{m^2 d^2}$; C_{qc} is a convex set (easy) ;

The set of quantum correlation matrices with commuting measurements C_{qc} is the set of correlation matrices $p(ab|xy)$ of the form

$$p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in a Hilbert space $\mathcal{H}$,
- for every $x \in [d]$, $(P_x^a)_{a \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $y \in [d]$, $(Q_y^b)_{b \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $x, y \in [d]$, and $a, b \in [m]$, we have $[P_x^a, Q_y^b] = 0$.

PVM (projector-valued measure) = finite family of orthogonal projections summing to Id.

$\mathsf{C}_{\mathrm{qc}} \subset [0,1]^{m^2 d^2}$; C_{qc} is a convex set (easy) ;
$\dim(\mathsf{C}_{\mathrm{qc}}) = m^2(d-1)^2 + 2m(d-1) < m^2 d^2$ — because of the nonsignalling conditions $p(a|xy) = p(a|xy'), \;\; p(b|xy) = p(b|x'y)$

The set of quantum correlation matrices with commuting measurements C_{qc} is the set of correlation matrices $p(ab|xy)$ of the form

$$p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in a Hilbert space $\mathcal{H}$,
- for every $x \in [d]$, $(P_x^a)_{a \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $y \in [d]$, $(Q_y^b)_{b \in [m]}$ is a PVM on $\mathcal{H}$,
- for every $x, y \in [d]$, and $a, b \in [m]$, we have $[P_x^a, Q_y^b] = 0$.

PVM (projector-valued measure) = finite family of orthogonal projections summing to Id.

$\mathrm{C}_{\mathrm{qc}} \subset [0,1]^{m^2 d^2}$; C_{qc} is a convex set (easy) ;
$\dim(\mathrm{C}_{\mathrm{qc}}) = m^2(d-1)^2 + 2m(d-1) < m^2 d^2$ — because of the nonsignalling conditions $p(a|xy) = p(a|xy'),\ \ p(b|xy) = p(b|x'y)$
C_{qc} is closed (not obvious, will follow from today's proof)

The set of quantum correlation matrices with tensor measurements $\mathrm{C}_{\mathrm{q}\otimes}$ is the set of correlation matrices $p(ab|xy)_{a,b\in[m];x,y\in[d]}$ of the form

$$p(ab|xy) = \langle \xi | P_x^a \otimes Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ are Hilbert spaces,
- for every $x \in [d]$, $(P_x^a)_{a\in[m]}$ is a PVM on $\mathcal{H}_1$,
- for every $y \in [d]$, $(Q_y^b)_{b\in[m]}$ is a PVM on $\mathcal{H}_2$.

The set of quantum correlation matrices with tensor measurements $\mathrm{C}_{\mathrm{q}\otimes}$ is the set of correlation matrices $p(ab|xy)_{a,b\in[m];x,y\in[d]}$ of the form

$$p(ab|xy) = \langle \xi | P_x^a \otimes Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ are Hilbert spaces,
- for every $x \in [d]$, $(P_x^a)_{a\in[m]}$ is a PVM on $\mathcal{H}_1$,
- for every $y \in [d]$, $(Q_y^b)_{b\in[m]}$ is a PVM on $\mathcal{H}_2$.

$\mathrm{C}_{\mathrm{q}\otimes} \subset \mathrm{C}_{\mathrm{qc}}$ because $[P_x^a \otimes \mathrm{Id}, \mathrm{Id} \otimes Q_y^b] = 0$;

The set of quantum correlation matrices with tensor measurements $\mathsf{C}_{\mathrm{q}\otimes}$ is the set of correlation matrices $p(ab|xy)_{a,b\in[m];x,y\in[d]}$ of the form

$$p(ab|xy) = \langle \xi | P_x^a \otimes Q_y^b | \xi \rangle$$

where

- ξ is a unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ are Hilbert spaces,
- for every $x \in [d]$, $(P_x^a)_{a\in[m]}$ is a PVM on $\mathcal{H}_1$,
- for every $y \in [d]$, $(Q_y^b)_{b\in[m]}$ is a PVM on $\mathcal{H}_2$.

$\mathsf{C}_{\mathrm{q}\otimes} \subset \mathsf{C}_{\mathrm{qc}}$ because $[P_x^a \otimes \mathrm{Id}, \mathrm{Id} \otimes Q_y^b] = 0$;
$\mathsf{C}_{\mathrm{q}\otimes}$ is convex (easy)

The set of quantum correlation matrices with tensor measurements $\mathrm{C}_{\mathrm{q}\otimes}$ is the set of correlation matrices $p(ab|xy)_{a,b\in[m];x,y\in[d]}$ of the form

$$p(ab|xy) = \langle\xi|P_x^a \otimes Q_y^b|\xi\rangle$$

where

- ξ is a unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ are Hilbert spaces,
- for every $x \in [d]$, $(P_x^a)_{a\in[m]}$ is a PVM on $\mathcal{H}_1$,
- for every $y \in [d]$, $(Q_y^b)_{b\in[m]}$ is a PVM on $\mathcal{H}_2$.

$\mathrm{C}_{\mathrm{q}\otimes} \subset \mathrm{C}_{\mathrm{qc}}$ because $[P_x^a \otimes \mathrm{Id}, \mathrm{Id} \otimes Q_y^b] = 0$;
$\mathrm{C}_{\mathrm{q}\otimes}$ is convex (easy)
$\dim(\mathrm{C}_{\mathrm{q}\otimes}) = \dim(\mathrm{C}_{\mathrm{qc}})$

The set of quantum correlation matrices with tensor measurements $\mathrm{C}_{\mathrm{q}\otimes}$ is the set of correlation matrices $p(ab|xy)_{a,b\in[m];x,y\in[d]}$ of the form

$$p(ab|xy) = \langle\xi|P_x^a \otimes Q_y^b|\xi\rangle$$

where

- ξ is a unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ are Hilbert spaces,
- for every $x \in [d]$, $(P_x^a)_{a\in[m]}$ is a PVM on $\mathcal{H}_1$,
- for every $y \in [d]$, $(Q_y^b)_{b\in[m]}$ is a PVM on $\mathcal{H}_2$.

$\mathrm{C}_{\mathrm{q}\otimes} \subset \mathrm{C}_{\mathrm{qc}}$ because $[P_x^a \otimes \mathrm{Id}, \mathrm{Id} \otimes Q_y^b] = 0$;
$\mathrm{C}_{\mathrm{q}\otimes}$ is convex (easy)
$\dim(\mathrm{C}_{\mathrm{q}\otimes}) = \dim(\mathrm{C}_{\mathrm{qc}})$
$\mathrm{C}_{\mathrm{q}\otimes}$ is not closed (cf. lecture 3).

Tsirelson's problem asks whether $\overline{\mathrm{C}_{\mathrm{q}\otimes}} = \mathrm{C}_{\mathrm{qc}}$. By the Hahn–Banach theorem, this is false if and only if there is a linear form G such that $\sup_{\mathrm{C}_{\mathrm{q}\otimes}} G < \max_{\mathrm{C}_{\mathrm{qc}}} G$.

In this talk, what we call a *game* is a linear form on $\mathbf{R}^{m^2 d^2}$ with rational coefficients (games satisfy some extra constraints, such as mapping correlation matrices to $[0,1]$)

In this talk, what we call a *game* is a linear form on $\mathbf{R}^{m^2 d^2}$ with rational coefficients (games satisfy some extra constraints, such as mapping correlation matrices to $[0,1]$)

Theorem 1 (Theorem 12.10 in the $\mathrm{MIP}^* = \mathrm{RE}$ paper)

There is a computable function which maps a Turing machine T *to a game* G *such that*

1. *If* T *halts on the empty word, then* $\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G = 1$,
2. *If* T *does not halt on the empty word, then* $\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G \leqslant 1/2$.

In this talk, what we call a *game* is a linear form on $\mathbf{R}^{m^2d^2}$ with rational coefficients (games satisfy some extra constraints, such as mapping correlation matrices to $[0,1]$)

Theorem 1 (Theorem 12.10 in the $\mathrm{MIP}^* = \mathrm{RE}$ paper)

There is a computable function which maps a Turing machine T to a game G such that

1. *If T halts on the empty word, then* $\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G = 1$*,*
2. *If T does not halt on the empty word, then* $\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G \leqslant 1/2$*.*

Formally, $f : \{0,1\}^* \to \{0,1\}^*$ and $\langle G\rangle = f(\langle \mathrm{T}\rangle)$. The parameters m, d of the game G depend on T and are included in $\langle G\rangle$.

We show the following. Consider m, d and a linear form G on $[0,1]^{m^2 d^2}$.

1. There is an algorithm which computes an increasing sequence (α_N) such that
$$\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \lim_{N\to\infty} \alpha_N = \sup_{\mathsf{C}_{\mathrm{q}\otimes}} G.$$
2. There is an algorithm which computes a decreasing sequence (β_N) such that
$$\beta_1 \geqslant \beta_2 \geqslant \cdots \geqslant \lim_{N\to\infty} \beta_N = \max_{\mathsf{C}_{\mathrm{qc}}} G.$$

We show the following. Consider m, d and a linear form G on $[0,1]^{m^2 d^2}$.

1. There is an algorithm which computes an increasing sequence (α_N) such that
$$\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \lim_{N\to\infty} \alpha_N = \sup_{\mathsf{C}_{\mathrm{q}\otimes}} G.$$
2. There is an algorithm which computes a decreasing sequence (β_N) such that
$$\beta_1 \geqslant \beta_2 \geqslant \cdots \geqslant \lim_{N\to\infty} \beta_N = \max_{\mathsf{C}_{\mathrm{qc}}} G.$$

Algorithm = computable function $\{0,1\}^* \to \{0,1\}^*$.

If Tsirelson problem has a positive answer, then for every linear form G

$$\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G = \max_{\mathsf{C}_{\mathrm{qc}}} G.$$

If Tsirelson problem has a positive answer, then for every linear form G

$$\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G = \max_{\mathsf{C}_{\mathrm{qc}}} G.$$

In that case, the algorithms 1. and 2. can be combined into a Turing machine T_0 which, given $\langle G \rangle$ as input, and computes the pair (α_N, β_N) for increasing integers N, until either $\alpha_N > 1/2$ (then it accepts G) or $\beta_N < 1$ (then it rejects G). This machine always halts.

If Tsirelson problem has a positive answer, then for every linear form G

$$\sup_{\mathsf{C}_{\mathrm{q}\otimes}} G = \max_{\mathsf{C}_{\mathrm{qc}}} G.$$

In that case, the algorithms 1. and 2. can be combined into a Turing machine T_0 which, given $\langle G \rangle$ as input, and computes the pair (α_N, β_N) for increasing integers N, until either $\alpha_N > 1/2$ (then it accepts G) or $\beta_N < 1$ (then it rejects G). This machine always halts.

Consider the Turing machine $\mathrm{D} = \mathrm{T}_0 \circ f$, where f is the function from Theorem 12.10 (recall that $f(\langle M \rangle)$ is a game with value $= 1$ or $\leqslant 1/2$ depending whether M halts on the empty word).

The Turing machine D solves the halting problem (on the empty word). This is a contradiction, and therefore the Tsirelon problem has a negative answer.

Algorithm 1: discretization

Fact: if $\mathsf{C}_{\mathrm{q}\otimes,N}$ is the same set as $\mathsf{C}_{\mathrm{q}\otimes}$, but with the restriction that $\dim(\mathcal{H}_1) \leqslant N$ and $\dim(\mathcal{H}_2) \leqslant N$, then

$$\overline{\bigcup_N \mathsf{C}_{\mathrm{q}\otimes,N}} = \overline{\mathsf{C}_{\mathrm{q}\otimes}}.$$

Algorithm 1: discretization

Fact: if $\mathsf{C}_{\mathrm{q}\otimes,N}$ is the same set as $\mathsf{C}_{\mathrm{q}\otimes}$, but with the restriction that $\dim(\mathcal{H}_1) \leqslant N$ and $\dim(\mathcal{H}_2) \leqslant N$, then

$$\overline{\bigcup_N \mathsf{C}_{\mathrm{q}\otimes,N}} = \overline{\mathsf{C}_{\mathrm{q}\otimes}}.$$

A POVM (positive operator-valued measure) is a finite family of positive operators (A_i) summing to Id. Every PVM is a POVM.

Algorithm 1: discretization

Fact: if $\mathsf{C}_{\mathrm{q}\otimes,N}$ is the same set as $\mathsf{C}_{\mathrm{q}\otimes}$, but with the restriction that $\dim(\mathcal{H}_1) \leqslant N$ and $\dim(\mathcal{H}_2) \leqslant N$, then

$$\overline{\bigcup_N \mathsf{C}_{\mathrm{q}\otimes,N}} = \overline{\mathsf{C}_{\mathrm{q}\otimes}}.$$

A POVM (positive operator-valued measure) is a finite family of positive operators (A_i) summing to Id. Every PVM is a POVM.

We can replace PVMs by POVMs in the definition of $\mathsf{C}_{\mathrm{q}\otimes}$. This is because of the Naimark dilation theorem: if $(A_1, \dots, A_n)$ is a POVM on $\mathcal{H}$, then there is an isometry $\iota : \mathcal{H} \to \mathcal{H}'$ and a PVM (P_i) on $\mathcal{H}'$ such that $A_i = \iota^* P_i \iota$.

Algorithm 1: discretization

Fact: if $\mathsf{C}_{\mathrm{q}\otimes,N}$ is the same set as $\mathsf{C}_{\mathrm{q}\otimes}$, but with the restriction that $\dim(\mathcal{H}_1) \leqslant N$ and $\dim(\mathcal{H}_2) \leqslant N$, then

$$\overline{\bigcup_N \mathsf{C}_{\mathrm{q}\otimes,N}} = \overline{\mathsf{C}_{\mathrm{q}\otimes}}.$$

A POVM (positive operator-valued measure) is a finite family of positive operators (A_i) summing to Id. Every PVM is a POVM.

We can replace PVMs by POVMs in the definition of $\mathsf{C}_{\mathrm{q}\otimes}$. This is because of the Naimark dilation theorem: if $(A_1, \dots, A_n)$ is a POVM on $\mathcal{H}$, then there is an isometry $\iota : \mathcal{H} \to \mathcal{H}'$ and a PVM (P_i) on $\mathcal{H}'$ such that $A_i = \iota^* P_i \iota$.

Proof: define $\mathcal{H}' = \oplus_{i=1}^n \mathcal{H}$, $P_i =$ the projection on the ith copy, and

$$\iota(x) = (A_1^{1/2}x, \dots, A_n^{1/2}x), \ \iota^*(x_1, \dots, x_n) = \sum_i A_i^{1/2} x_i.$$

Algorithm 1: discretization

With the definition via POVMs is it easy to prove $\overline{\bigcup \mathrm{C}_{\mathrm{q}\otimes,N}} = \overline{\mathrm{C}_{\mathrm{q}\otimes}}$: take finite-rank projectors Π_1, Π_2 such that $\|(\Pi_1 \otimes \Pi_2)\xi - \xi\| \leqslant \varepsilon$, and replace the POVMs (P_x^a), (Q_y^b) by the POVMs $(\Pi_1 P_x^a \Pi_1)$, $(\Pi_2 Q_y^b \Pi_2)$ on the finite-dimensional Hilbert spaces $\Pi_1(\mathcal{H}_1)$, $\Pi_2(\mathcal{H}_2)$.

Algorithm 1: discretization

With the definition via POVMs is it easy to prove $\overline{\bigcup \mathrm{C}_{\mathrm{q}\otimes,N}} = \overline{\mathrm{C}_{\mathrm{q}\otimes}}$: take finite-rank projectors Π_1, Π_2 such that $\|(\Pi_1 \otimes \Pi_2)\xi - \xi\| \leqslant \varepsilon$, and replace the POVMs (P_x^a), (Q_y^b) by the POVMs $(\Pi_1 P_x^a \Pi_1)$, $(\Pi_2 Q_y^b \Pi_2)$ on the finite-dimensional Hilbert spaces $\Pi_1(\mathcal{H}_1)$, $\Pi_2(\mathcal{H}_2)$.

Algorithm 1 computes a $\frac{1}{N}$-approximation of

$$\sup_{p \in \mathrm{C}_{\mathrm{q}\otimes,N}} G(p).$$

Indeed the unit sphere of $\mathbf{C}^N \otimes \mathbf{C}^N$, and the set

$$\{(P_1, \dots, P_m) \ : \ P_i \geqslant 0, \ \sum P_i = \mathrm{Id}\}$$

are compact, so there admit finite ε-dense subsets. Moreover, such subsets can obtained algorithmically. The algorithm optimizes over these finite subsets.

Algorithm 2: the NPA hierarchy

Consider the alphabet $\mathcal{S} = \{p_x^a\}_{x \in [d], a \in [m]} \cup \{q_y^b\}_{y \in [d], b \in [m]}$. We write $\mathcal{S}_N$ for the set of words of length at most N, and $\mathcal{S}^* = \bigcup \mathcal{S}_N$. The concatenation of the words s and t is denoted $s^\frown t$.

Algorithm 2: the NPA hierarchy

Consider the alphabet $\mathcal{S} = \{p_x^a\}_{x\in[d],a\in[m]} \cup \{q_y^b\}_{y\in[d],b\in[m]}$. We write $\mathcal{S}_N$ for the set of words of length at most N, and $\mathcal{S}^* = \bigcup \mathcal{S}_N$. The concatenation of the words s and t is denoted $s^\frown t$.

Let $p(ab|xy) \in \mathrm{C}_{\mathrm{qc}}$; so there are commuting PVMs (P_x^a), (Q_y^b) and a unit vector ξ. To a word $s \in \mathcal{S}$ corresponds an operator $\pi(s)$ on $\mathcal{H}$, such that $\pi(p_x^a) = P_x^a$, $\pi(q_y^b) = Q_y^b$ and $\pi(s^\frown t) = \pi(s)\pi(t)$.

Algorithm 2: the NPA hierarchy

Consider the alphabet $\mathcal{S} = \{p_x^a\}_{x\in[d],a\in[m]} \cup \{q_y^b\}_{y\in[d],b\in[m]}$. We write $\mathcal{S}_N$ for the set of words of length at most N, and $\mathcal{S}^* = \bigcup \mathcal{S}_N$. The concatenation of the words s and t is denoted $s^\frown t$.

Let $p(ab|xy) \in \mathsf{C}_{\mathrm{qc}}$; so there are commuting PVMs (P_x^a), (Q_y^b) and a unit vector ξ. To a word $s \in \mathcal{S}$ corresponds an operator $\pi(s)$ on $\mathcal{H}$, such that $\pi(p_x^a) = P_x^a$, $\pi(q_y^b) = Q_y^b$ and $\pi(s^\frown t) = \pi(s)\pi(t)$. Set

$$\Gamma_{s,t} = \langle \pi(s)\xi, \pi(t)\xi \rangle = \langle \xi, \pi(s)^*\pi(t)\xi \rangle.$$

Algorithm 2: the NPA hierarchy

Consider the alphabet $\mathcal{S} = \{p_x^a\}_{x\in[d],a\in[m]} \cup \{q_y^b\}_{y\in[d],b\in[m]}$. We write $\mathcal{S}_N$ for the set of words of length at most N, and $\mathcal{S}^* = \bigcup \mathcal{S}_N$. The concatenation of the words s and t is denoted $s^\frown t$.

Let $p(ab|xy) \in \mathrm{C}_{\mathrm{qc}}$; so there are commuting PVMs (P_x^a), (Q_y^b) and a unit vector ξ. To a word $s \in \mathcal{S}$ corresponds an operator $\pi(s)$ on $\mathcal{H}$, such that $\pi(p_x^a) = P_x^a$, $\pi(q_y^b) = Q_y^b$ and $\pi(s^\frown t) = \pi(s)\pi(t)$. Set

$$\Gamma_{s,t} = \langle \pi(s)\xi, \pi(t)\xi \rangle = \langle \xi, \pi(s)^*\pi(t)\xi \rangle.$$

The matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}^*}$ is positive, its entries satisfy some affine relations

- A1 $\Gamma_{p_x^a, q_y^b} = p(ab|xy)$,
- A2 If $g \in \mathcal{S}$ and $s, t \in \mathcal{S}^*$, then $\Gamma_{g^\frown s, g^\frown t} = \Gamma_{g^\frown s, t} = \Gamma_{s, g^\frown t}$,
- A3 If $a \neq a' \in [m]$, $x \in [d]$ and $s, t \in \mathcal{S}^*$, then $\Gamma_{p_x^a {}^\frown s, p_x^{a'} {}^\frown t} = 0$, and same for y, b, b'
- A4 If $x \in [d]$, $s, t \in \mathcal{S}^*$, then $\sum_a \Gamma_{p_x^a {}^\frown s, t} = \Gamma_{s,t}$, same for y [so $\Gamma_{\emptyset,\emptyset} = 1$]
- A5 If $x, y \in [d]$, $a, b \in [m]$ and $s, t \in \mathcal{S}^*$, then $\Gamma_{p_x^a {}^\frown s, q_y^b {}^\frown t} = \Gamma_{q_y^b {}^\frown s, p_y^a {}^\frown t}$.

Consider a correlation matrix $p(ab|xy)$, not necessarily in C_{qc}. A positive matrix $(\Gamma_{s,t})_{s,t \in \mathcal{S}^*}$ which satisfies axioms 1–5 from the previous slide is called a certificate for $p(ab|xy)$.

Consider a correlation matrix $p(ab|xy)$, not necessarily in C_{qc}. A positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}^*}$ which satisfies axioms 1–5 from the previous slide is called a certificate for $p(ab|xy)$.

Theorem 2

$p(ab|xy) \in \mathsf{C}_{\mathrm{qc}}$ *if and only if it admits a certificate.*

Consider a correlation matrix $p(ab|xy)$, not necessarily in C_{qc}. A positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}^*}$ which satisfies axioms 1–5 from the previous slide is called a certificate for $p(ab|xy)$.

Theorem 2

$p(ab|xy) \in \mathrm{C}_{\mathrm{qc}}$ *if and only if it admits a certificate.*

Since Γ is postive, it can be realized as a Gram matrix: there is a Hilbert space $\mathcal{H}$ and vectors $(v(s))_{s\in\mathcal{S}^*}$ in $\mathcal{H}$ such that

$$\Gamma_{s,t} = \langle v(s), v(t)\rangle$$

for every $s, t \in \mathcal{S}^*$. We can assume that $\mathcal{H} = \overline{\mathrm{span}}\{v(s) : s \in \mathcal{S}^*\}$.

Consider a correlation matrix $p(ab|xy)$, not necessarily in C_{qc}. A positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}^*}$ which satisfies axioms 1–5 from the previous slide is called a certificate for $p(ab|xy)$.

Theorem 2

$p(ab|xy) \in \mathrm{C}_{\mathrm{qc}}$ if and only if it admits a certificate.

Since Γ is postive, it can be realized as a Gram matrix: there is a Hilbert space $\mathcal{H}$ and vectors $(v(s))_{s\in\mathcal{S}^*}$ in $\mathcal{H}$ such that

$$\Gamma_{s,t} = \langle v(s), v(t) \rangle$$

for every $s, t \in \mathcal{S}^*$. We can assume that $\mathcal{H} = \overline{\mathrm{span}}\{v(s) : s \in \mathcal{S}^*\}$. We then define

- $\xi = v(\emptyset)$,
- $P_x^a =$ orthogonal projector onto $\overline{\mathrm{span}}\{v(p_x^a \frown s) \ : \ s \in \mathcal{S}^*\}$,
- $Q_y^b =$ orthogonal projector onto $\overline{\mathrm{span}}\{v(q_y^b \frown s) \ : \ s \in \mathcal{S}^*\}$.

- $\xi = v(\emptyset)$,
- P_x^a = orthogonal projector onto $\overline{\text{span}}\{v(p_x^a \frown s) \ : \ s \in \mathcal{S}^*\}$,
- Q_y^b = orthogonal projector onto $\overline{\text{span}}\{v(q_y^b \frown s) \ : \ s \in \mathcal{S}^*\}$.

We have

1. $\|\xi\|^2 = \|v(\emptyset)\|^2 = \langle v(\emptyset), v(\emptyset)\rangle = \Gamma_{\emptyset,\emptyset} = 1$,
2. for every x, y, a, b, we have $p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$,
3. for every x, $(P_x^a)_a$ is a PVM. The fact that $P_x^a P_x^{a'} = 0$ if $a \neq a'$ follows from Axiom 3 and the fact that $\sum_a P_x^a = \mathrm{Id}$ follows from Axiom 4,
4. for every y, $(Q_y^b)_b$ is a PVM. Same as before,
5. for every x, y, a, b, we have $[P_x^a, Q_y^b] = 0$. This follows from Axiom 5.

- $\xi = v(\emptyset)$,
- $P_x^a =$ orthogonal projector onto $\overline{\text{span}}\{v(p_x^a \frown s) \ : \ s \in \mathcal{S}^*\}$,
- $Q_y^b =$ orthogonal projector onto $\overline{\text{span}}\{v(q_y^b \frown s) \ : \ s \in \mathcal{S}^*\}$.

We have

1. $\|\xi\|^2 = \|v(\emptyset)\|^2 = \langle v(\emptyset), v(\emptyset)\rangle = \Gamma_{\emptyset,\emptyset} = 1$,
2. for every x, y, a, b, we have $p(ab|xy) = \langle \xi | P_x^a Q_y^b | \xi \rangle$,
3. for every x, $(P_x^a)_a$ is a PVM. The fact that $P_x^a P_x^{a'} = 0$ if $a \neq a'$ follows from Axiom 3 and the fact that $\sum_a P_x^a = \mathrm{Id}$ follows from Axiom 4,
4. for every y, $(Q_y^b)_b$ is a PVM. Same as before,
5. for every x, y, a, b, we have $[P_x^a, Q_y^b] = 0$. This follows from Axiom 5.

Question for C^*-algebraists: is this the GNS construction?

A compactness lemma

Say that a positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}_N}$ is a N-certificate for $p(ab|xy)$ if it satifies axioms A1-A5 but only for words with length at most N.

A compactness lemma

Say that a positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}_N}$ is a N-certificate for $p(ab|xy)$ if it satifies axioms A1-A5 but only for words with length at most N.

Lemma 3

A correlation matrix admits a certificate iff it admits a N-certificate for every N.

A compactness lemma

Say that a positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}_N}$ is a N-certificate for $p(ab|xy)$ if it satifies axioms A1-A5 but only for words with length at most N.

Lemma 3

A correlation matrix admits a certificate iff it admits a N-certificate for every N.

We claim that $|\Gamma^N_{s,t}| \leqslant 1$, and then for some subsequence $\lim_{N\to\infty} \Gamma^N_{s,t}$ exists for every s, t (diagonal extraction) and also satifies axioms A1–A5.

A compactness lemma

Say that a positive matrix $(\Gamma_{s,t})_{s,t \in \mathcal{S}_N}$ is a N-certificate for $p(ab|xy)$ if it satifies axioms A1-A5 but only for words with length at most N.

Lemma 3

A correlation matrix admits a certificate iff it admits a N-certificate for every N.

We claim that $|\Gamma^N_{s,t}| \leqslant 1$, and then for some subsequence $\lim_{N \to \infty} \Gamma^N_{s,t}$ exists for every s, t (diagonal extraction) and also satifies axioms A1–A5.

Since Γ^N is positive, it satisfies $|\Gamma^N_{s,t}| \leqslant |\Gamma^N_{s,s}|^{1/2} |\Gamma^N_{t,t}|^{1/2}$.

A compactness lemma

Say that a positive matrix $(\Gamma_{s,t})_{s,t\in\mathcal{S}_N}$ is a N-certificate for $p(ab|xy)$ if it satifies axioms A1-A5 but only for words with length at most N.

Lemma 3

A correlation matrix admits a certificate iff it admits a N-certificate for every N.

We claim that $|\Gamma^N_{s,t}| \leqslant 1$, and then for some subsequence $\lim_{N\to\infty}\Gamma^N_{s,t}$ exists for every s,t (diagonal extraction) and also satifies axioms A1–A5.

Since Γ^N is positive, it satisfies $|\Gamma^N_{s,t}| \leqslant |\Gamma^N_{s,s}|^{1/2}|\Gamma^N_{t,t}|^{1/2}$.
We prove $\Gamma^N_{s,s} \leqslant 1$ by induction on the length of s. For every $g\in\mathcal{S}$, we have $\Gamma^N_{g^\frown s,g^\frown s} = \Gamma^N_{g^\frown s,s} = \Gamma^N_{s,g^\frown s}$. Since the matrix $\begin{pmatrix} \Gamma^N_{s,s} & \Gamma^N_{s,g^\frown s} \\ \Gamma^N_{g^\frown s,s} & \Gamma^N_{g^\frown s,g^\frown s}\end{pmatrix}$ is positive, we have $\Gamma^N_{g^\frown s,g^\frown s} \leqslant \Gamma^N_{s,s}$.

Let $\mathsf{C}_{\mathrm{qc},N}$ be the set of correlation matrices which admit a N-certificate. We have proved that

$$\bigcap_{N \geqslant 1} \mathsf{C}_{\mathrm{qc},N} = \mathsf{C}_{\mathrm{qc}}.$$

This shows that C_{qc} is closed.

Let $\mathsf{C}_{\mathrm{qc},N}$ be the set of correlation matrices which admit a N-certificate. We have proved that

$$\bigcap_{N \geqslant 1} \mathsf{C}_{\mathrm{qc},N} = \mathsf{C}_{\mathrm{qc}}.$$

This shows that C_{qc} is closed.

Let $M = \mathrm{card}(\mathcal{S}_N)$. The set of N-certificates is the intersection of the cone PSD_M of $M \times M$ positive matrices with an affine subspace (given by the axioms A2–A5).

Let $\mathsf{C}_{\mathrm{qc},N}$ be the set of correlation matrices which admit a N-certificate. We have proved that

$$\bigcap_{N \geqslant 1} \mathsf{C}_{\mathrm{qc},N} = \mathsf{C}_{\mathrm{qc}}.$$

This shows that C_{qc} is closed.

Let $M = \mathrm{card}(\mathcal{S}_N)$. The set of N-certificates is the intersection of the cone PSD_M of $M \times M$ positive matrices with an affine subspace (given by the axioms A2–A5).

Fix a game G. The value $\beta_N^{opt} = \max_{\mathsf{C}_{\mathrm{qc},N}} G$ can be computed up to error ε in time $\mathrm{poly}(M, \log(1/\varepsilon))$ by semi-definite programming, so β_N^{opt} is a decreasing sequence which converges to $\max_{\mathsf{C}_{\mathrm{qc}}} G$.

Let $\mathsf{C}_{\mathrm{qc},N}$ be the set of correlation matrices which admit a N-certificate. We have proved that

$$\bigcap_{N \geqslant 1} \mathsf{C}_{\mathrm{qc},N} = \mathsf{C}_{\mathrm{qc}}.$$

This shows that C_{qc} is closed.

Let $M = \mathrm{card}(\mathcal{S}_N)$. The set of N-certificates is the intersection of the cone PSD_M of $M \times M$ positive matrices with an affine subspace (given by the axioms A2–A5).

Fix a game G. The value $\beta_N^{opt} = \max_{\mathsf{C}_{\mathrm{qc},N}} G$ can be computed up to error ε in time $\mathrm{poly}(M, \log(1/\varepsilon))$ by semi-definite programming, so β_N^{opt} is a decreasing sequence which converges to $\max_{\mathsf{C}_{\mathrm{qc}}} G$.

In a more elementary way: we can compute β_N, a $\frac{1}{N}$-approximation to β_N^{opt} by a discretization argument. For example, replace PSD_M by the cone of self-adjoint operators A which satisfy $\langle x|A|x\rangle \geqslant 0$ for every x in a finite ε-dense subset of the unit sphere.