Mathematical Aspects of Quantum Information Theory:

Lecture 2

Dario Trevisan

Università di Pisa
dario.trevisan@unipi.it

Plan

1. Postulates of Quantum Mechanics (conclusion)
   - C^*-algebras approach
2. Quantum Channels
   - Tensor products
   - Markov kernels
   - Kraus representation
   - Complete positivity
   - CP maps on C^*-algebras
   - Quantum Markov semigroups
   - Exercises

Plan

Infinite dimensional systems

The definitions (states, measurements and observables) are mathematically elementary for we are restricted to finite dimensional quantum systems H. (Heisenberg and) Schrödinger instead considered:

- the quantum system of a single particle on a line is $H = L^2(\mathbb{R}, dx)$,
- state vectors are wave functions $|\psi\rangle = (\psi(x))_{x\in\mathbb{R}}$
- the fundamental observables are the pair position Q and momentum P:

$$(Q\psi)(x) = x\psi(x), \quad (P\psi)(x) = -i\frac{d\psi}{dx}(x).$$

- The crucial property they satisfy is the *canonical commutation relation* (CCR):
- But these operators are not well-defined for every $\psi \in L^2(\mathbb{R}, dx)$! hence the need of more general spectral theorems.

A different route: observables first!

- One can instead search first for a family of bounded operators containing all the useful information about P and Q and argue then by duality to obtain the states of the quantum system.
- The classical analogy is that probability distributions (states) can be defined via Riesz theorem, as certain linear functionals over continuous functions on a compact topological space (observables).
- It turns out that the correct structure of such an abstract family is that of a C^*-algebra $\mathcal{A}$.

General definition

A C^*-algebra $\mathcal{A}$ is defined as follows:

- $\mathcal{A}$ is a complex Banach space,
- with an additional product operation $(a, b) \mapsto ab$ that yields a structure of Banach algebra, i.e., it is
  - associative,
  - distributive with respect to the addition operation,
  - there exists an identity element $\mathbb{1}$
  - the norm satisfies $\|ab\| \leq \|a\| \, \|b\|$ for every $a, b \in \mathcal{A}$
- and with an additional anti-linear map $* : \mathcal{A} \to \mathcal{A}$, $a \mapsto a^*$, that is
  - an involution $(a^*)^* = a$
  - satisfying $(ab)^* = b^* a^*$, for $a, b \in \mathcal{A}$
  - and the C^*-identity holds:

Remarks

- If $\mathcal{A}$ is a Banach algebra and $*$ is an enjoys all the properties but the C^*-identity, it is enough to prove that

$$\|a^* a\| \geq \|a\|^2 .$$

- A $*$-homomorphism between C^*-algebras $\mathcal{A}$, $\mathcal{B}$ is a map $\pi : a \mapsto \pi(a)$ which is well-behaved with respect to all the operations, i.e. it is a ring homomorphism and $\pi(a^*) = \pi(a)^*$.
- Two C^*-algebras as isomorphic if there exists an invertible $*$-homomorphism between them.

Examples

1. $\mathcal{A} = C(K;\mathbb{C})$ (with K compact Hausdorff) is a C^*-algebra:

2. The space of $d \times d$ complex matrices $\mathcal{A} = \mathbb{C}^{d\times d}$, endowed with the natural matrix sum and product operations, the matrix norm

$$\|A\|^2 = \sup_{v\in\mathbb{C}^d\setminus\{0\}} \frac{\|Av\|^2}{\|v\|^2} = \sup_{v\in\mathbb{C}^d\setminus\{0\}} \frac{\langle v|A^*Av\rangle}{\langle v|v\rangle}$$

   and A^* being the conjugate transpose of A, is a C^*-algebra.

3. The space of linear bounded operators $\mathcal{A} = \mathcal{B}(H)$ on a complex Hilbert space H endowed with the operator norm and the adjoint $A \mapsto A^*$ is also a C^*-algebra.

Further definitions

We say that $a \in \mathcal{A}$ is

- self-adjoint if $a = a^*$,
- positive if there exists $b \in \mathcal{A}$ such that $a = b^* b$,
- unitary if $aa^* = a^* a = \mathbb{1}$.

The spectrum of a is $\lambda \in \mathbb{C}$ such that $a - \lambda \mathbb{1}$ is not invertible (w.r.t. the product operation).

- Self-adjoint $a \in \mathcal{A}$ such that $\sigma(a) \subseteq [0, \infty)$ coincide with positive elements, i.e., one can represent $a = b^* b$ for some $b \in \mathcal{A}$ (this is not trivial to prove).

The C^*-algebra axiomatization of quantum mechanics

We reverse the order from the elementary approach:

1. observables for a quantum system are the self-adjoint elements in a C^*-algebra $\mathcal{A}$
2. states are then defined as continuous linear functionals

$$\eta : \mathcal{A} \mapsto \mathbb{C}$$

   that are
   - positive, i.e. $\eta(a) \geq 0$ for every positive $a = b^* b$
   - and $\eta(\mathbb{1}) = 1$.

- Elementary quantum systems H are recovered: let $\mathcal{A} = \mathcal{L}(H)$ and

$$\eta(A) = \mathrm{tr}[A\rho], \quad \text{for a density operator } \rho \in \mathcal{S}(H).$$

- Any C^*-algebra is isomorphic to a sub-algebra of $\mathcal{B}(H)$ for some Hilbert space (Gelfand-Naimark-Segal construction).

The Weyl algebra

How to describe the CCR with a suitable C^*-algebra?

- instead of unbounded Q and P, we introduce the *Weyl operators* $(W(r,s))_{(r,s)\in\mathbb{R}^2}$ formally given by

$$W(r,s) = e^{i(sQ-rP)}.$$

- A rigorous definition as bounded operator on $H = L^2(\mathbb{R}, dx)$ is

$$W(r,s)\psi(x) = e^{is(x-r/2)}\psi(x-r).$$

- The Weyl algebra is the C^*-algebra generated by the Weyl operators (as a closed sub-algebra of $\mathcal{B}(L^2(\mathbb{R}, dx))$).
- From the definition:

$$W(r,s)^* = W(-r,-s)$$

and

$$W(r_1,s_1)W(r_2,s_2) = e^{-i(r_1 s_2 - r_2 s_1)/2} W(r_1+r_2, s_1+s_2),$$

which encodes the CCR.

Characteristic function of a state

The Weyl algebra has a rich structure and its study would require an entire course on its own.

- Given a state η on the Weyl algebra, its characteristic function is

$$\mathbb{R}^2 \ni (r, s) \mapsto \eta(W(r, s)) \in \mathbb{C}.$$

- A state η is a quantum (bosonic) Gaussian state if its characteristic function is the exponential of a quadratic polynomial in the variables r, s (with complex coefficients).

Any $|\psi\rangle \in L^2(\mathbb{R}; dx)$ with unit norm induces a state on the Weyl algebra via

$$\eta(W(r, s)) = \int_{\mathbb{R}} \bar{\psi}(x) W(r, s) \psi(x) dx.$$

Question: for which $|\psi\rangle$ the induced state is Gaussian?

Exercises

Exercise(CCR cannot be realized by bounded operators)

Prove that one cannot define two operators $Q, P \in \mathcal{L}(H)$ satisfying the CCR on a finite dimensional Hilbert space H,

or ever as bounded operators, $Q, P \in \mathcal{B}(H)$ on a general Hilbert space H.

(Hint: compute $[Q, P^n]$ and consider its operator norm as $n \to \infty$)

Plan

- Consider finite dimensional Hilbert spaces H, K.
- Write $\mathcal{L}(H; K)$ for the space of linear operators $A : H \to K$.
- The adjoint operator $A^* : K \to H$ is defined by requiring

$$\langle \varphi | A^* \psi \rangle = \langle A\varphi | \psi \rangle \,, \quad \text{for every } |\psi\rangle \in K, \varphi \in H.$$

- Write $\mathcal{L}(H) = \mathcal{L}(H; H)$ endowed with the Hilbert-Schmidt scalar product

$$\langle A | B \rangle = \mathrm{tr}[A^* B], \quad \text{for } |A\rangle \,, |B\rangle \in \mathcal{L}(H).$$

- An isometry $U : H \to K$ is a linear map preserving the norms (or equivalently the scalar products)

$$\langle U\varphi | U\psi \rangle = \langle \varphi | \psi \rangle \,, \quad \text{for every } |\varphi\rangle \,, |\psi\rangle \in H,$$

or equivalently, such that $U^* U = \mathbb{1}_H$.

Tensor product

- $H \otimes K$: linear space generated by elementary tensors $|\varphi\rangle \otimes |\psi\rangle$ quotiented so that the expressions become bi-linear, e.g.,
- Dirac's notation: $|\varphi\rangle \otimes |\psi\rangle = |\varphi, \psi\rangle$.
- Scalar product:

$$\langle \varphi_0 \otimes \psi_0 | \varphi_0 \otimes \psi_0 \rangle = \langle \varphi_0 | \varphi_1 \rangle \langle \psi_0 | \psi_1 \rangle .$$

- $\dim(H \otimes K) = \dim(H)\dim(K)$ with orthonormal basis is given by

$$(|i, j\rangle)_{i \in I, j \in J} = (|i\rangle \otimes |j\rangle)_{i \in I, j \in J}$$

for orthonormal bases $(|i\rangle)_{i \in I} \subseteq H$, $(|j\rangle)_{j \in J} \subseteq K$.

Composite systems

- Tensor products are used in quantum mechanics to represent composite systems made by “joining” two quantum systems H, K.
- States on the composite system $H \otimes K$ are represented by density operators $\rho \in \mathcal{S}(H \otimes K)$,
- Observables are self-adjoint operators $A \in \mathcal{O}(H \otimes K)$.
- Let us recall some basic facts on operators $M \in \mathcal{L}(H \otimes K)$, and in particular the partial trace operation.

Tensor product of operators

- The tensor product extends to operators: for $A \in \mathcal{L}(H; \tilde{H})$, $B \in \mathcal{L}(K; \tilde{K})$, the operator $A \otimes B \in \mathcal{L}(H \otimes H; \tilde{H} \otimes \tilde{K})$ is defined as

$$(A \otimes B) |\varphi\rangle \otimes |\psi\rangle = |A\varphi\rangle \otimes |B\psi\rangle$$

- One has $(A \otimes B)^* = A^* \otimes B^*$, hence $A \otimes B \in \mathcal{O}(H \otimes K)$ if $A \in \mathcal{O}(H)$ and $B \in \mathcal{O}(K)$.
- $\sigma(A \otimes B) = \sigma(A) \cdot \sigma(B)$ (all possible pairwise products).
- $A \otimes B \geq 0$ is positive if both $A \geq 0$ and $B \geq 0$

Block matrix representation

- Choosing orthonormal bases $(|i\rangle)_{i\in I} \subseteq H$, $(|j\rangle)_{j\in J} \subseteq K$ yields the representation of any $M \in \mathcal{L}(H \otimes K)$:

$$M = \sum_{i,j,k,\ell} M_{ij,k\ell} \, |i,j\rangle \, \langle k,\ell| \,, \tag{1}$$

  with $M_{ij,k\ell} = \langle i \otimes j | M(k \otimes \ell)\rangle$.
- For fixed j and $\ell \in J$, set

$$M_{j,\ell} = \sum_{i,k} M_{ij,k\ell} \, |i\rangle \, \langle k| \in \mathcal{L}(H).$$

- M is identified with the block matrix

$$M = \left(M_{j,\ell}\right)_{j,\ell \in J}.$$

- If $K = \mathbb{C}^d$, such block matrix representation is always understood with respect to the computational basis, e.g. $M \in \mathcal{L}(H \otimes \mathbb{C}^2)$ is represented as

$$M = \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix}.$$

Partial trace

- On $\mathcal{L}(H \otimes K)$, the partial trace over H is the only operator

$$\mathrm{tr}_H : \mathcal{L}(H \otimes K) \to \mathcal{L}(K), \quad M \mapsto \mathrm{tr}_H[M]$$

  such that, for every $A \in \mathcal{L}(K)$, one has

$$\mathrm{tr}[A^* \mathrm{tr}_H[M]] = \mathrm{tr}[(\mathbb{1}_H \otimes A^*)M].$$

- tr_H is the adjoint of the partial tensor product operation $A \mapsto \mathbb{1}_H \otimes A$:

- By representing M a block matrix one has the formulas

- If $M \in \mathcal{O}(H \otimes K)$ so is $\mathrm{tr}_H[M] \in \mathcal{O}(K)$
- If $M = \rho \in \mathcal{S}(H \otimes K)$, then $\mathrm{tr}_H[\rho] \in \mathcal{S}(K)$, the reduced density operator.
- Similarly, one defines $\mathrm{tr}_K[M]$.

Separable and entangled states

- We say that $\rho \in \mathcal{S}(H \otimes K)$ is separable if it can be represented as a convex combination
$$\rho = \sum_{x \in \mathcal{X}} p_x \rho_x \otimes \sigma_x,$$
with $\rho_x \in \mathcal{S}(H)$, $\sigma_x \in \mathcal{S}(K)$ and $(p_x)_{x \in \mathcal{X}}$ a classical probability distribution over a finite set $\mathcal{X}$.

- States $\rho \in \mathcal{S}(H \otimes K)$ that are not separable are called entangled. Entangled states have no classical analogues (any classical joint probability distribution is "separable"). Example (Bell state):

Plan

- A Markov kernel from Ω to $\mathcal{X}$ (finite sets) is $N = (N(\omega, \cdot))_{\omega \in \Omega}$ such that

$$N(\omega, x) \in [0,1] \quad \text{for all } x \in \mathcal{X}, \text{ and} \quad \sum_{x \in \mathcal{X}} N(\omega, x) = 1.$$

- Two natural operations associated to a kernel N:
  1. given $f : \mathcal{X} \to \mathbb{C}$:
  $$N(f)(\omega) = \sum_{x \in \mathcal{X}} f(x) N(\omega, x),$$
  2. given $p : \Omega \to \mathbb{C}$:
  $$N^{\dagger}(p)(x) = \sum_{\omega} p(\omega) N(\omega, x).$$

  Both operations are linear and dual to each other.
- Both N and $N^{\dagger}$ are positive, i.e. and

$$N(1_{\Omega}) = 1_{\mathcal{X}}, \quad \sum_{x \in \mathcal{X}} N^{\dagger}(p)(x) = \sum_{\omega \in \Omega} p(\omega).$$

- $N^{\dagger}$ maps probability distributions on Ω to probability distributions on $\mathcal{X}$.

Plan

1. Postulates of Quantum Mechanics (conclusion)
   - C^*-algebras approach
2. Quantum Channels
   - Tensor products
   - Markov kernels
   - Kraus representation
   - Complete positivity
   - CP maps on C^*-algebras
   - Quantum Markov semigroups
   - Exercises

Non-sharp measurements

How build an analogue of N on a quantum system H?

First strategy:

- replace each $N(\cdot, x)$ with an observable $N_x \in \mathcal{O}(H)$ such that

$$0 \leq N_x \leq \mathbb{1}_H \quad \text{and} \sum_{x \in \mathcal{X}} N_x = \mathbb{1}_H.$$

- These are (elementary) positive operator valued measure (POVM).
- We are relaxing the sharp indicator observables $\mathbb{1}_{V_x}$ associated to a measurement $X = (\mathbb{1}_{V_x})_{x \in \mathcal{X}}$ with the operators $X = (N_x)_{x \in \mathcal{X}}$.
- How to transform $\rho \in \mathcal{S}(H)$?

$$\rho \mapsto \sum_{x \in \mathcal{X}} \sqrt{N_x} \rho \sqrt{N_x}.$$

Unitary evolutions

What about kernels N between two different systems H, K?

Second strategy:

- An isometry $U : H \to K$ "embeds" the state vector $|\psi\rangle$ on H into $U|\psi\rangle$ on K. On density operators:

$$\rho \in \mathcal{S}(H) \mapsto U\rho U^* \in \mathcal{S}(K).$$

- When $H = K$, this actually describes the evolution of closed quantum system (postulate). All the other transformations are evolutions of open quantum systems.

- Example: convex combinations over a family of isometries $(U_x)_{x\in\mathcal{X}}$ allows to define

$$\rho \mapsto \sum_{x\in\mathcal{X}} p_x U_x \rho U_x^*.$$

Kraus representation

- We consider transformations $\Phi : \mathcal{L}(H) \to \mathcal{L}(K)$ of the type

$$\Phi(A) = \sum_{x \in \mathcal{X}} B_x^* A B_x,$$

  where $(B_x)_{x \in \mathcal{X}} \subseteq \mathcal{L}(K; H)$ is a family of Kraus (or noise) operators.
- The dual $\Phi^\dagger : \mathcal{L}(K) \to \mathcal{L}(H)$ is represented by the family of adjoints:
- Φ (and $\Phi^\dagger$) is positive, i.e.,
- Φ is unital, $\Phi(\mathbb{1}_H) = \mathbb{1}_K$ if and only if
- Φ is unital if and only if $\Phi^\dagger$ is trace-preserving, $\mathrm{tr}[\Phi^\dagger(A)] = \mathrm{tr}[A]$.

Examples

1. Consider $\Phi : \mathcal{L}(\mathbb{C})(= \mathbb{C}) \to \mathcal{L}(H)$ given by

$$\Phi(\lambda) = \lambda \mathbb{1}_H.$$

Clearly, it is positive and unital. we can write

for a given orthonormal basis $(|x\rangle)_{x \in \mathcal{X}}$.

2. The dual map $\Phi^\dagger : \mathcal{L}(H) \to \mathcal{L}(\mathbb{C})$ is then represented as

which is the trace map.

Maps Φ represented by Kraus operators are stable

- with respect to linear combinations (with positive coefficient)
- with respect to composition.

Lemma

Let H, K be finite dimensional Hilbert spaces and let

$$\Phi : \mathcal{L}(K) \to \mathcal{L}(H)$$

be a $*$-homomorphism, i.e., Φ is linear and

$$\Phi(\mathbb{1}_K) = \mathbb{1}_H, \quad \Phi(AB) = \Phi(A)\Phi(B), \quad \Phi(A^*) = \Phi(A)^*.$$

Then, there exist Kraus operators $(B_x)_{x \in \mathcal{X}} \subseteq \mathcal{L}(H; K)$ representing Φ. One has in particular $|\mathcal{X}| = \mathrm{dim}(H)/\mathrm{dim}(K)$.

Sketch of proof

Plan

Question: is any linear and positive map $\Phi : \mathcal{L}(H) \to \mathcal{L}(K)$ represented by a suitable family of Kraus operators?

- This is not the case in general.
- $\Phi : \mathcal{L}(H) \to \mathcal{L}(K)$ is completely positive (CP) if, for every $d \in \mathbb{N}$,

$$\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^d)} : \mathcal{L}(H \otimes \mathbb{C}^d) \to \mathcal{L}(K \otimes \mathbb{C}^d) \tag{2}$$

  is positive.

- By representing $M \in \mathcal{L}(H \otimes \mathbb{C}^d)$ as block operator

$$M = (M_{ij})_{i,j=1}^d \subseteq \mathcal{L}(H),$$

  we have that

$$\Phi \otimes \mathbb{1}_{\mathbb{C}^d}(M) = (\Phi(M_{ij}))_{i,j=1}^d \subseteq \mathcal{L}(K).$$

  CP means:

$$M = (M_{ij})_{i,j=1}^d \geq 0 \Rightarrow (\Phi(M_{ij}))_{i,j=1}^d.$$

- Writing $M = A^* A$, with

$$A = \sum_{i,j=1}^{d} A_{ij} \otimes |i\rangle \langle j| \,, \quad A^* = \sum_{i,j=1}^{d} A^*_{ji} \otimes |i\rangle \langle j| \,,$$

CP means:

$$\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^d)}(A^* A) = \sum_{i,j=1}^{d} \sum_{k=0}^{d-1} \Phi(A^*_{ki} A_{kj}) \, |i\rangle \langle j| \geq 0.$$

- We specialize to “rank-one” block operators $A = \sum_{j=1}^{d} A_j \otimes |1\rangle \langle j|$, so that

$$\sum_{i,j=1}^{d} \Phi(A^*_i A_j) \, |i\rangle \langle j| \geq 0.$$

i.e., for every $|\psi_i\rangle_{i=1}^{d} \subseteq K$, testing with $v = \sum_{i=1}^{d} |\psi_i\rangle \otimes |i\rangle$,

$$\langle v | M v \rangle = \sum_{i,j=1}^{d} \langle \psi_i | \Phi(A^*_i A_j) \psi_j \rangle \geq 0$$

Some elementary facts about CP maps:

1. Any $\Phi_B(A) = B^* AB$ with $B \in \mathcal{L}(K; H)$ is CP, since

$$\Phi_B \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^d)} = \Phi_{B\otimes \mathbb{1}_{\mathbb{C}^d}}.$$

2. linear combinations with positive coefficients of CP maps are CP
3. the dual of a CP map is also CP, since $\Phi^\dagger \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^d)} = \left(\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^d)}\right)^\dagger$,
4. composition of CP maps is also CP.

Consequences:

- any Φ represented via Kraus operators in CP
- The trace map is CP, hence the partial trace

$$\operatorname{tr}_{H_1} = \operatorname{tr} \otimes \mathbb{1}_{\mathcal{L}(H_2)} : \mathcal{L}(H_1 \otimes H_2) \to \mathcal{L}(H_2).$$

  as well as the dual "partial tensoring" map

$$A \in \mathcal{L}(H_1) \mapsto A \otimes \mathbb{1}_{H_2} \in \mathcal{L}(H_1 \otimes H_2).$$

Quantum channels

A completely positive, trace preserving (CPTP) map $\Phi : \mathcal{L}(H) \to \mathcal{L}(K)$ is also called a quantum channel from the system H to K.

Theorem (Kraus representation of quantum channels)

Let H, K be finite dimensional quantum systems. Any quantum channel $\Phi^\dagger$ from H to K can be represented via a family of Kraus operators:

$$\Phi^\dagger(A) = \sum_{x \in \mathcal{X}} B_x A B_x^* \quad \text{for every } A \in \mathcal{L}(H).$$

One has $|\mathcal{X}| \leq \mathrm{dim}(H)\mathrm{dim}(K)$.

Strategy: factorize the dual map $\Phi : \mathcal{L}(K) \to \mathcal{L}(H)$ via an auxiliary system $\tilde{H}$:

$$\Phi(A) = U^* \pi(A) U,$$

where U is an isometry and π is a $*$-homomorphism.

Proof (sketch)

Stinespring representation

Up to isomorphism, one can let

1. $\tilde{H} = K \otimes \mathbb{C}^{\mathcal{X}}$,
2. $\pi(A) = A \otimes \mathbb{1}_{\mathbb{C}^{\mathcal{X}}}$,
3. $U |\psi\rangle = |\psi\rangle \otimes |0\rangle$.

This yields the Stinespring representation of the quantum channel:

$$\Phi^{\dagger}(\rho) = \mathrm{tr}_{\mathbb{C}^{\mathcal{X}}}[V (\rho \otimes |0\rangle \langle 0|) V^{*}],$$

where $V : K \otimes \mathbb{C}^{\mathcal{X}} \to K \otimes \mathbb{C}^{\mathcal{X}}$ is unitary.

Plan

Complete positivity on C^*-algebra

- A linear map $\Phi : \mathcal{A} \to \mathcal{B}$ between C^*-algebras is CP if

$$\sum_{i,j=1}^{d} b_i^* \Phi(a_i^* a_j) b_j$$

  is positive for every $(a_i)_{i=1}^d \subseteq \mathcal{A}$, $(b_i)_{i=1}^d \subseteq \mathcal{B}$, $d \geq 1$.

- It coincides with the previous notion when $\mathcal{A} = \mathcal{L}(H)$, $\mathcal{B} = \mathcal{L}(K)$.

- Φ is unital if $\Phi(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$.

- A state $\eta : \mathcal{A} \to \mathbb{C}$ defines a CP unital map:

Repeating the proof of the Kraus representation theorem (with some technicalities because of infinite dimensions!) yields the following:

Theorem (Stinespring dilation)

Let $\mathcal{A}$ be a C^*-algebra and H be a Hilbert space. Given any CP unital map $\Phi : \mathcal{A} \to \mathcal{B}(H)$, there exist

1. *a Hilbert space $\tilde{H}$,*
2. *an isometry $U : H \to \tilde{H}$,*
3. *a $*$-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(\tilde{H})$,*

such that, for every $a \in \mathcal{A}$,

$$\Phi(a) = U^* \pi(a) U,$$

and

$$\{\pi(a)U\psi \, : \, a \in \mathcal{A}, \psi \in H\} \subseteq \tilde{H} \quad \text{is dense.}$$

Such a triple $(\tilde{H}, U, \pi)$ is unique up to isomorphisms.

The GNS construction

When applied to $\Phi(a) = \eta(a)$ for a state $\eta : \mathcal{A} \to \mathbb{C}$ it yields the following

Theorem (Gelfand-Naimark-Segal)

Let $\mathcal{A}$ be a C^*-algebra and let $\eta : \mathcal{A} \to \mathbb{C}$ be a state. Then, there exists

1. *a Hilbert space H,*
2. *a unit norm vector $|\psi\rangle \in H$,*
3. *and a $*$-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(H)$*

such that, for every $a \in \mathcal{A}$,

$$\eta(a) = \langle \psi | \pi(a) \psi \rangle ,$$

and $\{\pi(a) |\psi\rangle\}_{a \in \mathcal{A}} \subseteq H$ is dense.
Such a triple is unique up to isomorphisms.

Plan

- By composing a quantum channel Φ from H into itself, one obtains the analogue of a Markov chain evolution

$$\rho_0, \Phi(\rho_0), \Phi^2(\rho), \Phi^3(\rho), \ldots.$$

- For $\Phi(\rho) = U\rho U^*$ with U unitary, it is the analogue of a discrete-time dynamical system.

- Continuous-time dynamics are described by quantum Markov semigroups $(\Phi^t)_{t\geq 0}$:
  1. for every $t \geq 0$, Φ^t is a quantum channel from H into itself,
  2. (semigroup law) for every $s, t \geq 0$, $\Phi^t\Phi^s = \Phi^{s+t}$,
  3. (strong continuity) for every $A \in \mathcal{L}(H)$, $t \mapsto \Phi^t(A)$ is continuous.
- The generator L is defined as:

- If H is finite-dimensional, L is a bounded operator with an explicit representation (the Lindblad form).
- Stone's theorem describes the generators of semigroups induced by unitary maps:

$$L(A) = -i[H, A]$$

for a suitable Hamiltonian H (self-adjoint but possibly unbounded).

Plan

Bell states

The simplest example of *entangled* states is provided by so-called Bell states in a two-qubit composite system $H = \mathbb{C}^2 \otimes \mathbb{C}^2$, defined as follows:

$$\left|\Phi^+\right\rangle = \left(|0,0\rangle + |1,1\rangle\right)/\sqrt{2}, \quad \left|\Phi^-\right\rangle = \left(|0,0\rangle + |1,1\rangle\right)/\sqrt{2},$$

$$\left|\Psi^+\right\rangle = \left(|0,1\rangle + |1,0\rangle\right)/\sqrt{2}, \quad \left|\Psi^-\right\rangle = \left(|0,1\rangle - |1,0\rangle\right)/\sqrt{2}.$$

1. Show that the four state vectors provide an orthonormal basis for the system.
2. Show that each of the four pure states corresponding to the Bell vectors is not separable, hence entangled.

Tensor product of Pauli operators

Consider the Pauli operators σ_x, σ_y on a single-qubit system $\mathbb{C}^2$.

1. Find the matrix representation (with respect to the computational basis in $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$) of the operators

$$A = \sigma_x \otimes \sigma_y, \quad \text{and} \quad B = \sigma_y \otimes \sigma_x.$$

2. Prove that A, B are self-adjoint operators and compute their spectra.
3. Compute $[A, B]$.
4. Assume that the system is prepared in the Bell state $|\Phi^+\rangle$. What is the probability of observing 1 if we measure A?

Partial transpose

Given finite-dimensional quantum systems H, K and an operator $A \in \mathcal{L}(H;K)$ define its *transpose* operator as $A^\tau : \mathcal{L}(K^*) \to \mathcal{L}(H^*)$ as

$$\tau(A) : \langle \varphi| \mapsto \tau(A)(\langle \varphi|) := \langle \varphi| A,$$

i.e., $\tau(A)(\langle \varphi|) = \langle \varphi| A$ is the linear functional on H given by

$$\langle \varphi| A : |\psi\rangle \mapsto \langle \varphi | A\psi \rangle .$$

1. Fix orthonormal bases $(|i\rangle)_{i\in I} \subseteq K$ and $(|j\rangle)_{j\in J} \subseteq H$. Write the associated matrix representation
$$A = (A_{ij})_{i\in I, j\in J} = (\langle i | Aj\rangle)_{i \in I, j\in J}$$
and compare it with the matrix representation of A^τ with respect to the bases $(\langle i|)_{i\in I} \subseteq K^*$, $(\langle j|)_{j\in J} \subseteq H$.
2. Prove that $A \mapsto \tau(A)$ is linear, and if $A \in \mathcal{O}(H)$ is an observable, then $A^\tau \in \mathcal{O}(H^*)$, and moreover if $A \geq 0$ then $\tau(A) \geq 0$ (i.e., the map τ is positive).
3. Show that already if $H = K = \mathbb{C}^2$, then τ is not completely positive (the *partial transpose* $\tau \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^2)}$ is not a positive map).

PPT criterion

Let H, K be finite dimensonal quantum systems. Denoting by $\tau : \mathcal{L}(H) \to \mathcal{L}(H^*)$ the transpose map (defined in the previous exercise), prove that

- if $\rho \in \mathcal{S}(H \otimes K)$ is separable, then its partial transpose $\tau \otimes \mathbb{1}_{\mathcal{L}(K)}$ is a density operator (in particular, it is positive).
- This motivates the so-called *positive partial trace* (PPT) sufficient criterion for entanglement: a state $\rho \in \mathcal{S}(H \otimes K)$ is entangled if its partial transpose $\tau \otimes \mathbb{1}_{\mathcal{L}(K)}(\rho)$ is not positive.
- Do Bell states satisfy the PPT criterion?