SUMMARY of basics of QUANTUM INFORMATION THEORY. 2023-2024

Anna Sanpera Trigueros

October 23, 2023

Abstract

Summary of the first part of course of Quantum Information (master on Quantum Science and Technologies, 2023-2024)

The QM formalism consist on

- A mathematical body (C*)-algebras. It is good to think of algebras as "matrices".
- A list of rules (the postulates) which gives the basis on how the formalism has to be applied in order to obtain and predict physical outcomes.

1 Quantum states

A quantum state is a mathematical object that must encodes all possible outcomes on any experiment that can perform on it. This is the meaning of Postulate 1.
P1 The state of a physical system S is encoded in a quantum state $\rho_S \in \mathcal{B}(\mathcal{H})$ which is an operator (matrix) acting on a Hilbert space.

- Associated to each *quantum system*, S, there is a Hilbert space $\mathcal{H}$. We consider $\dim(\mathcal{H}) = d < \infty$.
- A Hilbert space is **a vector space over the complex field** $\mathcal{V}(\mathbb{C})$ **with inner product** $\langle\cdot|\cdot\rangle \in \mathbb{C}$. Quantum states are normalized $|| \, |\psi\rangle \, || = \sqrt{\langle\psi|\psi\rangle} = 1$.
- Schwarz inequality: $|\langle\psi|\phi\rangle| \leq || \, |\psi\rangle \, || \cdot || \, |\phi\rangle \, ||$. Triangle inequality: $|| \, |\psi\rangle + |\phi\rangle \, || \leq || \, |\psi\rangle \, || + || \, |\phi\rangle \, ||$
- **P1**: The state of a system S is described by $\rho \in \mathcal{B}(\mathcal{H})$ with $\rho \geq 0$,tr$\rho = 1$. If S is, with probability p_i, in $|\psi_i\rangle$, ($\sum_i p_i = 1$), then $\rho = \sum_i p_i \, |\psi\rangle_i \langle\psi_i|$. To each ρ there are infinitely many different ensembles $\mathcal{E}_i = \{p_i, \, |\psi_i\rangle\}$. Pure states describe **isolated** systems $\rho = |\psi\rangle\langle\psi| \Leftrightarrow \{1, |\psi\rangle\}$, with $|\psi\rangle \in \mathcal{H}$.
- **Equivalence of ensembles***: Two ensembles are equivalent if they are unitarely related: $\{p_i, |\psi_i\rangle\}_{i=1}^n$ and $\{q_i, |\phi_i\rangle\}_{i=1}^m$ with n, m if $|\tilde{\phi}_j\rangle = \sum_i U_{ij} |\tilde{\psi}_i\rangle$ with $|\tilde{\phi}_j\rangle = \sum_i U_{ij} |\tilde{\psi}_i\rangle$ and $|\tilde{\psi}_j\rangle = \sqrt{p_j} |\psi_j\rangle$
- The simplest quantum system is a qubit ($\mathcal{H} = \mathbb{C}^2$) and can always be described by $\rho = \frac{\mathbb{1} + \vec{r}\vec{\sigma}}{2}$ with $\vec{r} \in \mathbb{R}^3$ and the Pauli matrices $\vec{\sigma} = (\sigma_x, \sigma_y \sigma_z)$ (also denoted by X, Y, Z). The Bloch sphere represents 1-qubit space. Pure states $|\psi\rangle$ lie in the surface, mixed states ρ inside.

2 Linear operators

Linear operators are maps $A : \mathcal{H}_{in} \to \mathcal{H}_{out}$ s.t. $A(\alpha |\psi\rangle + \beta |\phi\rangle) = \alpha A(|\psi\rangle) + \beta A(|\phi\rangle)$ ($A \leftrightarrow$ Matrix).

- The identity operator $\mathbb{1}$ is a map s.t. $\mathbb{1}(|\psi\rangle) = |\psi\rangle$ and $\mathbb{1} = \sum_i |i\rangle\langle i|$ for $i = 1 \cdots d$, where $\{|i\rangle\}_{i=1}^d$ is *any* orthonormal basis of $\mathcal{H}$.
- if $A : \mathcal{H}_{in} \to \mathcal{H}_{out}$ then $A = \mathbb{1}_{out} A \mathbb{1}_{in} = \sum_{ij} A_{ij} |i\rangle\langle j|$ where $\{|j\rangle\}, \{|i\rangle\}$ are orthonormal basis of $\mathcal{H}_{in}, \mathcal{H}_{out}$.

- The space of bounded operators $A \in \mathcal{B}(\mathcal{H})$ ($\mathrm{tr}A < \infty$) is itself a Hilbert space with the Hilbert-Schmidt inner product: $A, B \in \mathcal{B}(\mathcal{H})$, $\langle A|B\rangle = \mathrm{tr}(A^\dagger B)$.

- The adjoint of A is the operator $A^\dagger : \mathcal{H}_{out} \to \mathcal{H}_{in}$, $A^\dagger = \sum_{ij} (A_{ij})^* |j\rangle \langle i|$.

- Useful operators in Q.M.

  1. **Hermitian** $A = A^\dagger$
  2. **Semidefinite positive** $A \geq 0$ iff $A = B^\dagger B \Leftrightarrow \langle\psi|A|\psi\rangle \geq 0 \forall |\psi\rangle \Leftrightarrow$ A has positive semidefinite eigenvalues (in the complex field!). If $A \geq 0 \Rightarrow A$ Hermitian.
  3. **Unitary** $UU^\dagger = U^\dagger U = \mathbb{1}$
  4. Isometry $VV^\dagger = \mathbb{1}$ (operation that preserve distances)

- Representations of linear operators: 1. **Spectral Decomposition** Any Hermitian operator admits a decomposition $A = UDU^\dagger$, i.e. $A = \sum \lambda_i |\lambda_i\rangle \langle\lambda_i|$ with λ_i eigenvalues $\{|\lambda_i\rangle\}$ eigenvectors

- **Singular Value Decomposition** Any $A : \mathcal{H}_{in} \to \mathcal{H}_{out}$ admits a decomposition $A = UDV^\dagger$ where $V : \mathcal{H}_{in} \to \mathcal{H}_{in}$; $U : \mathcal{H}_{out} \to \mathcal{H}_{out}$ and $D : \mathcal{H}_{in} \to \mathcal{H}_{out}$ is diagonal. (used for the Schmidt decomposition)

- Functions of linear operators. Given a function $f : \mathbb{C} \to \mathbb{C}$ and an operator $A = A^\dagger : \mathcal{H}_{in} \to \mathcal{H}_{in}$, then $f(A) = \sum f(\lambda_i) |\lambda_i\rangle \langle\lambda_i|$. Useful functions in Q.I: $\log(A)$, $\mathrm{tr}A$, e^A.

3 Quantum Evolution

P2: The evolution of a **isolated** quantum system is given by a unitary map $U(t) : \mathcal{H} \to \mathcal{H}$ so that $|\Psi(t)\rangle = U(t)|\Psi(0)\rangle$ and equivalently $\rho(t) = U(t)\rho(0)U^\dagger(t)$.
(Evolution can also be antiunitary $A = U(t)K$ where K is charge conjugation= time reversal).
An **open** quantum system S is a system in contact with an environment E.
The evolution of an **open system is not unitary** but can be understood as a unitary evolution of $(S+E)$, i.e., $\rho_S(t) = Tr_E(U(\rho_S(0) \otimes \rho_E)U^\dagger)$.
In the Heisenberg picture, operators evolve according to $A(t) = U^\dagger(t)A(0)U(t)$

4 Quantum Measurements

P3 (standard version 1): To each physical property of a quantum system $S \Leftrightarrow A$, where $A = A^\dagger \in \mathcal{B}(\mathcal{H})$ (A is an observable).

P3 A generalized measurement M is a set operators $\{M_m : \mathcal{H}_{in} \to \mathcal{H}_{in}, s.t.$and $\sum_m M_m^\dagger M_m = \mathbb{1}\}$. If S is encoded in ρ, measuring $\{M_m\}$ produces outcome m with probability $p_m = p(m|\rho) = Tr(M_m \rho M_m^\dagger)$ and leaves S in $\rho_m = \frac{M_m \rho M_m^\dagger}{p_m}$

- A projective measurement P is a set of operators $\{P_m : \mathcal{H}_{in} \to \mathcal{H}_{in}\ s.t.\ P_m^2 = P_m,\ P_m P_n = \delta_{mm},\ \sum_m P_m = \mathbb{1}\}$. If S is encoded in ρ, measuring $\{P_m\}$ produces outcome m with probability $p_m = \mathrm{tr}(P_m \rho)$ and leaves the state in $\rho_m = \frac{P_m \rho P_m}{p_m}$. The expectation value of the observable P is $\langle P\rangle = \sum m p_m = \mathrm{tr}(P\rho)$ and its variance $\Delta P = \sqrt{\langle P^2\rangle - \langle P\rangle^2}$. Physical quantities are obtained by projective (also called von Neumann) measurements $\Leftrightarrow$ observables.

- A POVM E is a set of operators $\{E_m \mid E_m \geq 0,\ \sum_m E_m = \mathbb{1}\}$. Measuring E_m we obtain outcome m with probability $p_m = \mathrm{tr}(\rho E_m)$ $E = \sum m E_m$ is in general not an observable and in general we cannot say which is the state of the system after measuring a POVM. In terms of Kraus operators we can write $E_m = K_m^\dagger K_m$. There are many Kraus operators associated to the same POVM. POVM can be understand as projective measurements in a larger space (Neumark extension).

-

5 Quantum channels, operations, Q: Instruments

Quantum channels (also called quantum operations or quantum maps) are the only allowed operations on quantum states. Quantum Channels have different representations, i.e. are expressed in different but equivalent ways.

- A **quantum channel** is a CPTP map, i.e. $\Lambda : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$, which is linear, positive ($\Lambda(\rho_{in}) \geq 0$), completely positive ($(\mathbb{1}_c \otimes \Lambda)\rho_{c,in} \geq 0$), and trace preserving $\mathrm{tr}\Lambda(\rho) = \mathrm{tr}(\rho)$. [$\Lambda$ maps operators onto operators, $\Lambda \equiv$superoperator].
- **Choi-Jamiołkowski representation**: isomorphism between quantum channels and bipartite states. If Λ is a CPTP map, $E_\Lambda = (\mathbb{1}_A \otimes \Lambda_{in,out})(|\Omega\rangle\langle\Omega|)$ isomorphism between maps acting in $\mathcal{B}(\mathcal{H}_{in}, \mathcal{H}_{out})$ and operators (states) $\mathcal{B}(\mathcal{H}_{in} \times \mathcal{H}_{out}$. To each map Λ there exist an operator $E_\Lambda = (\mathbb{1}_A \otimes \Lambda_{in,out})(|\Omega\rangle\langle\Omega|)$, where $|\Omega\rangle = \sum |i,i\rangle$ is the unnormalized maximally entangled state $i = 1, cdots, d$. e elements of $E_\Lambda \in cB(\mathcal{H}_{in} \times \mathcal{H}_{out}$
- **Kraus representation**. Λ is a CPTP map iff $\Lambda(\rho) = \sum_k K_k \rho K_k^\dagger$ where the set $\{K_k\}$ are Kraus operators fulfilling: $K_k^\dagger K_k \geq 0\ \forall k, \sum_k K_k^\dagger K_k = \mathbb{1}$. The minimal number of Kraus operators is $r_k \leq d_{in} d_{out}$
- Freedom of Kraus representations*: Two sets of Kraus operators $\{K_j\}$ and $\{\tilde{K}_l\}$ represent the same quantum channel Λ iff there exist a unitary transformation such that $K_j = \sum_l U_{kl} K_l$.
- **Matrix representation** Recall that $\mathcal{B}(\mathcal{H})$ + Hilbert-Schmidt inner product form a Hilbert space with basis $\{|i\rangle\langle j|\}$. If $\Lambda : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ is a CPTP map then $M_{ij}^{kl}(\Lambda) = \mathrm{tr}[|l\rangle\langle k|\Lambda(|i\rangle\langle j|)]$.
- **Stinespring dilation***: Any CPTP map $\Lambda : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ can be expressed as: $\mathrm{c}\Lambda(\rho) = \mathrm{tr}_E(U(\rho \otimes |0\rangle_E \langle 0| U^\dagger)$ where E denotes the environment and $U \in \mathcal{B}(\mathcal{H}_{in} \otimes \mathcal{B}(\mathcal{H}_E))$ is a unitary matrix. The dimension of the environment $d_E \leq d^2$. (Any CPTP map is the effect of a unitary evolution in a larger space. *simplest formulation of the Stinespring).
- Using Stinespring dilation is easy to see that: (i) a quantum state ρ is a CPTP map $\rho : \mathcal{C} \to \mathcal{B}(\mathcal{H})$ such that $\rho = \mathrm{tr}_E(|\psi\rangle\langle\psi|)$ with $|\psi\rangle = U|0\rangle \in \mathcal{H} \otimes \mathcal{H}_E$. (ii) Measurements can also be thought as CPTP channels.
- Any map acting on a qubit can be expressed as a function of $\{\mathbb{1}, X, Y, Z\}$
- A **quantum instrument** is a set of CP-maps $\{T_i\}$ such that $\sum_i T_i = T$ is a CPTP map. It can be thought as the components of the CPTP map T or as a POVM $T_i = \sqrt{E_i}\rho\sqrt{E_i}$ where $\{E_i \geq 0\ \ \sum E_m = \mathbb{1}\}$. A quantum instrument can be understood as a noisy channel that produces a classical and a quantum output.

The **church of Hilbert space** can be summarized as:

- Mixed states $\rho \ \Rightarrow$ **Purification** $\Rightarrow$ there exist $|\Psi\rangle_{AB}$ in a larger Hilbert space s.t. $\rho = Tr_B |\Psi\rangle_{AB}$
- CTPTs $\Lambda(\rho) \ \Rightarrow$ **Steinspring dilation** $\Rightarrow$ there exist a unitary U in a larger Hilbert space s.t. $\Lambda(\rho) = Tr_E(U(\rho \otimes \rho_E)U^\dagger)$, and without loosing generality we can assume $\rho_E = |E\rangle\langle E|$.
- POVMs $\{E_m\} \Rightarrow$ **Naimark dilation** $\Rightarrow$ there exist a set of Projectors $\{\tilde{P}_m\}$ in a larger Hilbert space s.t. $p(m) = Tr(E_m \rho) = Tr(\tilde{P}(\rho \otimes |\omega\rangle\langle\omega|)$

6 Composite systems

P4: The state of a composite quantum system S is encoded in an operator $\rho \in \mathcal{B}\left(\bigotimes_{i=1}^N \mathcal{H}_i\right)$. If the state of each constituent system is given by ρ_i then the state of the composite system is $\rho = \bigotimes_{i=1}^N \rho_i$

- Bipartite systems: Let $\mathcal{H}_1$ and $\mathcal{H}_2$ with orthonormal basis $\{|i\rangle_1\}_{i_1=1\cdots d_1}$ and $\{|i\rangle_2\}_{i_2=1\cdots d_2}$. An orthonormal basis of $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is given by $\{|i_1\ i_2\rangle\} = \{|i_1\rangle\}_{i_1=1}^{d_1} \otimes \{|i_2\rangle\} i_2 = 1^{d_2}$
- Any pure state $|\psi\rangle_{1,2} \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written in the $\{|i_1\rangle\}_{i_1=1}^{d_1}, \{|i_2\rangle\}_{i_1=1}^{d_2}$ basis as$|\psi\rangle_{1,2} = \sum_{i_1,i_2} c_{i_1\ i_2} |i_1\ i_2\rangle$
- Pure states of the form $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle = |\psi\rangle_{1,2} = \sum_{i_1=1,i_2=1}^{d_1,d_2} \phi_{i_1}\chi_{i_2} |i_1\rangle \otimes |i_2\rangle$ are product states

- Operators: Suppose $A : \mathcal{H}_1 \to \mathcal{H}_1$ and $B : \mathcal{H}_2 \to \mathcal{H}_2$, then $C = A \otimes B : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathcal{H}_1 \otimes \mathcal{H}_2$.
- Let $\mathcal{H} = \bigotimes_{i=1}^{N} \mathcal{H}_i$. A unitary transformation $U : \mathcal{H} \to \mathcal{H}$ is local iff $U = \bigotimes_{i=1}^{N} U_i$, where $U_i : \mathcal{H}_i \to \mathcal{H}_i$. Otherwise the unitary is non local.
- A measurement with operators $\{M_m : \mathcal{H} \to \mathcal{H}\}_{m=1}^{k}$ is local iff $M_m = \bigotimes_{i=1}^{N} M_m^{(i)}$
- Schmidt decomposition. Any **bipartite** state $|\Psi\rangle \in \mathcal{H}_{AB}$, can be written as $|\Psi\rangle_{AB} = \sum_{k=1}^{\min(d_1,d_2)} \sqrt{\lambda_k}\, |u_k\, v_k\rangle$ where $\{|u_k\rangle\}_{k=1}^{d_1}, \quad \{|v_k\rangle\}_{k=1}^{d_2}$ are orthonormal basis of $\mathcal{H}_A$ and of $\mathcal{H}_B$ respectively. The coefficients $\lambda_k \geq 0$ are the Schmidt coefficients, $\sum_{k=1}^{\min(d_1,d_2)} \lambda_k = 1$. The number of Schmidt coefficients is the Schmidt rank r_S
- Entangled pure states. A bipartite pure state is entangled if $r_S > 1$.
- A maximally entangled pure state $\Omega = \frac{1}{\sqrt{d}} \sum_i |i,i\rangle$.
- In $\mathcal{H}_2 \otimes \mathcal{H}_2$ (2-qubits) the Bell states: $\{|\Psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}},\ |\Phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}\}$ are maximally entangled and form the Bell basis.
- Reduced density matrix. Given a composite quantum state $|\Psi\rangle \in \bigotimes_{k=1}^{N} \mathcal{H}$ the reduced density matrix of subsystem k $\rho_K \in \mathcal{B}(\mathcal{H}_k)$ (also call the marginal) is the quantum state obtained by tracing out all subsytems $i = 1, \cdot N$ except k.
- The reduced states of a bipartite entangled pure state with Schmidt decomposition $|\Psi\rangle_{AB} = \sum_{k=1}^{\min(d_1,d_2)} \sqrt{\lambda_k}\, |u_k, v_k\rangle$ are diagonal in the Schmidt basis e.g. $\rho_A = \sum_{k=1}^{d_1} \lambda_k |u_k\rangle \langle u_k|$.
- Purification: Given ρ_A with spectral decomposition $\rho_A = \sum_k \lambda_k |u_k\rangle \langle u_k|$, the state can always be purified to a bipartite state $|\Psi\rangle_A B$ such that $\rho_A = tr_B |\Psi\rangle_{AB} \langle\Psi|$. The minimal dilation (the minimal dimension of the Hilbert space $\mathcal{H}_B$ is $dim(\mathcal{H}_B) = rank(\rho_A)$ where the rank of a matrix is the number of eigenvalues different from zero.
- Simple quantum protocols using entanglement: Teleportation, super-dense coding

6.1 Entanglement in bipartite states: characterization, criterion and measures

- A state $\rho_{AB} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be separable (no entangled) iff it can be written as $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i = \sum_m q_m |e_m^A\rangle \langle e_m^A| \otimes |f_m^B\rangle \langle f_m^B|$ with $\sum_i p_i = \sum_m p_m = 1$.
- The unit of entanglement for qubits is the e-bit (entanglement contained in a maximally entangled states of 2 qubits)
- **A measure of entanglement** E fulfills: (i) $E(\rho) \geq 0$, (ii) $E(\sigma) = 0$ if the state is separable and (iii) monotone $E(\Lambda(\rho) \leq E(rho)$ where Λ is a LOCC (local operations plus classical communication)
- The von Neumann entropy of a quantum state $S(\rho) = -Tr\rho log(\rho)$.
- The **entanglement entropy** is the standard measure for pure states ($E(|\psi\rangle_{AB}) = S(\rho_A) = S(\rho_B)$
- Given a N-partite pure state, one can always calculate the entanglement entropy w.r.t. a given bi-partition $E_k(|\psi\rangle_{A/B}) = S(\rho_A) = S(\rho_B)$ where $A = 1,2,...k$ and $B = N - k$
- The entanglement of formation is the convex roof extension of the entanglement entropy for mixed states (difficult to calculate and use).
- The entanglement cost and entanglement of distillation are asympototic measures of entanglement for mixed states (difficult to use)
- The **concurrence** is an *operationally* measure of entanglement for mixed states of 2 qubits $C(\rho_{AB}) = min(0, \mu_1 - \mu_2 - \mu_3 - \mu_4)$ where $\{\mu_i\}$ are the eigenvalues in decreasing order of $R = \sqrt{\sqrt{\tilde{\rho}_{AB}}\rho_{AB}\sqrt{\tilde{\rho}_{AB}}}$ with $\tilde{\rho}_{AB} = (Y \otimes Y)\rho_{AB}^*(Y \otimes Y)$

- The relative entropy between two states $S(\rho||\sigma) = Tr(\rho(\log\rho - \log\sigma))$
- The relative entropy of entanglement of a mixed state ρ_{AB} is $E_{RE}(\rho_{AB}) = min(\sigma \in S)S(\rho_{AB}||\sigma)$ where σ is a separable states and minimization is done over all separable states. (difficult to measure)+
- Partial transpose. Given $\rho_{AB} = \sum_{iu\mu\nu} \rho_{ij}^{\mu\nu} (|i\rangle\langle j|)_A \otimes (|\mu\rangle\langle\nu|)_B \Rightarrow \rho_{AB}^{T_B} = \sum_{ij\mu\nu} \rho_{ij}^{\mu\nu} (|i\rangle\langle j|)_A \otimes (|\nu\rangle\langle\mu|)_B$
- PPT entanglement criterion: (Positivity under Partial Transposition)
- if ρ_{AB} is separable $\Rightarrow \rho_{AB}^{T_A} \geq 0$, and, $\rho_{AB}^{T_B} \geq 0$
- In $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ PPT $\Leftrightarrow$ separability
- In $\mathbb{C}^n \otimes \mathbb{C}^m$ with $n \cdot m > 6$, PPT is necessary but not sufficient for separablity
- Majorization entanglement criterion: if ρ_{AB} is separable then $\lambda(\rho_{AB}) \prec \lambda(\rho_A)$ and $\lambda(\rho_{AB}) \prec \lambda(\rho_B)$, where $\lambda(\cdot)$ are the eigenvalues of the matrix arranged in decreasing order.
- Entropy entanglement criterion: if ρ_{AB} is separable then $S(\rho_{AB}) \geq S(\rho_A)$ and $S(\rho_{AB}) \geq S(\rho_B)$, where $S(\cdot)$ is the von Neumann entropy.
- **Negativity** measure $\mathcal{N}(\rho_{AB} = \frac{||\rho_{AB}^{T_B}||-1}{2}$ corresponds to the sum of the negative eigenvalues of the partial transpose
- An **entanglement witness** W is an (super-operator) s.t. : (i) $Tr(W\sigma) \geq 0$, for all separable states σ, but there exist at least an **entangled state** ρ s.t. (ii) $Tr(W\rho) < 0$
- Because Choi-Jamiołkowski isomorphims, associated to each entanglement witness W there is a positive (but not CP) map Λ and vice-versa
- **Decomposable** entanglement witnesses $\Leftrightarrow W = P + Q^{T_A}$ with $P, Q \geq 0$
- A non-decomposable witness $W \neq P + Q^{T_A} \Leftrightarrow$ detects at least one PPTentangled state (PPTES)
- Notice that $Tr(W\rho^{T_A}) = Tr(W^{T_A}\rho)$