CHAPTER 5 – MATHEMATICS OF FINITE-DIMENSIONAL QUANTUM INFORMATION THEORY

§ 5.1 Quantum systems and quantum states

A quantum system is a physical system with one or more quantum-mechanical degrees of freedom that are either discrete or continuous:

- position and momentum of a particle
- spin of a particle (e.g., spin along z-axis of an electron)
- polarization of a photon

.....

Motivating example: spin of an electron

Two possible "basis states": spin up ($\uparrow$), spin down ($\downarrow$)

Assign to each vectors in a vector space $\mathbb{C}^2$ known as state space:

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Superposition principle (experimentally confirmed): quantum system can be prepared in a state $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$,

where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$.

The probabilities of finding electron in spin-up or spin-down are given by $\Pr(\uparrow) = |\langle\uparrow|\psi\rangle|^2 = |\alpha|^2$ and $\Pr(\downarrow) = |\langle\downarrow|\psi\rangle|^2 = |\beta|^2$.

More formally:

1) The state space describing a quantum system is given by a Hilbert space, a complex inner-product space that is complete.

We restrict our attention to finite-dimensional Hilbert spaces $\mathcal{X} \cong \mathbb{C}^d$.

2) Observable quantities are represented by Hermitian operators

$A \in \mathrm{Herm}(\mathcal{X}) = \{ X \in \mathcal{L}(\mathcal{X}) : X^\dagger = X \}$.

The real eigenvalues of A can be measured in an experiment.

3) A state of a quantum system assigns an expectation value to observables, that is, it describes the expected measurement statistics of an observable in a quantum system.

We identify states with density operators $\rho \in \mathcal{L}(\mathcal{X})$ satisfying:

- positivity: $\rho \geq 0$ $(:\Leftrightarrow \langle \varphi | \rho | \varphi \rangle \geq 0 \ \forall |\varphi\rangle \in \mathcal{X})$
- normalization: $\mathrm{tr}\,\rho = 1$.

The expectation of an observable A w.r.t. a state ρ is given by

$$\langle A \rangle_\rho = \mathrm{tr}(\rho A).$$

The set of density matrices of a finite-dim. Hilbert space is convex and compact. That is, if ρ_i are density matrices and λ_i probabilities then $\rho = \sum_i \lambda_i \rho_i$ is also a density matrix.

4) A pure state is an extreme point in the convex set of density matrices, that is, it cannot be written non-trivially as $\rho = \sum_i \lambda_i \rho_i$.

A pure density matrix has rank 1 and can be written as a projector $\rho = |\psi\rangle\langle\psi|$ for some vector $|\psi\rangle \in \mathcal{H}$ with $\langle\psi|\psi\rangle = 1$ ($\Leftrightarrow \operatorname{tr}\rho = 1$).

$|\psi\rangle$ is also often called a pure state or state vector.

A density matrix (state) that is <u>not</u> pure is called mixed.

5) A collection of state vectors $(|\psi_i\rangle)_i$ with probabilities $(p_i)_i$ is called a pure-state ensemble for a mixed state ρ if

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| .$$

Every mixed state has infinitely many pure-state ensembles realizing it.

Particularly useful: spectral decomposition $\rho = \sum_i \lambda_i |v_i\rangle\langle v_i|$, where $(\lambda_i)_i$ are the eigenvalues of ρ and $\{|v_i\rangle\}$ is an orthonormal basis of eigenvectors of ρ: $\rho|v_i\rangle = \lambda_i |v_i\rangle$.

6) Because $\rho \geq 0$ and $\operatorname{tr}(\rho) = 1$, we have $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$.

Hence, the eigenvalues of a density matrix form a probability distribution, thus generalizing "classical" states.

§ 5.2 Measurements

Projective measurements: Let A be an observable on a quantum system $\mathcal{H}$ in the state ρ. Consider the spectral decomposition

$$A = \sum_\alpha x_\alpha P_\alpha ,$$

where x_α are the eigenvalues of A and P_α are the orthogonal projectors onto the corresponding eigenspaces.

They satisfy: a) $P_\alpha \geq 0$ (in particular $P_\alpha^\dagger = P_\alpha$)

b) $P_\alpha P_\beta = \delta_{\alpha\beta} P_\alpha$

c) $\sum_\alpha P_\alpha = \mathbb{1}$.

$\{P_\alpha\}_\alpha$ is called a **projective measurement**, that gives the value x_α with probability $p_\alpha = \mathrm{tr}(\rho P_\alpha)$.

For the p_α to be probabilities, we only need a) and b) above!

This is a generalized notion of measurement,

$$\{E_k\}_k \text{ with } E_k \geq 0 \text{ and } \sum_k E_k = \mathbb{1},$$

called a **positive operator-valued measure (POVM)**. The E_k are often called effect operators. The outcome "k" is obtained with probability $p_k = \mathrm{tr}(\rho E_k)$.

§ 5.3 Composite systems and entanglement

Consider two quantum systems A and B with associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The joint system AB is described by the tensor product $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$.

Density matrices: $\rho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \cong \mathcal{L}(\mathcal{H}_A) \otimes \mathcal{L}(\mathcal{H}_B)$

The marginal state ρ_A of a bipartite state ρ_{AB} is defined via

$$\mathrm{tr}\left(\rho_{AB}\left(X_A \otimes \mathbb{1}_B\right)\right) = \mathrm{tr}\left(\rho_A X_A\right) \quad \forall\, X_A \in \mathcal{L}(\mathcal{H}_A). \qquad (*)$$

This uniquely defines a linear map $\mathrm{tr}_B : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_A)$ called the partial trace. Choosing some ONB $\{|e_i\rangle_B\}_{i=1}^{|B|}$ for $\mathcal{H}_B$,

$$\mathrm{tr}_B\, X_{AB} = \sum_{i=1}^{|B|} \left(\mathbb{1}_A \otimes \langle e_i|_B\right) X_{AB} \left(\mathbb{1}_A \otimes |e_i\rangle_B\right)$$

The equation $(*)$ shows that the marginal ρ_A describes the effective state of system A when doing a local measurement.

We distinguish different types of correlations between A and B:

1) Product states: $\rho_{AB} = \omega_A \otimes \sigma_B$ for states ω_A and σ_B.

   In a product state, any local measurements do not depend on the other system, hence A and B are completely uncorrelated.

2) Separable states: $\varrho_{AB} = \sum_i p_i\, \omega_A^{(i)} \otimes \sigma_B^{(i)}$ for states $(\omega_A^{(i)})$ and $(\sigma_B^{(i)})_i$ and a probability distribution $(p_i)_i$.

Separable states describe classical correlation between A and B corresponding to the index i. Conditioned on this value i, the state $\omega_A^{(i)} \otimes \sigma_B^{(i)}$ is uncorrelated.

3) Entangled states are states that are not separable.

They describe quantum correlations.

Ex.: Let $\{|0\rangle, |1\rangle\}$ be a basis for $\mathbb{C}^2$ and consider

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right),$$

called EPR state, Bell state, or maximally entangled state.

$$\phi^+ = |\phi^+\rangle\langle\phi^+| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$ is <u>not</u> separable.

Note: A pure separable state is automatically a product state.

Detecting separability is generally hard!

It is NP-hard to decide whether a given mixed state is separable.

However, for pure states there is a nice (and efficient) criterion based on the singular value decomposition.

$\boxed{\text{Prop}}$ (Schmidt decomposition)

Let $|\psi\rangle_{AB}$ be a pure bipartite quantum state. Then there are sets of orthonormal vectors $\{|e_i\rangle_A\}_{i=1}^r$ and $\{|f_j\rangle_B\}_{j=1}^r$ and strictly positive real numbers $(\lambda_i)_{i=1}^r$ such that

$$|\psi\rangle_{AB} = \sum_{i=1}^r \sqrt{\lambda_i}\, |e_i\rangle_A \otimes |f_i\rangle_B .$$

The Schmidt coefficients $(\lambda_i)_{i=1}^r$ satisfy $\sum_{i=1}^r \lambda_i = 1$, and are unique up to reordering. The integer r is called Schmidt rank of $|\psi\rangle_{AB}$. $|\psi\rangle_{AB}$ is entangled iff $r>1$. The marginals of $|\psi\rangle_{AB}$ are given by

$$\rho_A = \mathrm{tr}_B\, \psi_{AB} = \sum_{i=1}^r \lambda_i\, |e_i\rangle\langle e_i|_A$$

$$\rho_B = \mathrm{tr}_A\, \psi_{AB} = \sum_{i=1}^r \lambda_i\, |f_i\rangle\langle f_i|_B .$$

These are spectral decompositions, i.e., ρ_A and ρ_B have the same spectrum given by the Schmidt coefficients, and the Schmidt vectors $\{|e_i\rangle_A\}$ and $\{|f_j\rangle_B\}$ can be completed to eigenbases of ρ_A and ρ_B, resp.

<u>Proof sketch:</u> Consider ONBs $\{|v_i\rangle_A\}_{i=1}^{|A|}$ and $\{|w_j\rangle_B\}_{j=1}^{|B|}$, and expand $|\psi\rangle_{AB} = \sum_{i,j} x_{i,j}\, |v_i\rangle_A \otimes |w_j\rangle_B$. All claims now follow from the singular value decomposition of the matrix X with coefficients $x_{i,j}$.

$\square$

Def (Purification)

Let ρ_A be a mixed quantum state. Any state $|\psi\rangle_{AR} \in \mathcal{H}_A \otimes \mathcal{H}_R$ satisfying $\mathrm{tr}_R\, \psi_{AR} = \rho_A$, where $\mathcal{H}_R$ is some auxiliary Hilbert space, is called a purification of ρ_A.

Prop Let ρ_A be a mixed quantum state.

i) A purification of ρ exists on $\mathcal{H}_A \otimes \mathcal{H}_R$, where $\dim \mathcal{H}_R \geq \mathrm{rank}\, \rho_A$.

ii) Let $|\psi\rangle_{AR_1}$ and $|\varphi\rangle_{AR_2}$ be two purifications of ρ_A, and w.l.o.g. assume $\dim \mathcal{H}_{R_1} \leq \dim \mathcal{H}_{R_2}$. Then there exists an isometry $V: \mathcal{H}_{R_1} \to \mathcal{H}_{R_2}$ s.t. $|\varphi\rangle_{AR_2} = (\mathbb{1}_A \otimes V)|\psi\rangle_{AR_1}$.

Proof: i) Consider a spectral decomposition $\rho_A = \sum_{i=1}^{r} \lambda_i |v_i\rangle\langle v_i|_A$, where $\lambda_i > 0$ s.t. $r = \mathrm{rank}(\rho_A)$. Take $\mathcal{H}_R = \mathbb{C}^r$ with ONB $\{|w_i\rangle_R\}_{i=1}^{r}$, then $|\psi\rangle_{AR} := \sum_{i=1}^{r} \sqrt{\lambda_i}\, |v_i\rangle_A \otimes |w_i\rangle_R$ is the desired purification.

ii) Follows easily from Schmidt decomposition. $\square$

§ 5.4 Distance measures

There are many ways of measuring how close quantum states are, which is important because we want to quantify approximations.

Here, we focus on two measures: fidelity and trace norm.

First, we define the trace norm of a linear operator:

$$X \in \mathcal{L}(\mathcal{H}): \quad \|X\|_1 = \operatorname{tr}\sqrt{X^\dagger X} = \sum_{i=1}^{d} s_i(X)$$

where $d = \dim \mathcal{H}$ and $s_i(X)$ are the singular values of X.

If X is Hermitian with real eigenvalues λ_i, then $\|X\|_1 = \sum_{i=1}^{d} |\lambda_i|$.

$\|.\|_1$ is a norm in the mathematical sense.

$\boxed{\text{Def}}$ (Trace distance)

Let ρ and σ be quantum states on $\mathcal{H}$. Then their trace distance is defined as $D(\rho,\sigma) := \frac{1}{2}\|\rho - \sigma\|_1$.

Properties of the trace distance:

1) $D(.,.)$ is a metric, i.e., non-neg., symmetric, and satisfies the triangle inequality.

2) $0 \leq D(\rho,\sigma) \leq 1$, and $D(\rho,\sigma) = 0 \iff \rho = \sigma$
   and $D(\rho,\sigma) = 1 \iff \operatorname{supp}\rho \perp \operatorname{supp}\sigma$ (where $\operatorname{supp} X := (\ker X)^\perp$)

3) $D(\rho,\sigma) = D(U\rho U^\dagger, U\sigma U^\dagger)$ for all unitaries U, and
   $D(\rho_A, \sigma_A) \leq D(\rho_{AB}, \sigma_{AB})$.

4) $D(\rho,\sigma) = \sup\{\operatorname{tr}[P(\rho-\sigma)] : P \geq 0 \text{ and } \mathbb{1} - P \geq 0.\}$

5) $D(\rho,\sigma)$ is related to the max. probability of distinguishing ρ and σ.

$\boxed{\text{Def}}$ (Fidelity)

The fidelity $F(\rho,\sigma)$ of quantum states ρ and σ is defined as

$$F(\rho,\sigma) = \| \sqrt{\rho}\sqrt{\sigma} \|_1 = \operatorname{tr}\left(\sigma^{1/2}\rho\,\sigma^{1/2}\right)^{1/2}.$$

Properties of the fidelity:

1) $0 \leq F(\rho,\sigma) \leq 1$, and $F(\rho,\sigma) = 1$ iff $\rho = \sigma$,

   $F(\rho,\sigma) = 0$ iff $\operatorname{supp}\rho \perp \operatorname{supp}\sigma$.

2) $F(\rho,\sigma) = F(\sigma,\rho)$, but F is <u>not</u> a metric.

3) $F(\rho,\sigma) = F(U\rho U^\dagger, U\sigma U^\dagger)$ for all unitaries U,

   and $F(\rho_{AB},\sigma_{AB}) \leq F(\rho_A,\sigma_A)$.

4) $F(.,.)$ is jointly concave: $F\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \geq \sum_i p_i F(\rho_i,\sigma_i)$.

5) For pure states $|\psi\rangle$ and $|\varphi\rangle$, $F(\psi,\varphi) = |\langle\psi|\varphi\rangle|$.

6) Uhlmann's theorem:

$$F(\rho,\sigma) = \max\left\{ |\langle\psi^\rho|\varphi^\sigma\rangle| : |\psi^\rho\rangle \text{ purifies } \rho,\ |\varphi^\sigma\rangle \text{ pur. } \sigma \right\}.$$

$\boxed{\text{Prop}}$ (Fuchs-van de Graaf inequalities)

For any two quantum states ρ and σ,

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$