Contents

1. Basic notions in quantum information theory

The field is motivated by the fact that we want to control quantum systems.

1. Can we construct and manipulate quantum systems?
2. If so, which are the scientific and technological applications?

Entanglement frontier: highly complex quantum systems, which are more complex and richer than classical systems. However, quantum systems have *decoherence*, which classical systems don't. "Quantum advantage" gives speed up over classical systems.

Quantum vs classical information theory:

- True randomness.
- Uncertainty.
- Entanglement.

Note we always work with finite-dimensional Hilbert spaces, so take $\mathbb{H} = \mathbb{C}^N$.

1.1. Qubits and basic operations

Notation 1.1 Vectors are denoted by $|\psi\rangle \in \mathbb{C}^n$, dual vectors by $\langle\psi| \in (\mathbb{C}^n)^*$, and inner products by $\langle\psi|\varphi\rangle \in \mathbb{C}$. $|\psi\rangle\langle\psi| : \mathbb{C}^n \to \mathbb{C}^n$ are rank-one projectors.

Definition 1.2 Another important basis of $\mathbb{C}^2$ is $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Definition 1.3 For an operator $T : \mathbb{H} \to \mathbb{H}$, the **operator norm** of T is

$$\|T\| = \|T\|_{\mathbb{H}\to\mathbb{H}} := \sup_{x\in H} \frac{\|T(x)\|_{\mathbb{H}}}{\|x\|_{\mathbb{H}}}$$

Notation 1.4 Let $B(\mathbb{H})$ denote the space of bounded linear operators, i.e. T such that $\|T\| < \infty$.

Notation 1.5 Denote the dual of the operator T by T^*, i.e. the operator that satisfies $\langle y|T(x)\rangle = \langle T^*(y)|x\rangle$ for all $x, y \in \mathbb{H}$.

Definition 1.6 A **quantum measurement** is a collection of measurement operators $\{M_n\}_n \subseteq B(\mathbb{H})$ which satisfies $\sum_n M_n^* M_n = \mathbb{I}$, the identity operator.

Given $|\varphi\rangle$, the probability that $|n\rangle$ occurs after this operation is $p(n) = \langle\varphi|M_n^* M_n|\varphi\rangle$. After performing this operation, the state of the system is $\frac{1}{\sqrt{p(n)}} M_n|\varphi\rangle$.

Example 1.7 A measurement in the computational basis is $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Note M_0 and M_1 are self-adjoint. Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. Then $p(i) = \langle\varphi|M_i|\varphi\rangle = |\alpha_i|^2$. The state after measurement is $\frac{\alpha_i}{|\alpha_i|}|i\rangle$, which is equivalent to $|i\rangle$.

Note that $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are operationally identical: the phase does not affect the measurement probabilities.

Definition 1.8 A quantum measurement $\{M_n\}_n \subseteq B(\mathbb{H})$ is **projective measurement** if the M_n are orthogonal projections (i.e. they are self-adjoint (Hermitian) and $M_n M_m = \delta_{nm} M_n$).

Definition 1.9 An **observable** is a Hermitian operator, which we can express as its spectral decomposition

$$M = \sum_n \lambda_n M_n,$$

where $\{M_n\}_n$ is a projective measurement. The possible outcomes of the measurement correspond to its eigenvalues λ_n of the observable. Note that the expected value of the measurement is

$$\sum_n \lambda_n p(n) = \sum_n \lambda_n \langle \varphi | M_n | \varphi \rangle = \langle \varphi | M | \varphi \rangle.$$

Definition 1.10 $T : \mathbb{H} \to \mathbb{H}$ is **positive (semi-definite)** if $\langle \psi | T | \psi \rangle \geq 0$ for all $|\psi\rangle \in H$.

Definition 1.11 A **POVM (positive operator valued measurement)** is a collection $\{E_n\}_n$ where $E_n = M_n^* M_n$ for a general measurement $\{M_n\}_n$. Note that each E_n is positive.

Note that $\sum_n E_n = \mathbb{I}$ and the probability of obtaining outcome m on $|\psi\rangle$ is $p(m) = \langle \psi | E_m | \psi \rangle$. We use POVMs when we care only about the probabilities of the different measurement outcomes, and not the post-measurement states.

Conversely, given a POVM $\{E_n\}_n$, we can define a general measurement $\{\sqrt{E_n}\}_n$.

Remark 1.12 Any transformation on a normalised quantum state must map it to a normalised quantum state, and so the operation must be unitary.

Definition 1.13 The **Pauli matrice** are

$$\sigma_0 = \mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_X = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\sigma_Y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_Z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The Pauli matrices are unitaries, and we can think of them as quantum logical gates.

Definition 1.14 The **trace** of $T : \mathbb{H} \to \mathbb{H}$ is

$$\operatorname{tr} T = \operatorname{tr} M = \sum_i M_{ii} \in \mathbb{C},$$

where M is a matrix representation of T in any basis (this is well-defined since the trace is cyclic and linear).

Proposition 1.15 For any state $|\varphi\rangle$ and any operator A,

$$\operatorname{tr}(A |\varphi\rangle\langle\varphi|) = \langle \varphi | A | \varphi \rangle.$$

Proof (Hints). Straightforward. □

Proof. $\operatorname{tr}(A|\varphi\rangle\langle\varphi|) = \sum_i \langle i|A|\varphi\rangle\langle\varphi|i\rangle$ for an orthonormal basis $\{|i\rangle\}$. Any basis where $|\varphi\rangle = |j\rangle$ for some j instantly yields the result. Alternatively, we have

$$\operatorname{tr}(A|\varphi\rangle\langle\varphi|) = \sum_i \langle i|A|\varphi\rangle\langle\varphi|i\rangle = \sum_i \langle\varphi|i\rangle\langle i|A|\varphi\rangle = \langle\varphi|I|A|\varphi\rangle = \langle\varphi|A|\varphi\rangle.$$

□

Suppose we don't fully know the state of the system, but know that it is $|\varphi_i\rangle$ with probability p_i. We want to be able to consider the $\sum_i p_i|\varphi_i\rangle$ as a state, but this isn't normalised (except when some $p_i = 1$). To solve this issue, we assume each $|\varphi_i\rangle$ to the rank-one projector $|\varphi_i\rangle\langle\varphi_i|$, and we describe the unknown state by $\rho = \sum_i p_i|\varphi_i\rangle\langle\varphi_i|$. This gives rise to the following definition:

Definition 1.16 A **density matrix/operator** is a linear operator $\rho \in B(\mathbb{H})$ which is:

- Hermitian,
- Positive semi-definite, and
- Satisfies $\operatorname{tr}\rho = 1$.

1.2. Postulates of quantum mechanics (Heisenberg picture)

Postulate 1.17 Given an isolated physical system, there exists a complex (separable) Hilbert space $\mathbb{H}$ associated with it, called **state space**. The physical system is described by a **state vector**, which is a normalised vector in $\mathbb{H}$.

Postulate 1.18 Given an isolated physical system, its evolution is described by a unitary. If the state of the system at time t_1 is $|\varphi_1\rangle$ and at time t_2 is $|\varphi_2\rangle$, then there exists a unitary U_{t_1,t_2} such that $|\varphi_2\rangle = U_{t_1,t_2}|\varphi_1\rangle$.

This can be generalised with the Schrodinger equation: the time evolution of a closed quantum system is given by $i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\varphi(t)\rangle = H|\varphi(t)\rangle$. The Hermitian operator H is called the **Hamiltonian** and is generally time-dependent.

Definition 1.19 Let the spectral decomposition of H be

$$H = \sum_i E_i|E_i\rangle\langle E_i|,$$

where the E_i are the **energy eigenvalues** and the $|E_i\rangle$ are the **energy eigenstates** (or **stationary states**).

The minimum energy is called the **ground state energy** and its associated eigenstate is called the **ground state**. The **(spectral) gap** of H is the (absolute) difference between the ground state energy and the next largest energy eigenvalue. When the gap is strictly positive, we say the system is **gapped**. The states $|E_i\rangle$ are called **stationary**, since they evolve as $|E_i\rangle \to \exp(-iE_it/\hbar)|E_i\rangle$.

We have $|\varphi(t_2)\rangle = U(t_1,t_2)|\varphi(t_1)\rangle$ where $U(t_1,t_2) = \exp(-iH(t_2-t_1)/\hbar)$ which is a unitary. In fact, any unitary U can be written in the form $U = \exp(iK)$ for some Hermitian K.

Postulate 1.20 Given a physical system with associated Hilbert space $\mathbb{H}$, quantum measurements in the system are described by a collection of measurements $\{M_n\}_n \subseteq B(\mathbb{H})$ such that $\sum_n M_n^* M_n = \mathbb{I}$, as in Definition 1.6. The index n refers to the measurement outcomes that may occur in the experiment, and given a state $|\varphi\rangle$ before measurement, the probability that n occurs is

$$p(n) = \langle\varphi| M_n^* M_n |\varphi\rangle.$$

The state of the system after measurement is $\frac{1}{\sqrt{p(n)}} M_n |\varphi\rangle$

Postulate 1.21 Given a composite physical system, its state space $\mathbb{H}$ is also composite and corresponds to the tensor product of the individual state spaces $\mathbb{H}_i$ of each component: $\mathbb{H} = \mathbb{H}_1 \otimes \cdots \otimes \mathbb{H}_N$. If the state in each system i is $|\varphi_i\rangle$, then the state in the composite system is $|\varphi_1\rangle \otimes \cdots \otimes |\varphi_N\rangle$.

Definition 1.22 Given $|\varphi\rangle \in H_1 \otimes \cdots \otimes H_N$, $|\varphi\rangle$ is **entangled** if it cannot be written as a tensor product of the form $|\varphi_1\rangle \otimes \cdots \otimes |\varphi_n\rangle$. Otherwise, it is **separable** or a **product state**.

Example 1.23 The **EPR pair** (**Bell state**) $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled.

1.3. Postulates of quantum mechanics (Schrodinger picture)

Postulate 1.24 Given an isolated physical system, the state of the system is completely described by its density operator, which is Hermitian, positive semi-definite and has trace one.

If we know the system is in state ρ_i with probability p_i, then the state of the system is $\sum_i p_i \rho_i$.

Pure states are of the form $\rho = |\varphi\rangle\langle\varphi|$, **mixed states** are of the form $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$.

Postulate 1.25 Given an isolated physical system, its evolution is described by a unitary. If the state of the system is ρ_1 at time t_1 and is ρ_2 at time t_2, then there is a unitary U depending only on t_1, t_2 such that $\rho_2 = U\rho_1 U^*$.

Postulate 1.26 The same as Postulate 1.20, except we specify that after measurement $\{M_n\}_n$, the probability of observing n is $p(n) = \mathrm{tr}(M_n^* M_n \rho)$ and the state after measurement is $\frac{1}{p(n)} M_n \rho M_n^*$.

Postulate 1.27 The same as Postulate 1.21, except that the state of the composite system is $\rho = \rho_1 \otimes \cdots \otimes \rho_n$, where ρ_i is the state of ith individual system.

Remark 1.28 The Heisenberg and Schrodinger postulates are mathematically equivalent.