Part I
Introduction to quantum mechanics

I. OVERVIEW

II. QUANTUM STATES

A. State vectors

The most fundamental object in representing quantum systems is the *state vector*, a vector representation for the quantum wave-function. A state vector resides in an N-dimensional complex Hilbert space, $\mathcal{H} \in \mathbb{C}^N$, where N denotes the number of basis states supporting the system. These vector representations for quantum states can quickly become unwieldy, since their dimensionality grows exponentially with the number of constituent subsystems. For example, a single qubit resides in a 2-dimensional Hilbert, whereas an n-qubit system resides in a 2^n-dimensional one.

Mathematically, we can employ the following alternate state vector representations, where the latter is referred as *Dirac notation* (with $|n\rangle$ denoting the basis states),

$$\begin{aligned} |\psi\rangle &= \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix} \\ &= \sum_{n=1}^{N} \alpha_n |n\rangle . \end{aligned} \tag{1}$$

Here $\alpha_n \in \mathbb{C}$ are referred to as the *amplitudes* of the state, which for normalisation satisfy,

$$\sum_n |\alpha_n|^2 = 1, \tag{2}$$

In this book we will largely we dealing with qubits, which are supported by two basis states, $|0\rangle$ and $|1\rangle$, and can therefore be written as,

$$\begin{aligned} |\psi\rangle &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \alpha |0\rangle + \beta |1\rangle . \end{aligned} \tag{3}$$

Also useful is the *dual* of a state vector, which is simply the complex conjugate transpose (†) of the vector, capturing the same information about the state in conjugate form),

$$\begin{aligned} \langle\psi| &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger \\ &= (\alpha^*, \beta^*) \\ &= \alpha^* \langle 0| + \beta^* \langle 1| . \end{aligned} \tag{4}$$

For two generic state vectors,

$$\begin{aligned} |\psi\rangle &= \sum_n \alpha_n |n\rangle , \\ |\phi\rangle &= \sum_n \beta_n |n\rangle , \end{aligned} \tag{5}$$

the *overlap* between them is defined as,

$$\langle\psi|\phi\rangle = \sum_n \alpha_n \beta_n^*, \tag{6}$$

which is mathematically equivalent to their vector dot product. This quantity has the useful intuitive interpretation as the *distinguishability* between quantum states, which plays an important role in measurement theory and the theory of quantum information. Thus, the normalisation condition from Eq. (2) can equivalently be written,

$$\langle\psi|\psi\rangle = 1. \tag{7}$$

Because basis states are orthonormal, this implies that for basis states $|m\rangle$ and $|n\rangle$ we have the trivial identity,

$$\langle m|n\rangle = \delta_{m,n}. \tag{8}$$

B. Composite systems

The joint state vector of a multi-partite system is represented using a tensor (or Kronecker) product Hilbert space, which has dimensionality equal to the product of their individual dimensions, hence yielding the dreaded (cherished) exponential growth in the complexity of quantum systems,

$$\mathcal{H}_{A,B} = \mathcal{H}_A \otimes \mathcal{H}_B, \tag{9}$$

where,

$$\begin{aligned} \mathcal{H}_A &\in \mathbb{C}^M, \\ \mathcal{H}_B &\in \mathbb{C}^N, \\ \mathcal{H}_{A,B} &\in \mathbb{C}^{MN}. \end{aligned} \tag{10}$$

The state vector of two independent subsystems is simply given by their tensor product[1],

$$\begin{aligned} |\psi\rangle_{A,B} &= |\psi\rangle_A \otimes |\phi\rangle_B \\ &= \sum_{m,n} \alpha_m \beta_n |m\rangle \otimes |n\rangle . \end{aligned} \tag{11}$$

This is a so-called *separable* state, since the state vector can be factorised into independent terms characterising

————

[1] Often the $\otimes$ symbol is omitted for brevity and left implicit.

each of the subsystems. However, more generally we may have,

$$|\psi\rangle_{A,B} = \sum_{m,n} \lambda_{m,n} |m\rangle \otimes |n\rangle. \qquad (12)$$

where in general, $\lambda_{m,n}$ may not be separable as $\lambda_{m,n} = \alpha_m \beta_n$. In this case no physical description exists for either subsystem in isolation, which may only be described collectively. Now the state is said to be *entangled*, a uniquely quantum class of quantum states with no classical analogue. The best-known example is the *Bell state*,

$$|\psi\rangle_{A,B} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$
$$= \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B). \qquad (13)$$

It is obvious upon inspection that this state cannot be written in separable form as $|\psi\rangle_{A,B} = |\psi\rangle_A \otimes |\phi\rangle_B$, and is hence entangled. Entanglement is one of the key unique features of quantum physics, which underpins the operation of most quantum information processing protocols, including quantum computing in particular, where extremely complex many-particle entanglement is present and exploited for computational advantage.

C. Density operators

The state vector formalism presented above applies to *pure states*, i.e ones which are exhibit perfect quantum coherence (i.e superposition), and no classical randomness. But realistic physical systems combine both classical probabilities *and* quantum superposition amplitudes. To capture both of these features simultaneously we employ *density operators*. For an N-dimensional Hilbert space, the density operator, $\hat{\rho}$, is an $N \times N$ complex Hermitian matrix,

$$\hat{\rho} = \hat{\rho}^\dagger, \qquad (14)$$

which satisfies,

$$\text{tr}(\hat{\rho}) = \sum_i \hat{\rho}_{i,i} = 1, \qquad (15)$$

for normalisation.

Thus, in the special case of a qubit, density operators are 2×2 complex matrices,

$$\hat{\rho} = \begin{pmatrix} a & c \\ c^* & b \end{pmatrix},$$

where diagonal elements are necessarily real, and off-diagonal ones may be complex.

The intuitive physical interpretation of density matrices is as follows. Diagonal elements represent the classical probabilities of the respective basis states. Off-diagonal elements represent *coherences* between basis states, i.e whether they exist as a classical probability distribution (when the coherence is zero) or as a quantum superposition (when non-zero).

The density operator captures all information (classical and quantum) that can be known about a physical system under the standard laws of quantum physics, and is therefore a very powerful representation to employ.

For a pure state (a qubit in this example), the density operator takes the form,

$$\hat{\rho} = |\psi\rangle \langle\psi|$$
$$= \begin{pmatrix} |\alpha|^2 & \alpha\beta \\ \alpha^*\beta^* & |\beta|^2 \end{pmatrix}.$$

A classical mixture of quantum states $\hat{\rho}_i$ with probability distribution p_i takes the form,

$$\hat{\rho} = \sum_i p_i \hat{\rho}_i, \qquad (16)$$

where the probabilities are normalised such that,

$$\sum_i p_i = 1. \qquad (17)$$

An important measure on density operators is their *purity*, which quantifies to what extent the system is coherent (i.e *not* probabilistic),

$$\mathcal{P} = \text{tr}(\hat{\rho}^2), \qquad (18)$$

where,

$$\frac{1}{N} \leq \mathcal{P} \leq 1, \qquad (19)$$

and $\mathcal{P} = 1$ only for pure states.

D. Reduced states

Suppose there exists a bipartite system, to which we only have access to one subsystem. Since in general quantum states are not always separable, we now necessarily have an incomplete physical description of what we have access to. This physical description is obtained by taking the *partial trace* of the joint system, tracing out the subsystem to which we don't have access,

$$\hat{\rho}_A = \text{tr}_B(\hat{\rho}_{A,B}). \qquad (20)$$

$\hat{\rho}_A$ is referred to as the *reduced state* of system A.

The partial trace is a linear operator defined as,

$$\text{tr}_B(\hat{\rho}_A \otimes \hat{\rho}_B) = \text{tr}(\hat{\rho}_B) \cdot \hat{\rho}_A,$$
$$\text{tr}_B(\hat{\rho} + \hat{\sigma}) = \text{tr}_B(\hat{\rho}) + \text{tr}_B(\hat{\sigma}). \qquad (21)$$

From the cyclic property of the trace, it follows that,

$$\operatorname{tr}(|\psi\rangle\langle\phi|) = \langle\psi|\phi\rangle. \tag{22}$$

A useful property of the reduced state of larger pure state is that its purity characterises how entangled that subsystem is with the peripheral system. For example, a joint system which is separable and pure exhibit reduced states which are also pure. But the reduced state of an entangled state, such as that shown in Eq. (13), is necessarily mixed. Thus the purity $\mathcal{P}$ of the reduced states of a joint system may be used as a metric for quantifying the degree of entanglement in the system. This provides an extremely important link between entanglement and decoherence – the loss of coherence in an observed quantum system can always be attributed to it becoming entangled to the external environment, to which we don't have access.

III. EVOLUTION

Thus far we have only provided a description for the state of quantum systems. What about their evolution? In quantum mechanics the evolution of an N-dimensional state is given by arbitrary $N \times N$-dimensional unitary transformations, $\mathrm{U}(N)$, which satisfy,

$$\hat{U}^\dagger \hat{U} = \hat{\mathbb{1}}. \tag{23}$$

Intuitively, this corresponds to the class of higher-dimensional complex rotations that preserve the orthonormality of quantum states. In principle, any unitary operator is physically allowed, although most are challenging to artificially engineer!

The evolution of quantum state vectors under unitary transformation is simply given by matrix multiplication,

$$|\psi'\rangle = \hat{U}|\psi\rangle, \tag{24}$$

or for density operators by conjugation,

$$\hat{\rho}' = \hat{U}\hat{\rho}\hat{U}^\dagger. \tag{25}$$

This provides, a discrete-time description for the evolution of quantum states. Sometimes an alternate continuous-time description is employ. Here the system is governed by a Hamiltonian, $\hat{H}$, the quantum analogue of a classical Hamiltonian, which relates to unitary evolution via,

$$\hat{U} = e^{-i\hat{H}t}, \tag{26}$$

over evolution time t.

IV. MEASUREMENT

The final ingredient in our toolbox of allowed quantum operations is measurement. After all, what use is a quantum protocol if we can't read out the answer?

So-called *projective measurement* in quantum mechanics are described by sets of *measurement projectors*,

$$\hat{M}_i = |m_i\rangle\langle m_i|, \tag{27}$$

where,

$$\sum_i \hat{M}_i = \hat{\mathbb{1}}. \tag{28}$$

Each projector in the set corresponds to a possible allowed measurement outcome. After measuring a given outcome the state is disturbed and collapses (i.e *projected*) into being in the state corresponding to the measurement outcome. If the set of projectors corresponds to the eigenbasis of some unitary operator $\hat{U}$, we can say that the measurement is performed in the $\hat{U}$-basis.

Importantly, and this is a key feature of quantum mechanics, we cannot control what the measurement outcome is. It occurs randomly according to some classical probability distribution, given by the overlaps between the projectors and the quantum state.

The set of possible projected states following measurement is given by,

$$|\psi_i\rangle = \frac{\hat{M}_i|\psi\rangle}{\sqrt{p_i}},$$
$$\hat{\rho}_i = \frac{\hat{M}_i\hat{\rho}\hat{M}_i^\dagger}{p_i}, \tag{29}$$

where those outcomes occur with probabilities,

$$p_i = \langle\psi|\hat{M}_i^\dagger\hat{M}_i|\psi\rangle,$$
$$p_i = \operatorname{tr}(\hat{M}_i\hat{\rho}\hat{M}_i^\dagger). \tag{30}$$

More general classes of measurements are allowed, given by measurement operators $\hat{M}_i$ comprised of linear combinations of projectors. The same rules above for the action of these measurement operators apply, Eqs. (29, 30).

As a simple example, consider the superposition state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{31}$$

Now we have,

$$p_0 = |\langle 0|\psi\rangle|^2 = \frac{1}{2},$$
$$p_1 = |\langle 1|\psi\rangle|^2 = \frac{1}{2}, \tag{32}$$

and,

$$|\psi_0\rangle = \sqrt{2}|0\rangle\langle 0|\psi\rangle = |0\rangle,$$
$$|\psi_1\rangle = \sqrt{2}|1\rangle\langle 1|\psi\rangle = |1\rangle. \tag{33}$$

Thus, we see that with 50:50 probability the measurement randomly collapses the measured state onto the $|0\rangle$ or $|1\rangle$ states.