Chapter 2 Quantum Mechanics: Hilbert Space Formalism.

Quantum Information Science uses quantum properties to help store, process, and transmit information. In this chapter, we describe some basic background on quantum mechanics. We first use vector states to describe quantum systems. Then we demonstrate the formulation using density matrices.

Copenhagen interpretation

A1 A vector state $|x\rangle$ is a unit vector in a Hilbert space $\mathcal{H}$ (usually $\mathbb{C}^n$). Linear combinations (superposition) of the physical states are allowed in the state space.

A2 An observable of a state $|x\rangle$ corresponds to a Hermitian operators A such that a measurement will change the state $|x\rangle$ to an eigenstate (eigenvector) $|u\rangle$ of A with a probability $|\langle u|x\rangle|^2$.

In the finite dimensional case, suppose the observable and the state are represented by

$$A = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| = \sum_{j=1}^{n} \lambda_j P_j,$$

and

$$|x\rangle = \sum_{j=1}^{n} c_j |u_j\rangle \in \mathbb{C}^n \quad \text{with} \quad c_j = \langle u_j|x\rangle.$$

When a measurement is applied, the state (wave function) $|x\rangle = \sum_{j=1}^{n} c_j |u_j\rangle$ becomes (**collapses** to) $|u_j\rangle$ with a probability $|c_j|^2 = |\langle u_j|x\rangle|^2$. (The eigenvalue λ_j indicates that $|x\rangle$ changes to $|u_j\rangle$.)

The complex coefficients $c_1, \ldots, c_n$ are called the probability amplitude of the state $|x\rangle$ (with respect to the observable associated with A).

A3 The time dependence of a state is governed by the Schrödinger equation

$$i\hbar\frac{d|x\rangle}{dt} = H|x\rangle,$$

where $\hbar$ is the Planck constant with

$$\hbar = 6.6260700410^{-34}m^2kg/s,$$

and H is a Hermitian operator (matrix) corresponding to the energy of the system known as the Hamiltonian. In the Schrödinger equation, if $H(t)$ does not depend on t, then

$$|x(t)\rangle = e^{-iHt/\hbar}|x(0)\rangle.$$

Otherwise,

$$|x(t)\rangle = \exp\left(\frac{-i}{\hbar}\int_0^t H(s)ds\right)|x(0)\rangle.$$

It is inspiring to think about the 1×1 case. We can solve

$x'(t) = kx(t)$ so that $x(t) = e^k x(0)$.

Remark One may regard $|x(0)\rangle$ changes because the Hamiltonian $H(t)$ changes according to time. This is known as the Heisenberg picture of quantum mechanics. One may also assume that the state $|x(t)\rangle$ is changing according to time. This is known as the Schrödinger picture.

Example If

$$H = \frac{-\hbar}{2} w\sigma_x \quad \text{and} \quad |\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{so that} \quad i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle,$$

then

$$\begin{aligned} |\psi(t)\rangle &= ((\cos wt/2)I_2 + (i\sin wt/2)\sigma_x)|\psi(0)\rangle \\ &= [(\cos wt/2)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + i\sin wt/2)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}]|\psi(0)\rangle \\ &= \begin{pmatrix} \cos wt/2 \\ i\sin wt/2 \end{pmatrix}. \end{aligned}$$

If we apply the observable $A = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$, then the measurement $|\psi(t)\rangle$ will collapse to $|e_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|e_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ with probabilities $|\langle e_1|u_1\rangle|^2 = \cos^2(wt/2)$ and $|\langle e_2|u_1\rangle|^2 = \sin^2(wt/2)$, respectively.

If we apply the observable $A = 3P_1 + 2P_2$ with $P_1 = |u_1\rangle\langle u_1|$ and $P_2 = |u_2\rangle\langle u_2|$ with $|u_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$ and $|u_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$, then the measurement $|\psi(t)\rangle$ will collapse to $|u_1\rangle$ and $|u_2\rangle$ with probabilities

$$|\langle u_1|\psi(t)\rangle|^2 = \frac{1}{2}|(1,-i)(\cos(wt/2), i\sin(wt/2)^t|^2$$

$$= (\cos(wt/2) + \sin(wt/2))^2/2$$

and

$$|\langle u_2|\psi(t)\rangle|^2 = \frac{1}{2}|(1,i)(\cos(wt/2), i\sin(wt/2)^t|^2$$

$$= (\cos(wt/2) - \sin(wt/2))^2/2.$$

The uncertainty principle

Let $\text{Exp}_x(A) = \langle x|A|x\rangle = \mu$ and $\text{Var}_x(A) = \text{Exp}_x((A-\mu I)^2) = \langle x|(A-\mu I)^2|x\rangle = \|(A-\mu I)|x\rangle\|^2$.

In an deterministic model, the variance of measurements should go to zero as the apparatus is made very accurate.

Theorem For any observables A and B and for any quantum state $|x\rangle$, if $[A,B] = AB - BA$ is the commutator of A and B, and

$$\Delta(A) = \sqrt{\text{Var}_x(A)} = \sqrt{\langle x|(A-\alpha I)^2|x\rangle},$$

where $\alpha = \langle x|A|\rangle$ is the expectation value, then

$$\Delta(A)\Delta(B) \geq \frac{1}{2}|\langle x|[A,B]|x\rangle|.$$

The equality holds if and only if there is $\theta \in [0, 2\pi)$ such that

$$\cos\theta A|x\rangle + i\sin\theta B|x\rangle = 0.$$

Proof. Let $\hat{A} = A - \alpha I$ and $\hat{B} = B - \beta I$. Note first that $\Delta(A)\Delta(B) = \sqrt{\langle\psi|\hat{A}^2|\psi\rangle}\sqrt{\langle\psi|\hat{B}^2|\psi\rangle}$ and $\langle\psi|[A,B]|\psi\rangle = \langle\psi|[\hat{A},\hat{B}]|\psi\rangle$. So, we need to show that $4\langle\psi|\hat{A}^2|\psi\rangle\langle\psi|\hat{B}^2|\psi\rangle \geq |\langle\psi|[\hat{A},\hat{B}]|\psi\rangle|^2$. Note that the matrices

$$C_1 = \begin{pmatrix} \langle\psi|\hat{A}^2|\psi\rangle & \langle\psi|\hat{A}\hat{B}|\psi\rangle \\ \langle\psi|\hat{B}\hat{A}|\psi\rangle & \langle\psi|\hat{B}^2|\psi\rangle \end{pmatrix} \text{ and } C_2 = \begin{pmatrix} \langle\psi|\hat{A}^2|\psi\rangle & -\langle\psi|\hat{B}\hat{A}|\psi\rangle \\ -\langle\psi|\hat{A}\hat{B}|\psi\rangle & \langle\psi|\hat{B}^2|\psi\rangle \end{pmatrix}$$

are positive semi-definite as proved by checking that all their principal minors are nonnegative using the Cauchy-Schwartz inequality. Thus, $C = C_1 + C_2$ is positive semi-definite and

$$4\langle\psi|\hat{A}^2|\psi\rangle\langle\psi|\hat{B}^2|\psi\rangle - |\langle\psi|[\hat{A},\hat{B}]|\psi\rangle|^2 = \det(C) \geq 0.$$

The equality $\det(C) = 0$ holds if and only if C is singular, equivalently, the positive semi-definite matrices C_1 and C_2 are singular and share a common null vector. Since C_1 and C_2 have the same trace, we see that

(1) $C_1 = C_2 = (\mathrm{tr}\ C_1)|u\rangle\langle u|$ for some unit vector $|u\rangle \in \mathbb{C}^n$, and

(2) $\langle\psi|\hat{A}\hat{B}|\psi\rangle = -\langle\psi|\hat{B}\hat{A}|\psi\rangle$, i.e., $\langle\psi|\{\hat{A},\hat{B}\}|\psi\rangle = 0$.

Condition (1) implies $\det(C_1) = 0$, namely $\langle\psi|\hat{A}^2|\psi\rangle\langle\psi|\hat{B}^2|\psi\rangle = |\langle\psi|\hat{A}\hat{B}|\psi\rangle|^2$. By the Cauchy-Schwartz inequality, $\hat{A}|\psi\rangle$ and $\hat{B}|\psi\rangle$ are linearly dependent. Condition (2) implies that $\langle\psi|\hat{A}\hat{B}|\psi\rangle \in i\mathbb{R}$. So, $\hat{A}|\psi\rangle$ and $i\hat{B}|\psi\rangle$ are linearly dependent over $\mathbb{R}$. Thus, there is $\theta \in [0, 2\pi)$ such that $\cos\theta\hat{A}|\psi\rangle + i\sin\theta\hat{B}|\psi\rangle$ is the zero vector. Conversely, if $\cos\theta\hat{A}|\psi\rangle + i\sin\theta\hat{B}|\psi\rangle$ is the zero vector, one readily checks that $C_1 = C_2$ and $\det(C_1 + C_2) = 0$. □

Example It is known that $[P,Q] = i\alpha\hbar I$ for quantities such as position and momentum operator, where α is a constant. Then

$$\Delta(P)^2\Delta(Q)^2 \geq |\alpha\hbar|.$$

Note that such examples only exists for infinite dimensional operators because of $\mathrm{tr}\,(AB - BA) = 0$ for matrices.

Bipartite and multipartite systems

A system may have two components described by two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. Then the bipartite system is represented by $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. A general state in $\mathcal{H}$ has the form

$$|x\rangle = \sum_{i,j} c_{ij} |e_{1,i}\rangle \otimes |e_{2,j}\rangle \quad \text{with} \sum_{i,j} |c_{ij}|^2 = 1,$$

where $\{|e_{r,1}\rangle, |e_{r,2}\rangle, \dots\}$ is an orthonormal basis for $\mathcal{H}_r$ with $r \in \{1, 2\}$.

Then $\{|e_{1,i} e_{2,j}\rangle : i = 1, 2, \dots, j = 1, 2, \dots\}$ is an orthonrmal basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Example For example, $\mathbb{C}^2$ has orthonormal basis $\{|0\rangle, |1\rangle\}$ with

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Then $\mathbb{C}^2 \otimes \mathbb{C}^2$ has orthonormal basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ consisting of the 4 columns of the identity matrix I_4.

Similarly, $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ has orthonormal basis $\{|000\rangle, \dots, |111\rangle\}$ consisting of the columns of I_8.

In general, if $U = [|u_1\rangle \cdots |u_m\rangle]$ such that the columns of U form an orthonormal basis for $\mathbb{C}^m$, and $V = [|v_1\rangle \cdots |v_n\rangle]$ such that the columns of V form an orthonormal basis for $\mathbb{C}^n$, then the columns of $U \otimes V = [|u_1 v_1\rangle \cdots |u_m v_n\rangle]$ form an orthonormal basis for $\mathbb{C}^m \otimes \mathbb{C}^n$.

Separable states, entangled states, Schmidt decomposition

A state of the form $|x\rangle = |x_1\rangle \otimes |x_2\rangle$ is a **separable state** or a **tensor product state**. Otherwise, it is an **entangled state**.
Example Let

$$|x\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} \in \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Question How to detect that it is a tensor state?

Answer Check whether the rows of the matrix $C = \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}$ are multiples of each other. If yes, we can write $C = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} (b_1 \ b_2)^t$ for some unit vectors $|u\rangle = (a_1, a_2)^t, |v\rangle = (b_1, b_2)^t$. Then $|x\rangle = |u\rangle \otimes |v\rangle$. If not, $|x\rangle$ is entangled.

Remark Most states in $\mathcal{H}_1 \otimes \mathcal{H}_2$ are entangled states, which are most useful for quantum computing.

Theorem Suppose $\mathcal{H}_1, \mathcal{H}_2$ have finite dimensions, say, m and n. Every state $|x\rangle$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ admits a **Schmidt decomposition**

$$|x\rangle = \sum_{j=1}^{r} s_j |u_j\rangle \otimes |v_j\rangle,$$

where $s_j > 0$ are the Schmidt coefficients satisfying $\sum_{j=1}^{r} s_j^2 = 1$, r is the **Schmidt number** of $|x\rangle$, $\{|u_1\rangle, \ldots, |u_r\rangle\}$ is an orthonormal set of $\mathcal{H}_1$ and $\{|v_1\rangle, \ldots, |v_r\rangle\}$ is an orthonormal set of $\mathcal{H}_2$.

Proof. Assume $\mathcal{H}_1$ and $\mathcal{H}_2$ orthonormal bases $\{|e_{1,1}, \ldots, |e_{1,m}\rangle\}$ and $\{|e_{2,1}, \ldots, |e_{2,n}\rangle\}$. Every state has the form

$$|x\rangle = \sum_{j=1} c_{rs} |e_{1,r}\rangle \otimes |e_{2,s}\rangle.$$

If C has rank one, then $C = (a_1, \ldots, a_m)^t (b_1, \ldots, b_n)$ so that $C = |u\rangle \otimes |v\rangle$ with $|u\rangle = \sum_{j=1}^{m} a_j |e_{1,j}\rangle$ and $|v\rangle = \sum_{j=1}^{n} b_j^* |e_{2,j}\rangle$. Because $\||x\rangle\| = 1$, we may assume that $(a_1, \ldots, a_m)^t$ and $(b_1, \ldots, b_n)^t$ are unit vectors and so are $|u\rangle, |v\rangle$.

In general, suppose $C = [c_{ij}]$ has singular decomposition

$$\sum_{j=1}^{r} s_j |\alpha_j\rangle\langle|\beta_j| = \sum_{j=1}^{r} s_j C_j,$$

where $C_j = |\alpha_j\rangle\langle\beta_j|$ for $j = 1, \ldots, r$.

One can then use C_j as the coefficient matrix of $|x_j\rangle$ to construct tensor state $|x_j\rangle = |u_j\rangle \otimes |v_j\rangle$ so that

$$|x\rangle = \sum_{j=1}^{r} s_j |x_j\rangle = \sum_{j=1}^{r} s_j |u_j\rangle \otimes |v_j\rangle. \qquad \square$$

Example Suppose $|x\rangle = \sum_{i,j} c_{ij}|e_{1,i}e_{2,j}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^3$ with

$$(c_{ij}) = UDV^t = d_1|u_1\rangle\langle v_1| + d_2|u_2\rangle\langle v_2|,$$

where

$$U = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \quad D = \tfrac{1}{5}\begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}, \quad V = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & \sqrt{2} & 0 \end{pmatrix}.$$

Then

$$|x\rangle = \frac{4}{5}|u_1\rangle|v_1\rangle + \frac{3}{5}|u_2\rangle|v_2\rangle,$$

where

$$|u_1\rangle = (1, i)^t/\sqrt{2},\ |u_2\rangle = (1, -i)^t/\sqrt{2},$$
$$|v_1\rangle = (1, 1, 0)^t/\sqrt{2},\ |v_2\rangle = (0, 0, 1)^t.$$

Remark Extending the results to $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$ for $k \geq 3$ is an open problem.

No-cloning theorem

Theorem (Wootters and Zurek) An unknown quantum system cannot be cloned by unitary transformations.

Proof. Suppose there would exist a unitary transformation U that makes a clone of a quantum system. Namely, suppose U acts, for any state $|\varphi\rangle$, as

$$U : |\varphi 0\rangle \to |\varphi\varphi\rangle.$$

Let $|\varphi\rangle$ and $|\phi\rangle$ be two states that are linearly independent. Then we should have $U|\varphi 0\rangle = |\varphi\varphi\rangle$ and $U|\phi 0\rangle = |\phi\phi\rangle$ by definition. Then the action of U on $|\psi\rangle = \frac{1}{\sqrt{2}}(|\varphi\rangle + |\phi\rangle)$ yields

$$U|\psi 0\rangle = \frac{1}{\sqrt{2}}(U|\varphi 0\rangle + U|\phi 0\rangle) = \frac{1}{\sqrt{2}}(|\varphi\varphi\rangle + |\phi\phi\rangle).$$

If U were a cloning transformation, we must also have

$$U|\psi 0\rangle = |\psi\psi\rangle = \frac{1}{2}(|\varphi\varphi\rangle + |\varphi\phi\rangle + |\phi\varphi\rangle + |\phi\phi\rangle),$$

which contradicts the previous result. Therefore, there does not exist a unitary cloning transformation. □

Remark There is proof using the fact that information cannot be transmitted faster than light speed. See the supplementary note.

Qubits

- Mathematically, qubit is a vector in $|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ with $|a|^2 + |b|^2$ realized by physical quantum states such as the vertically and horizontally polarized photons, or spin 1/2 in NMR system.

- Note that measurement will give $|0\rangle$ or $|1\rangle$ even a qubit can assume infinitely many states. The probability for the measurement on $|x\rangle$ yielding $|0\rangle$ is $\langle x|(|0\rangle\langle 0|)|x\rangle = |a|^2$.

- Even if we can get the information $|a|$ and $|b|$ by **measuring** many identical $|x\rangle$ if it is available, we cannot get complete information of $|x\rangle\langle x|$.

- Using the measurable states $P_1 = |0\rangle\langle 0|, P_2 = |1\rangle\langle 1|$ to get information of $\langle x|P_1 x\rangle, \langle x|P_2 x\rangle$, we have the "diagonal entries" of $\rho = |x\rangle\langle x|$, which are $|a|^2, |b|^2$.

- In order to obtain complete information of $|x\rangle\langle x|$, we may apply unitary $U_1, \ldots, U_r$ and measure the diagonal $U_j|x\rangle\langle x|U_j^\dagger$ to access information of the off-diagonal entries. Such study is known as **state tomography** problem.

One may consider qutrits in $\mathbb{C}^3$ and qudits in $\mathbb{C}^n$.

Bloch sphere and Bloch ball

Since two unit vectors $|x\rangle$ and $e^{it}|x\rangle$ represent the same quantum state, it is convenient to use the rank one orthogonal projection $\rho = |x\rangle\langle x|$, which will be called a pure state, to represent the state.

More generally, one may consider the mixed state $\rho \in M_n$ of the form

$$\sum_{j=1}^{r} p_r |x_j\rangle\langle x_j|$$

with probability vector $(p_1, \ldots, p_r)$ and pure states $|x_1\rangle\langle x_1|, \ldots, |x_r\rangle\langle x_r|$.

For qubits, a mixed state has the form

$$\rho = \frac{1}{2}(I_2 + u \cdot \sigma) = \frac{1}{2}(\sigma_0 + u_1\sigma_1 + u_2\sigma_2 + u_3\sigma_3)$$

with $|u| = \sqrt{u_1^2 + u_2^2 + u_3^2} \leq 1$.

Here $(\sigma_1, \sigma_2, \sigma_3) = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices"

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- The eigenvalues of ρ are $\frac{1}{2}(1 \pm |u|)$.
- ρ is a pure state if and only if $|u| = 1$.
- In such a case, we may let

$$u = (u_1, u_2, u_3) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta).$$

Multi-qubit systems and entangled states

Given n qubits $|x_1\rangle, \ldots, |x_n\rangle$, we can consider the tensor product $|x_1\rangle \otimes \cdots \otimes |x_n\rangle \in \mathbb{C}^N$ with $N = 2^n$. Most state vectors

$$\sum_{i_k=0,1} a_{i_1 \cdots i_n} |x_{i_1}\rangle \otimes \cdots \otimes |x_{i_n}\rangle \in \mathbb{C}^N$$

are entangled state vectors, which are not of the tensor form.

Notation We often assume $|x_j\rangle \in \{|0\rangle, |1\rangle\}$, and regard

$$|x\rangle = |x_{i_1} \cdots x_{i_n}\rangle = |q_{n-1} \cdots q_0\rangle$$

as a binary number, and

$$|\psi\rangle = \sum_{i_k=0,1} a_{i_1 \cdots i_n} |x_{i_1} \cdots x_{i_n}\rangle.$$

Example

$$|x\rangle = \frac{1}{2} \sum_{i,j \in \{0,1\}} |ij\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2} \sum_{x=0}^{3} |x\rangle.$$

In quantum computing, we often implement quantum operation of the form:

$$\sum_x |x\rangle|0\rangle \mapsto \sum_x |x\rangle|f(x)\rangle.$$

For example, if $f(0) = f(1) = 1$, there is U such that

$$U|00\rangle = |01\rangle, \quad U|10\rangle = |11\rangle.$$

There are many choices for U. For example, we may set $U|01\rangle = |00\rangle, U|11\rangle = |10\rangle$.

Some important entangled states

Example The Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

are entangled states and form an orthonormal basis for the two qubit systems.

Example In the 3 qubit system, we have that GHZ state and W state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad \text{and} \quad |W\rangle \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle).$$

Example One can do measurement of the first qubit for a state vector in a n qubit system. For instance,

$$|x\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1.$$

We measure the first qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. Set

$$|x\rangle = |0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(c|0\rangle + d|1\rangle)$$

$$= u|0\rangle((a/u)|0\rangle + (b/u)|1\rangle) + v|1\rangle((c/v)|0\rangle + (d/v)|1\rangle),$$

where $u = \sqrt{|a|^2 + |b|^2}$ and $v = \sqrt{|c|^2 + |d|^2}$. We can measure the first qubit, say, by setting $A = (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes I_2$ so that

$$M_0 = |0\rangle\langle 0| \otimes I_2, \quad M_1 = |1\rangle\langle 1| \otimes I_2.$$

Applying M_0 and M_1, we obtain 0 with probability $\langle x|M_0|x\rangle = u^2$ and 1 with probability v^2; the state $|x\rangle$ collapses to

$$|0\rangle \otimes ((a/u)|0\rangle + (b/u)|1\rangle) \text{ and } |1\rangle \otimes ((c/v)|0\rangle + (d/v)|1\rangle), \text{ r}$$

espectively, upon measurement.

Einstein-Podolsky-Rosen (EPR) Phenomenon

- Consider the EPR state
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$
Alice gets the first particle and Bob gets the second one.

- When Alice measures, Bob's particle will change instantaneously to $|1\rangle$ or $|0\rangle$ depending on the measured outcome of Alice being $|0\rangle$ or $|1\rangle$.

- For example, set up the apparatus for the observable
$$A = |0\rangle\langle 0| \otimes I_2 - |1\rangle\langle 1| \otimes I_2.$$

- If Alice sees the reading 1, then Bob's qubit is to $|1\rangle$; if Alice sees the reading -1, then Bob's qubit is $|0\rangle$.

- Alice cannot control her measurement and hence the reading of Bob! So, it does not violate the special theory of relativity. (It is impossible that information travels faster than light!)

- However, they can measure their individual states around the same time, and decide to make a move according to $|01\rangle$ or $|10\rangle$ occur.

- Bell proposed an experiment which confirmed that there cannot be a hidden rule governing the measurement of the entangled pair.

Measurements

For each outcome m, construct a measurement operator M_m so that the probability of obtaining outcome m in the state $|x\rangle$ is computed by

$$p(m) = \langle x|M_m^\dagger M_m|x\rangle$$

and the state immediately after the measurement is

$$|m\rangle = \frac{M_m|x\rangle}{\sqrt{p(m)}}.$$

Example Let $M = \{M_0, M_1\}$ with $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Then for $|x\rangle = a|0\rangle + b|1\rangle$ with $a \neq 0$, $p(0) = |a|^2$, $M_0|x\rangle = a|0\rangle/|a|$, which is the same as the vector state $|0\rangle$.

- In general, suppose an observable M is given with measurement operators M_m. Then setting $P_i = M_i^\dagger M_i$, we require that $\sum_m P_m = I_n$.
- If there are many copy of a state $|x\rangle$, then the expected value of M is

  $$E(M) = \langle M\rangle = \sum_m mp(m) = \sum_m m\langle x|P_m|x\rangle = \langle x|M|x\rangle.$$

  Here M can be identified with $\sum_m mP_m$.
- The standard derivation is

  $$\Delta(M) = \sqrt{\langle(M - \langle M\rangle)^2} = \sqrt{\langle M^2\rangle - \langle M\rangle^2}.$$

- The variance (square of standard deviation) is

  $$\langle(M - \langle M\rangle)^2\rangle = \langle x|M^2|x\rangle - \langle x|M|x\rangle^2.$$

Another proof of no-cloning theorem

The no-cloning theorem may be proved by using the special theory of relativity, which assumes no information can propagate faster than the speed of light.

Suppose Alice and Bob share a Bell state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle).$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Readers are encouraged to verify the second equality. Alice keeps the first qubit while Bob keeps the second. If Alice wants to send Bob a bit "0", she measures her qubit in $\{|0\rangle, |1\rangle\}$ basis while if she wants to send "1", she employs $\{|+\rangle, |-\rangle\}$ basis for her measurement. Bob always measures his qubit in $\{|0\rangle, |1\rangle\}$ basis.

After Alice's measurment and before Bob's measurment, Bob's qubit is $|0\rangle$ or $|1\rangle$ if Alice sent "0" while it is $|+\rangle$ or $|-\rangle$ if Alice sent "1".

Suppose Bob is able to clone his qubit. He makes many copies of his qubit and measures them in $\{|0\rangle, |1\rangle\}$ basis. If Alice sent "0", Bob will obtain $0, 0, 0, \ldots$ or $1, 1, 1, \ldots$ while if she sent "1", Bob will obtain approximately 50% of 0's and 50% of 1's. Suppose Bob received $|\pm\rangle$ and made N clones, then the probability of obtaining the same outcome is $1/2^{N-1}$, which is negligible if N is sufficiently large. Note that Bob obtains the bit Alice wanted to send immediately after Alice's measurement assuming it does not take long to clone his qubit. This could happen even if Alice and Bob are separated many light years apart, thus in contradiction with the special theory of relativity. $\square$