Summary of Chapter 2 of Nielsen and Chuang's book: Quantum Computation and Quantum Information

Sofia Tarricone

GT Quantique

IPhT, 10 Janvier 2023

Chapter 2: introduction to quantum mechanics

Outline

$\#1$: state space and state vector

Postulate 1

"Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space."

Example The simplest quantum mechanical system (and the system which is most used in the book) is the qubit.
A qubit has a two dimensional state space with $|0\rangle$, $|1\rangle$ forming an orthonormal basis for that state space, so that the arbitrary state vector has the form

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

with $|a|^2 + |b|^2 = 1$.

Remark For real physical systems described in terms of qubits $\rightarrow$ Chapter 7.

#2 : dynamics

Postulate 2 (discrete time)

"The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by

$$|\psi'\rangle = U|\psi\rangle.$$

where U is a unitary operator (i.e. $UU^\dagger = U^\dagger U = I$) which depends only on the times t_1 and t_2."

Example For the qubit, examples of U are X the bit flip, Z the phase flip, Y and H the Hadamard gate.

Postulate 2' (continuous time)

"The time evolution of the state of a closed quantum system is described by the Schrödinger equation

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

where $\hbar$ is a constant (for us fixed to 1) and H is a fixed Hermitian operator (i.e. $H = H^\dagger$) known as the Hamiltonian of the closed system."

Remark Solving Schrödinger equation $|\psi(t_2)\rangle = \exp(-iH(t_2 - t_1))|\psi(t_1)\rangle$.

#3 : measurements

Postulate 3

"Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the state space of the system being measured, where m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \text{ probability that } m \text{ occurs}$$

and the state after the measurement is $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$. The measurement operators satisfy the completeness equation $\sum_m M_m^\dagger M_m = I$, which expresses the fact that probabilities has to sum up to 1."

Example Measurement of a qubit in the computational basis is done by taking $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Then if the state before measurement is $|\psi\rangle = a|0\rangle + b|1\rangle$ one has

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2,\ p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = |b|^2,$$

and post-measurement states are respectively $\frac{a}{|a|}|0\rangle$ and $\frac{b}{|b|}|1\rangle$ (which are effectively just $|0\rangle$ and $|1\rangle$ since they differ only by a multiplier of modulus 1.)

Indistiguishability of non-orthogonal quantum states

Suppose $|\psi_i\rangle, i = 1, \ldots, n$ are orthonormal states. Then it is possible to distinguish them by using quantum measurements in the following way:

- construct $M_i = |\psi_i\rangle\langle\psi_i|$ for each $i = 1, \ldots, n$ and M_0 as the positive square root of the positive operator $I - \sum_i |\psi_i\rangle\langle\psi_i|$ (so that the collection $\{M_m\}_{m=0}^n$ satisfies the completeness equation).
- if the state $|\psi_i\rangle$ is prepared then

$$p(i) = \langle\psi_i|M_i|\psi_i\rangle = 1.$$

However non-orthogonal quantum states can't be reliably distinguished.

Projective measurement

Definition

A projective measurement is an observable M, i.e. Hermitian operator on the state space of the system being observed. It has a spectral decomposition

$$M = \sum_m mP_m$$

where P_m is the orthogonal projector onto the eigenspace of eigenvalue m which is the possible outcome of the observable. If $|\psi\rangle$ is prepared then

$$p(m) = \langle\psi|P_m|\psi\rangle = \text{ probability that m occurs}$$

and the state after measurement is $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

Remark Postulate 3 reduces to a projective measurement when we require the general measurement operators M_m to be orthogonal projectors : Hermitian operators such that $M_m M_{m'} = \delta_{m,m'} M_m$.

Example On a qubit, Z is a projective measurement which decomposes as $Z = +1P_1 - 1P_{-1}$ where $P_1 = |0\rangle\langle 0|$ and $P_{-1} = |1\rangle\langle 1|$.

Heisenberg uncertainty principle

- Average values of the observable M is given by

$$\langle M \rangle = \sum_m m p(m) = \sum_m m \langle \psi | P_m | \psi \rangle = \langle \psi | M | \psi \rangle.$$

- Standard deviation associated to observation of M is given by

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

- If C, D are two observable, $|\psi\rangle$ a quantum state, the Heisenberg uncertainty principle states that

$$\Delta(C)\Delta(D) \geq \frac{|\langle \psi | \left[C, D \right] | \psi \rangle|}{2}.$$

Positive Operator-Valued Measure

Definition

A POVM is defined as a collection of positive operators $\{E_m\}$ such that $\sum_m E_m = I$. Notice that $p(m) = \langle\psi|E_m|\psi\rangle$.

Example For a given collection $\{M_m\}$ of general measurements, one can define a POVM by taking the positive operators $E_m = M_m^\dagger M_m$.
For a projective measurement $M = \sum_m mP_m$ the POVM elements are $E_m = P_m$.

Why introducing general measurements then?

- General measurements are mathematically easier.
- Important problems in quantum computation/information need general measurements (e.g. optimal way to distinguish a set of quantum states).
- Projective measurements are *repeatable* in the sense that: for $|\psi\rangle$ being the initial state, if the outcome of the measure is m then the post-measurement state is $|\psi_m\rangle = P_m|\psi\rangle/\sqrt{p(m)}$ and applying again P_m does not change it, i.e. $\langle\psi_m|P_m|\psi_m\rangle = 1$. There are measurements which do not have this property.
- POVMs are best viewed as a special case of general measurements, providing the simplest means by which one can study general measurement statistics, without caring about post-measurement state.

$\#4$: composite systems

Postulate 4

"The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered $1, \ldots, n$*, and system number* i *is prepared in the state* $|\psi_i\rangle$*, the joint state of the total system is* $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$*."*

Remark Projective measurements and unitary dynamics together with Postulate 4 give general measurements (with properties as stated in Postulate 3).

- Construct an ancilla system with state space M and orthonormal basis in 1-1 correspondence with possible outcomes of the measurement $|m\rangle$.
- Define U on $Q \otimes |0\rangle$ (here $|0\rangle$ is any fixed state of M), as

$$U|\psi\rangle|0\rangle = \sum_m M_m|\psi\rangle|m\rangle.$$

  Then U preserves inner products between states of $Q \otimes |0\rangle$ and thus it can be extended to the all space $Q \otimes M$ as unitary operator.
- Consider the projective measurement on $Q \otimes M$ given by orthogonal projectors $P_m = I_Q \otimes |m\rangle\langle m|$ then one can obtain $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ and the post-measurement state of M will be $|m\rangle$ and of Q will be $M_m|\psi\rangle/\sqrt{p(m)}$.

Outline

Entangled states

Definition

A state of a composite system that can't be written as a product of states of its component systems is called an entangled state.

Example $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is an entangled state.

Indeed : suppose instead that there exist qubits $|a\rangle, |b\rangle$ such that $|\beta_{00}\rangle = |a\rangle|b\rangle$. Then by writing them in the computational basis

$$|a\rangle = a_0|0\rangle + a_1|1\rangle, \; |b\rangle = b_0|0\rangle + b_1|1\rangle.$$

we obtain

$$|\beta_{00}\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle.$$

Thus we should have

$$a_0 b_1 = 0, \; a_1 b_0 = 0, \; a_0 b_0 = \frac{1}{\sqrt{2}} = a_1 b_1$$

which gives the contraddiction.

Superdense Coding

The task

Alice wants to send two bits of classical information to Bob but she is only allowed to send a single qubit to him.

This can be accomplished by using the entangled state $|\beta_{00}\rangle$ and following this procedure.

- A third part prepares the Bell state $|\beta_{00}\rangle$ and sends to Alice the first qubit $|\psi_A\rangle = (|0_A\rangle + |1_A\rangle)/\sqrt{2}$ and to Bob the second one $|\psi_B\rangle = (|0_B\rangle + |1_B\rangle)/\sqrt{2}$.
- Before send her qubit to Bob, Alice performs a transformation in function of the message she wants Bob to receive:

$$00 \to I \to (|0\rangle + |1\rangle)/\sqrt{2}, \quad 01 \to X \to (|1\rangle + |0\rangle)/\sqrt{2},$$

$$10 \to Z \to (|0\rangle - |1\rangle)/\sqrt{2}, \quad 11 \to iY \to (-|1\rangle + |0\rangle)/\sqrt{2}$$

Alice sends...

Once Alice has sent her (transformed) qubit to Bob, he has in his hands one of the following resulting states

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\beta_{00}\rangle, \quad \frac{|10\rangle + |01\rangle}{\sqrt{2}} = |\beta_{01}\rangle$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\beta_{10}\rangle, \quad \frac{-|10\rangle + |01\rangle}{\sqrt{2}} = |\beta_{11}\rangle$$

which are exactly the four states of the Bell basis, which is an orthonormal basis for a two qubits space.
These states can then be distinguished by an appropriate quantum measurement. By doing a measurement in the Bell basis Bob can determine which of the four possible bit strings Alice sent.

Remark Notice that Alice never had to interact with the second qubit. If she only had the opportunity to transmit a single classical bit, the task would have been impossible to accomplish $\rightarrow$ Chapter 12.

...and Bob decodes

In other words, to decode the information that Alice sent, Bob can do the following

- apply a CNOT with control qubit being Alice's qubit and target qubit being his own qubit.
- on the result Bob applies then the transformation $H_1 I_2$ which gives him one of the four states of the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, that tells him which two bits information Alice wanted to send.

Example Suppose that Alice sent to Bob the qubit $(|0\rangle + |1\rangle)/\sqrt{2}$ (willing to send him the message 00) and so he has in his hands $|\beta_{00}\rangle$. Then

$$|\beta_{00}\rangle \xrightarrow{\text{CNOT}} |\beta'_{00}\rangle = (|00\rangle + |10\rangle)/\sqrt{2} \xrightarrow{H_1 I_2} |\beta''_{00}\rangle = \frac{1}{\sqrt{2}}(\underbrace{H|0\rangle}_{=\frac{|0\rangle+|1\rangle}{\sqrt{2}}}|0\rangle + \underbrace{H|1\rangle}_{=\frac{|0\rangle-|1\rangle}{\sqrt{2}}}|0\rangle) = |00\rangle$$

which tells Bob that Alice's message was indeed 00.

Outline

The density operator

Definition

Suppose that a quantum system is in one of the states $|\psi_i\rangle$ with probability p_i. Then $\{|\psi_i\rangle, p_i\}$ is called the ensamble of pure states of the system and the density operator associated to it is

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

A quantum system whose state $|\psi\rangle$ is known exactly is said to be in a pure state. In this case the density operator is simply $\rho = |\psi\rangle\langle\psi|$. Otherwise, ρ is in a mixed state.
Property $\mathrm{tr}(\rho^2) = 1$ if and only if ρ is in a pure state.

Theorem

An operator ρ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions:

- *(Trace condition) ρ has trace equal to one.*
- *(Positivity condition) ρ is a positive operator.*

Recovering the 4 postulates

1. Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its density operator ρ which is positive and of trace 1.
2. The evolution of a closed quantum system is described by a unitary transformation U. That is, the density operator ρ at t_1 and the one ρ' at t_2 are related

$$\rho \xrightarrow{U} \rho' = U\rho U^\dagger .$$

3. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the state space of the system being measured, where m refers to the measurement outcomes. If the system is described by ρ then

$$p(m) = \mathrm{tr}\left(M_m^\dagger M_m \rho\right)$$

   and the density operator of the system after measurement is $M_m^\dagger \rho M_m / \mathrm{tr}(M_m^\dagger M_m \rho)$.
4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered $1, \ldots, n$, and system number is described by the density operator ρ_i then the composite system is described by $\rho_1 \otimes \cdots \otimes \rho_n$.

Unitary freedom in the ensamble for density matrices

Example Consider the density operator

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.$$

It is also obtained for a quantum system prepared in the states

$$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle, \quad |b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$$

both with probability $1/2$.

Question What class of ensambles of states does give rise to a particular density matrix?

Theorem

For normalized sets of states $|\psi_i\rangle$, $|\varphi_j\rangle$ with probability distribution p_i, q_j, the density matrix is the same

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_j q_j |\varphi_j\rangle\langle\varphi_j|$$

if and only if

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle$$

for some unitary matrix u_{ij}.

Reduced density operator and quantum entanglement

The reduced density operator describes sub-systems of composite quantum systems.

Definition

Suppose there are two physical systems A, B described by the density operator ρ^{AB}. The reduced density operator for the system A is defined by

$$\rho_A = \operatorname{tr}_B(\rho^{AB})$$

where the partial trace over B acts as

$$\operatorname{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \operatorname{tr}(|b_1\rangle\langle b_2|) .$$

Another Hallmark of quantum entanglement. Consider again the Bell state $|\beta_{00}\rangle$. The density operator for a system in the pure state $|\beta_{00}\rangle$ is

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) = \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|\right) .$$

Tracing out the second qubit one finds a density operator for the first qubit which is

$$\rho^1 = \operatorname{tr}_2(\rho) = \cdots = \frac{I}{2}$$

which is a mixed state!

Outline

Schmidt decomposition theorem

Theorem

Suppose $|\psi\rangle$ is a pure state of a composite system AB. Then there exist orhonormal states for the system A, $|i_A\rangle$ and orthonormal states for the system B, $|i_B\rangle$ such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

with λ_i real non-negative numbers satisfying $\sum_i \lambda_i^2 = 1$.

Remark 1 Notice that taking the reduced density operator for the systems A and B we obtain respectively

$$\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|, \quad \rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|.$$

The fact that ρ^A, ρ^B shares the same eigenvalues implies that they share as well many other properties which depend on the eigenvalues.

Remark 2 λ_i are called Schmidt coefficients and the number of non-zero λ_i is called the Schmidt number of $|\psi\rangle$ and it quantifies the amount of entanglement of the state $|\psi\rangle$.

Purification procedure

Definition

For a given quantum system A with density operator

$$\rho^A = \sum_i p_i |i_A\rangle\langle i_A|,$$

a purification isa pure state of a composite system $|AR\rangle$, where R is an artificial quantum system having the same state space of A, such that

$$\mathrm{tr}\left(|AR\rangle\langle AR|\right) = \rho^A.$$

The pure state $|AR\rangle$ is built up by taking an orthonormal basis $|i_R\rangle$ and defining

$$|AR\rangle = \sum_i \sqrt{p_i}|i_A\rangle|i_R\rangle.$$

Remark For application in quantum computation / quantum information $\rightarrow$ see Part III.

Outline

The setting

"To obtain Bell's inequality, we're going to do a thought experiment, which we will analyze using our common sense notions of how the world works".

The experiment Charlie prepares two particles and he sends one particle to Alice, and the second particle to Bob, which are going to perform some measurements of physical properties P_Q, P_R and P_S, P_T respectively.

Assumptions

1. They perform their measurement simultaneously so that they cannot disturb one the result of the other and also they are far enough a part so that measurement on one system cannot influence measurement on the other.
2. These are *objective* properties, which values Q, R, S, T are revealed by the experiment but exists independently of it.

Proof of CHSH inequality

CHSH inequality

The CHSH inequality states that

$$\mathbb{E}(QS) + \mathbb{E}(RS) + \mathbb{E}(RT) - \mathbb{E}(QT) \leq 2.$$

- Notice that
$$QS + RS + RT - QT = (Q + R)S + (R - Q)T$$
and either $(Q + R)S$ either $(R - Q)T = 0$ since $R, Q = \pm 1$. In both case then $QS + RS + RT - QT = \pm 2$.
- Denoting $p(q, r, s, t)$ the probability that right before the measurement the system is in a state such that $Q = q$, $R = r$, $S = s$, $T = t$, we can write
$$\mathbb{E}\left(QS + RS + RT - QT\right) = \sum_{qrst} p(q, r, s, t)(qs+rs+rt-qt) \leq \sum_{qrst} p(q, r, s, t) 2 \leq 2.$$
- And also
$$\begin{aligned}\mathbb{E}\left(QS + RS + RT - QT\right) &= \sum_{qrst} p(q, r, s, t) qs + \sum_{qrst} p(q, r, s, t) rs \\ &+ \sum_{qrst} p(q, r, s, t) rt - \sum_{qrst} p(q, r, s, t) qt \\ &= \mathbb{E}(QS) + \mathbb{E}(RS) + \mathbb{E}(RT) - \mathbb{E}(QT).\end{aligned}$$

QM violation

Suppose that Charlie prepares a quantum system in the two qubits state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

and it sends the first qubit to Alice while the second to Bob.
They perform measurements of the following observables

$$Q = Z_1, \quad S = \frac{-Z_2 - X_2}{\sqrt{2}},$$
$$R = X_1, \quad T = \frac{Z_2 - X_2}{\sqrt{2}}.$$

Direct computation shows that

$$\langle QS\rangle = \frac{1}{\sqrt{2}} = \langle RS\rangle = \langle RT\rangle, \ \langle QT\rangle = -\frac{1}{\sqrt{2}}$$

which gives the contraddiction with CHSH inequality since

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} > 2!$$

Tsirelson's inequality

Moreover, this is the *maximal* violation of CHSH inequality since the Tsirelson's inequality assures that

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle \leq 2\sqrt{2}$$

for any Q, R, S, T written as $Q = \vec{q}\cdot\vec{\sigma}$, $R = \vec{r}\cdot\vec{\sigma}$, $S = \vec{s}\cdot\vec{\sigma}$, $T = \vec{t}\cdot\vec{\sigma}$ and $\vec{q}, \vec{r}, \vec{s}, \vec{t}$ being unitary vectors in $\mathbb{R}^3$.

Conclusion

Experiments with photons confirmed the prediction of QM equation

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$$

resolving the paradox in our computation.

"The CHSH inequality is not obeyed by Nature."

Question What was wrong in our computation to get CHSH inequality then?

Many studies pointed out that the answer is hidden behind the two assumptions we made:

1. *realism*, the fact that the physical properties P_Q, P_R, P_S, P_T to have definite values Q, R, S, T which exist independent of observation;
2. *locality*, the fact that Alice performing her measurement does not influence the result of Bob's measurement.