QIP Course 7: Properties of Density Matrices

Ryutaroh Matsumoto

Nagoya University, Japan
Send your comments to ryutaroh.matsumoto@nagoya-u.jp

August 2018
@ Tokyo Tech.

Copyright

Answers of prev. exercises

1, 2, 6. $\frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

3. Let P be a projection matrix of rank 1. Show that $\mathrm{Tr}[P] = 1$.

Answer: Let P map a vector in a linear space V to its subspace W. Since the rank of P is one, we have $\dim W = 1$. Let $|\varphi\rangle \in W$ be a vector of length one. Then we have $P = |\varphi\rangle\langle\varphi|$ by the definition of the projection matrix in page 2-11.
Let $\{|\varphi\rangle, |u_2\rangle, ..., |u_n\rangle\}$ be an ONB of V. (There always exists such an ONB. See your linear algebra textbook.) By the same computation as page 6-5, we can see $\mathrm{Tr}[P] = 1$.

4. Let M be a 2×2 Hermitian matrix with its spectral decomposition $M = \lambda_1 P_1 + \lambda_2 P_2$ with $\lambda_1 \neq \lambda_2$. Show that $\mathrm{Tr} P_1 = \mathrm{Tr} P_2 = 1$ by using your answer to Problem 3.

Answer: $\lambda_1 \neq \lambda_2$ implies that the rank of P_1 and P_2 is one. By the problem 3 we see $\mathrm{Tr} P_1 = \mathrm{Tr} P_2 = 1$.

5, 7. All the measurement outcomes have probability 0.5 because $\mathrm{Tr}[\frac{1}{2} I P] = 0.5$.

Interpretation of exercises

These exercises show that measurement of the single qubit of system A in $|\Psi\rangle = (|1_A 0_B\rangle + |0_A 1_B\rangle)/\sqrt{2}$ gives the same probability distribution of outcomes as the probabilistic mixture of $|0_A\rangle$ and $|1_A\rangle$ with probability 0.5. Therefore, no observable on the system A can distinguish $|\Psi\rangle$ and the probabilistic mixture of $|0_A\rangle$ and $|1_A\rangle$ with probability 0.5.

Contradiction to the locality by Q6

In physics, the locality (in Einstein's sense) means that the effect of some event cannot propagate faster than light. Suppose it is false. Then we could be affected by the event at the most distant place of the universe, which seems very unlikely, and also disables sensible investigation of our universe.

On the other hand, from B's viewpoint, B's state looks like $I_{2\times 2}/2$ with $|\Psi\rangle = (|1_A 0_B\rangle + |0_A 1_B\rangle)/\sqrt{2}$. Suppose that A measures the observable Z and got eigenvalue $+1$ as the measurement outcome. The state after measurement is $|1_A 0_B\rangle$, whose partial trace over A (= state of B) is $|0_B\rangle\langle 0_B|$. A and B can be very far apart (e.g. the opposite of the entire universe), and the measurement by A at very distant place suddenly changed B's state from $I_{2\times 2}/2$ to $|0_B\rangle\langle 0_B|$. Doesn't it look like a violation of the locality?? I will resolve this contradiction later.

Privacy of superdense coding

In superdense coding, the sender sends

$$(U \otimes I)(|0_A 0_B\rangle + |1_A 1_B\rangle)/\sqrt{2} = (U|0_A\rangle \otimes |0_B\rangle + U|1_A\rangle \otimes |1_B\rangle)/\sqrt{2}$$

for some 2×2 unitary matrix U.
Its corresponding density operator is

$$\frac{1}{2}(U|0_A\rangle\langle 0_A|U^* \otimes |0_B\rangle\langle 0_B| + U|1_A\rangle\langle 1_A|U^* \otimes |1_B\rangle\langle 1_B| + U|0_A\rangle\langle 1_A|U^* \otimes |0_B\rangle\langle 1_B| + U|1_A\rangle\langle 0_A|U^* \otimes |1_B\rangle\langle 0_B| \quad (1)$$

Observe that $\mathrm{Tr}[|0_B\rangle\langle 1_B|] = \mathrm{Tr}[|1_B\rangle\langle 0_B|] = 0$ and $\mathrm{Tr}[|0_B\rangle\langle 0_B|] = \mathrm{Tr}[|1_B\rangle\langle 1_B|] = 1$.
Thus, the partial trace of (1) over B is

$$\begin{aligned} \frac{1}{2}(U|0_A\rangle\langle 0_A|U^* + U|1_A\rangle\langle 1_A|U^*) &= \frac{1}{2}(U(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|)U^*) \\ &= UIU^*/2 \\ &= I/2 \end{aligned}$$

Whichever information the sender sends, the transmitted state is the

Properties of density operators

What kind of a matrix ρ can be a density matrix?

1. $\rho = \rho^*$ (Hermitian matrix).
2. All eigenvalules of ρ is nonnegative.
3. $\mathrm{Tr}\rho = 1$.

The state represented by a state vector is called pure state. The above three conditions gurantee that ρ can be represented as a probabilistic mixture of pure states as follows:
Let the spectral decomposition of ρ be

$$\rho = \sum_{i=1}^{n} \lambda_i |\varphi_i\rangle\langle\varphi_i|.$$

By the second condition, $\lambda_i \geq 0$ for all i, and by the third condition $\lambda_1 + \cdots + \lambda_n = 1$.
ρ can be seen as the state of the system whose state is $|\varphi_i\rangle$ with probability λ_i.

State after measurement

Let M be an observable with spectral decomposition

$$M = \sum_{i=1}^{n} iP_i.$$

After getting the outcome i, the state becomes

$$\frac{P_i \rho P_i}{\mathrm{Tr}[P_i \rho P_i]} = \frac{P_i \rho P_i}{\mathrm{Tr}[\rho P_i]}. \tag{2}$$

This is consistent with the definition of state change of pure states (Exercise 2).

"Consistent" means that the physical states after measurement

- computed by the vector representation, and
- computed by the density matrix representation

are the same.

No cloning theorem

Quantum information cannot be copied. Suppose that there is a unitary operator U such that for an arbitrary state $|\varphi\rangle$ and a fixed state $|\psi\rangle$

$$U(|\varphi\rangle \otimes |\psi\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \tag{3}$$

Then U is not linear (Exercise. Hint: consider what happens if we try to copy $|\varphi_1\rangle + |\varphi_2\rangle$).
Therefore, there is no unitary operator copying quantum information.

Classical error correction is done by adding redundant information by copying original information. Because of the no cloning theorem, error correction for quantum information had been thought to be impossible.

The quantum error correction is a useful tool for understanding the security of quantum cryptography. (But I will not teach it.)

Probability theory on a finite sample space

Ω: sample space $\underline{(|\Omega| < \infty)}$

$P : 2^{\Omega} \to [0, 1]$ is said to be a probability if

- $P(\Omega) = 1$, and
- $P(E) = \sum_{\omega \in E} P(\{\omega\})$.

A (real) random variable X is just a function from Ω to $\mathbf{R}$. Then probability of X becoming x is just $P(\{\omega \in \Omega \mid X(\omega) = x\})$.

We can embed the above notations into the quantum theory.

Embedding probability theory into quantum theory

Given Ω, P, X can be embedded into the quantum theory as follows: Consider $|\Omega|$-dimensional complex linear space with an ONB $\{|\omega\rangle \mid \omega \in \Omega\}$. Let ρ be the matrix

$$\rho = \sum_{\omega\in\Omega} P(\{\omega\})|\omega\rangle\langle\omega|. \tag{4}$$

For X, define the observable

$$A = \sum_{\omega\in\Omega} X(\omega)|\omega\rangle\langle\omega|.$$

Then $\Pr[X = z]$ is equal to the probability of obtaining z as an outcome by measuring the observable A of a system in the state ρ (verify this in Exercise 6).

Please remember this (used in p.14)

A pure state corresponds to a probability P with $P(\omega) = 1$ and $P(\omega') = 0$ for $\omega' \in \Omega \setminus \{\omega\}$.

Marginal distribution as a partial trace

Let $\Omega \times \Sigma$ as a finite sample space and P_{XY} be a probability on $\Omega \times \Sigma$.
When $\Omega \subset \mathbf{R}$ and $\Sigma \subset \mathbf{R}$, P_{XY} can be regarded as a joint probability mass function of two random variables $X(\omega) = \omega$ and $Y(\sigma) = \sigma$.
Define

$$\rho_{XY} = \sum_{\omega \in \Omega, \sigma \in \Sigma} P_{XY}(\omega, \sigma) |\omega\rangle\langle\omega| \otimes |\sigma\rangle\langle\sigma|.$$

The partial trace of ρ_{XY} over Y (or Σ) gives the density matrix corresponding to the marginal probability distribution of X.

Schrödinger and Heisenberg Pictures

In the popular version of quantum theory, the density matrix is considered to evolve when the physical object of interest evolves. This is called the Schrödinger picture.
On the other hand, one can regard the observable evolves and the density matrix stays the same as the physical object evolves. This is called the Heisenberg picture.

They are equivalent.

I explained the Schrödinger picture. The standard probability theory uses the Heisenberg picture, because it uses the single probability (measure) and multiple random variables. Their difference makes the connection between the partial trace and the marginalization a bit awkward.

Purification of a density matrix

Every density matrix is the partial trace of a pure state in some larger linear space. Let ρ be a density matrix and write

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|,$$

where vectors $|\varphi_i\rangle$ are chosen to be orthogonal to each other, $p_i \geq 0$ and $1 = \sum_i p_i$.
Let L be another linear space with $\{|i_L\rangle\}$ as its ONB. Then

$$\rho = \mathrm{Tr}_L[\sum_i \sqrt{p_i}|\varphi_i\rangle \otimes |i_L\rangle \sum_i \sqrt{p_i}\langle\varphi_i| \otimes \langle i_L|]. \tag{5}$$

A pure state corresponds to a deterministic probability distribution. Purification means that deterministic phenomenon in a larger system looks random in a smaller system. Sounds puzzling?

Correspondence between probability and quantum theories

- density matrix $\leftrightarrow$ probability
- observable $\leftrightarrow$ random variable
- partial trace $\leftrightarrow$ marginalization
- purification $\leftrightarrow$ **NOTHING**
- entanglement $\leftrightarrow$ statistical dependence (or correlation)

Most of problems in probability theory and statistics have their quantum counterpart **with mathematical and practical significance**. But quantum problems are terribly much more difficult than their classical counterparts, because of the non-commutativity of matrices (or operators in the general case).

When a quantum question can be handled within the probability theory?

If all the density matrices and observable appearing in a question are simultaneously diagonalizable (i.e., there exists a common pair of unitary matrices (U, U^*) that diagonalizes all the density matrices and observable simultaneously), then we can translate the quantum question into the language of probability theory by reversing the described process.

This unit may be conceptually heavy. In the next few units I introduce Shor's quantum factorization algorithm, which is terribly heavy only in the computation. Please be glad and feel relieved :-)
Please bring Matlab or Maple or something similar. (The lecturer has only "bc" on Linux.) We need softwares to handle exercises.

On the locality

If we view as quantum states similar to joint probability distributions, then the paradox of locality disappears as follows.
Suppose that there is an urn having one black ball and one white ball. Someone picks balls and put one ball to the box A and the other to the box B. The joint probability distribution is

$$\Pr[A = \text{black}, B = \text{white}] = \Pr[A = \text{white}, B = \text{black}] = 0.5,$$

and the marginal probability of B is

$$\Pr[B = \text{white}] = \Pr[B = \text{black}] = 0.5.$$

Suppose that A and B are moved far apart, A is opened, and white is observed. Then the joint probability changes to

$$\Pr[A = \text{black}, B = \text{white}] = 0, \Pr[A = \text{white}, B = \text{black}] = 1,$$

and the marginal probability of B is

$$\Pr[B = \text{white}] = 0, \Pr[B = \text{black}] = 1.$$

B's marginal distribution suddenly changed, but the physical reality does

Exercise

1. Prove Eq. (2).
2. When ρ is a pure state $|\varphi\rangle\langle\varphi|$, is the state after measurement defined by Eq. (2) the same as $P_i|\varphi\rangle/\|P_i|\varphi\rangle\|$? P_i is the same as Eq. (2). Do not answer "One is a vector while the other is a matrix. Thus, they are different." I am asking whether or not they correspond to the same physical state.
4. Explain why Eq. (3) is not linear.
5. Verify Eq. (4) is a density matrix.
6. Verify the claim at the bottom of p.11.
7. Compute a purification of the density matrix $\begin{pmatrix} 9/25 & 0 \\ 0 & 16/25 \end{pmatrix}$. Then compute the partial trace of your answer, and see if the original density matrix is restored.
8. (If you have the guts) Verify Eq. (5).
9. Express your view on p.17 in front of students in the classroom at the beginning of next unit. (Objection to the lecturer's view is more welcomed, because it initiates discussion)