

## Eigenvalues of a density operator

Last time after class someone asked a good question about the eigenvalues of density operators. I never actually showed that these must satisfy  $0 \leq \lambda_i \leq 1$ , so let's do that now.

Let's start from the definition of the density operator corresponding to a given mixed ensemble,

$$\begin{aligned}\rho &= \sum_k p_k |\Psi_k\rangle\langle\Psi_k| \\ &= \sum_k p_k \mathbf{P}_k,\end{aligned}$$

where  $\mathbf{P}_k$  is the projector onto  $|\Psi_k\rangle$ , which itself is a normalized pure state that occurs in the ensemble with relative probability  $p_k$ . For any arbitrary normalized state  $|\Phi\rangle$  in the entire Hilbert space,

$$\langle\Phi|\rho|\Phi\rangle = \sum_k p_k \langle\Phi|\mathbf{P}_k|\Phi\rangle.$$

Since all of the  $p_k$  and  $\langle\Phi|\mathbf{P}_k|\Phi\rangle$  must be between 0 and 1, it follows that

$$0 \leq \langle\Phi|\rho|\Phi\rangle \leq 1$$

for absolutely *any* (normalized) choice of the state  $|\Phi\rangle$ . This includes, in particular, the eigenstates of  $\rho$ , for which we have the deduction

$$\begin{aligned}\rho|\psi_j\rangle &= \lambda_j|\psi_j\rangle, \\ \langle\psi_j|\rho|\psi_j\rangle &= \lambda_j, \\ 0 &\leq \lambda_j \leq 1.\end{aligned}$$

## Cyclic property of the Trace operation...

For any pair of operators **A** and **B**,

$$\text{Tr}[\mathbf{AB}] = \text{Tr}[\mathbf{BA}]. \quad 1$$

To see this, let's pick a complete orthonormal basis for the relevant Hilbert space and write matrix representations:

$$\mathbf{A} = \sum_{ij} a_{ij} |i\rangle\langle j|,$$

$$\mathbf{B} = \sum_{ij} b_{ij} |i\rangle\langle j|. \quad 2$$

By definition of the trace,

$$\text{Tr}[\mathbf{AB}] = \sum_i \langle i|\mathbf{AB}|i\rangle, \quad 3$$

but we can insert a 'closure relation'

$$\sum_j |j\rangle\langle j| = \mathbf{1} \quad 4$$

in the middle to obtain

$$\begin{aligned}
 \text{Tr}[\mathbf{AB}] &= \sum_{ij} \langle i | \mathbf{A} | j \rangle \langle j | \mathbf{B} | i \rangle \\
 &= \sum_{ij} a_{ij} b_{ji} \\
 &= \sum_{ji} b_{ij} a_{ji} \\
 &= \text{Tr}[\mathbf{BA}].
 \end{aligned}
 \tag{5}$$

Just for amusement, let's look at an alternative proof that holds when either **A** or **B** is Hermitian. Let's say that **A** is Hermitian, and therefore has real eigenvalues and a complete set of orthogonal eigenvectors:

$$\begin{aligned}
 \mathbf{A} |m\rangle &= \alpha_m |m\rangle, \\
 \langle m | \mathbf{A} &= \alpha_m \langle m|.
 \end{aligned}
 \tag{6}$$

We can therefore choose to take our trace in the eigenbasis of **A**, so

$$\begin{aligned}
 \text{Tr}[\mathbf{AB}] &= \sum_m \langle m | \mathbf{AB} | m \rangle \\
 &= \sum_m \alpha_m \langle m | \mathbf{B} | m \rangle \\
 &= \sum_m \langle m | \mathbf{BA} | m \rangle \\
 &= \text{Tr}[\mathbf{BA}].
 \end{aligned}
 \tag{7}$$

An analogous proof holds when **B** is Hermitian.

Since the product of operators is still an operator,

$$\begin{aligned}
 \text{Tr}[\mathbf{ABC D}] &= \text{Tr}[\mathbf{D ABC}], \\
 \text{Tr}[\mathbf{A BCD}] &= \text{Tr}[\mathbf{BCD A}],
 \end{aligned}
 \tag{8}$$

and so on and so forth... Hence one says that the trace operation is *cyclic*.

## Measurements on density operators

Let's return to our two-dimensional Hilbert space with orthonormal basis kets  $|x\rangle$  and  $|y\rangle$ . Once again, suppose we are given a mixed ensemble of quantum states

$$\begin{aligned}
 p : \quad |\Psi_A\rangle &= a_x |x\rangle + a_y |y\rangle, \\
 1-p : \quad |\Psi_B\rangle &= b_x |x\rangle + b_y |y\rangle,
 \end{aligned}
 \tag{9}$$

and a measurement specified by the projectors

$$\begin{aligned}\mathbf{P}_x &= |x\rangle\langle x|, \\ \mathbf{P}_y &= |y\rangle\langle y|.\end{aligned}\tag{10}$$

Recall that the frequency with which we expect to obtain outcome  $x$  in a series of such measurements is given by

$$\begin{aligned}\Pr(x) &= [\Pr(\Psi_A)\Pr(x|\Psi_A) + \Pr(\Psi_B)\Pr(x|\Psi_B)] \\ &= [p\langle\Psi_A|\mathbf{P}_x|\Psi_A\rangle + (1-p)\langle\Psi_B|\mathbf{P}_x|\Psi_B\rangle] \\ &= [p|a_x|^2 + (1-p)|b_x|^2].\end{aligned}\tag{11}$$

In the previous lecture, we introduced the density operator corresponding to a mixed ensemble of quantum states. For this particular case,

$$\rho = p|\Psi_A\rangle\langle\Psi_A| + (1-p)|\Psi_B\rangle\langle\Psi_B|.\tag{12}$$

We can conveniently represent ensemble-averaged quantities such as  $\Pr(x)$  in terms of  $\rho$ :

$$\begin{aligned}\Pr(x) &= \text{Tr}[\rho\mathbf{P}_x] \\ &= \text{Tr}[\mathbf{P}_x\rho].\end{aligned}\tag{13}$$

To see that this is true we simply write out the trace,

$$\begin{aligned}\text{Tr}[\rho\mathbf{P}_x] &= \langle x|\rho\mathbf{P}_x|x\rangle + \langle y|\rho\mathbf{P}_x|y\rangle \\ &= \langle x|\rho|x\rangle \\ &= p\langle x|\Psi_A\rangle\langle\Psi_A|x\rangle + (1-p)\langle x|\Psi_B\rangle\langle\Psi_B|x\rangle \\ &= p|a_x|^2 + (1-p)|b_x|^2.\end{aligned}\tag{14}$$

In general, the probability of obtaining the outcome  $x$  in a measurement of  $\{\mathbf{P}_x, \dots\}$  on a mixed ensemble with density operator  $\rho \leftrightarrow \{p_i, |\Psi_i\rangle\}$  is given by

$$\begin{aligned}\Pr(x) &= \sum_i \Pr(i)\Pr(x|i) \\ &= \sum_i p_i \langle\Psi_i|\mathbf{P}_x|\Psi_i\rangle \\ &= \sum_{ij} p_i \langle\Psi_i|\mathbf{P}_x|j\rangle\langle j|\Psi_i\rangle \\ &= \sum_{ij} p_i \langle j|\Psi_i\rangle\langle\Psi_i|\mathbf{P}_x|j\rangle \\ &= \sum_j \langle j|\sum_i p_i |\Psi_i\rangle\langle\Psi_i|\mathbf{P}_x|j\rangle \\ &= \text{Tr}[\rho\mathbf{P}_x].\end{aligned}\tag{15}$$

What about the post-measurement state? For pure quantum states

$$|\Psi_i\rangle \mapsto \frac{\mathbf{P}_x|\Psi_i\rangle}{\sqrt{\langle\Psi_i|\mathbf{P}_x|\Psi_i\rangle}},\tag{16}$$

and for density operators

$$\rho \mapsto \frac{\mathbf{P}_x \rho \mathbf{P}_x}{\text{Tr}[\rho \mathbf{P}_x]}. \quad 17$$

Once again, the role of the projection operator is to enforce consistency of the post-measurement state with the actual outcome of the measurement; the denominator ensures that the post-measurement state is still normalized (i.e.  $\text{Tr}[\rho] = 1$ ).

## Combining ensembles

If  $\rho_A$  and  $\rho_B$  are valid density operators, then so is

$$\rho = p \rho_A + (1 - p) \rho_B. \quad 18$$

Here  $0 \leq p \leq 1$ . We say that the set of density operators is ‘closed under convex combination.’

At the ensemble level, if  $\rho_A$  corresponds to  $\{p_i^A, |\Psi_i^A\rangle\}$  (and similarly for  $\rho_B$ ) we can think of  $\rho$  as representing the combined ensemble

$$\begin{aligned} p p_1^A &: |\Psi_1^A\rangle \\ (1-p)p_1^B &: |\Psi_1^B\rangle \\ p p_2^A &: |\Psi_2^A\rangle \\ (1-p)p_2^B &: |\Psi_2^B\rangle \\ \vdots &: \vdots \end{aligned} \quad 19$$

## Evolution of density operators

Under Hamiltonian evolution (according to the Schrödinger Equation), we know that we can use a time development operator to express the evolution of a pure quantum state:

$$\begin{aligned} |\Psi(t)\rangle &= \mathbf{T}(t,0)|\Psi(0)\rangle, \\ \langle \Psi(t)| &= \langle \Psi(0)|\mathbf{T}(0,t). \end{aligned} \quad 20$$

Hence for a density operator,

$$\begin{aligned} \rho(t) &= \sum_i p_i |\Psi_i(t)\rangle \langle \Psi_i(t)| \\ &= \sum_i p_i \mathbf{T}(t,0) |\Psi_i(0)\rangle \langle \Psi_i(0)| \mathbf{T}(0,t) \\ &= \mathbf{T}(t,0) \rho(0) \mathbf{T}(0,t). \end{aligned} \quad 21$$

In addition to being formally appealing, we can use this result to show that  $\text{Tr}[\rho]$  is preserved by Hamiltonian evolution:

$$\begin{aligned}
\text{Tr}[\rho(t)] &= \text{Tr}[\mathbf{T}(t,0)\rho(0)\mathbf{T}(0,t)] \\
&= \text{Tr}[\mathbf{T}(0,t)\mathbf{T}(t,0)\rho(0)] \\
&= \text{Tr}[\rho(0)].
\end{aligned}$$

22

More generally, Hamiltonian evolution preserves the eigenvalue spectrum of a density operator – prove this yourself as an exercise!

Note that where I say ‘Hamiltonian evolution’ I simply mean evolution according to the Schrödinger Equation. Some people also refer to ‘unitary evolution’ since  $\mathbf{T}(t,0)$  is unitary.

## Empiricism: What is a quantum state?

The following is not really a ‘standard’ interpretation of the state vector, but to my mind it’s the only one that makes sense. I learned this way of thinking from Christopher Fuchs, who sometimes attributes it to James Hartle.

- A quantum state  $|\Psi\rangle$  or  $\rho$  is a mathematical object that compactly **represents our knowledge** about the preparation of a physical system.
- There is no reason to believe that  $|\Psi\rangle$  or  $\rho$  are ‘physical’ objects in the way that hydrodynamic waves or electromagnetic wavepackets are physical objects. Of course, some people choose to believe this.
- In this picture, the Schrodinger Equation describes how our compact description of a system’s preparation should change as a function of time, given that we know the proper Hamiltonian.
- Given that  $|\Psi\rangle$  and  $\rho$  are mathematical objects representing states of knowledge, there is nothing particularly mysterious about the measurement ‘collapse’ rule

$$|\Psi\rangle \mapsto \frac{\mathbf{P}|\Psi\rangle}{\sqrt{\langle\Psi|\mathbf{P}|\Psi\rangle}}.$$

When we gain information about a system by performing a measurement on it, our description of it needs to change in order for us to keep doing the best possible job of predicting the statistics of further measurements. It needs to change instantaneously, and even discontinuously.

Within this overall framework, we think of pure states  $|\Psi\rangle$  as representing ‘minimal uncertainty’ states, whereas density operators  $\rho$  are used to represent the additional uncertainties (probabilities) inherent in a mixed ensemble.

What’s bizzare about quantum mechanics is that even for a pure state  $|\Psi\rangle$ , there are countless observables  $\mathbf{O}_q$  whose uncertainty  $\Delta\mathbf{O}_q$  is nonzero! As hinted last time in our discussion of Heisenberg Uncertainty Relations, this fact becomes even more bizzare in

infinite dimensions.

## Random-basis quantum cryptography

As an application of what we've learned so far, let's look at the cryptographic key distribution protocol of C. H. Bennett and G. Brassard (*Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175; also, C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992)).

A common way to encrypt data (string of meaningful bits) is the so-called "one-time pad," which requires a secret key (string of random bits) with length equal to that of the data. The encrypted version of the data is obtained simply by performing a bitwise XOR between the plain data and the secret key:

*data* : 01011011101111...  
*key* : 01101010001101...  
*encrypted* : 00110001100010...

Recall that the XOR operation is defined by the following truth table:

XOR(0,0) = 0, XOR(0,1) = 1,  
XOR(1,0) = 1, XOR(1,1) = 0.

If the key is truly random, the encrypted data is now statistically independent of the plain data. The encrypted data can only be decrypted by someone who knows the secret key. The procedure is then quite simple, corresponding to another XOR:

*encrypted* : 00110001100010...  
*key* : 01101010001101...  
*data* : 01011011101111...

The drawback of one-time pad is that the communicators always need to have lots of secret key available (it's no good if you re-use it). In general, when all the available key has been used up the two parties have to either get together to decide on some new key bits, or they must use a trusted courier to "carry" new key information from one party to the other. Quantum cryptographic key distribution seeks to use quantum phenomena to allow generation of shared random key over *public* communication channels.

The basic idea is simple. Let the two communicators be named Alice and Bob (a common convention in the field of cryptography). Alice will send Bob a sequence of two-level quantum systems, each of which is randomly prepared in one of four possible states:

$$|0\rangle, |1\rangle, |x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |y\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Alice doesn't initially say anything to anybody about the sequence of states. Every time Bob receives one of these quantum systems, he randomly chooses to make one of two standard

measurements:

$$\{|0\rangle\langle 0|, |1\rangle\langle 1|\} \quad \text{or} \quad \{|x\rangle\langle x|, |y\rangle\langle y|\}.$$

After the entire transmission is done, Alice publicly announces for each transmission whether the state was selected from the  $0, 1$  basis or the  $x, y$  basis (but without actually revealing which of the two basis states was sent). Bob also announces whether he measured in the  $0, 1$  basis or the  $x, y$  basis, but without revealing his result. In cases where they happened to choose the same basis, Bob should have been able to perfectly recover the identity of the state that Alice sent. They can check this by using up a subset of the transmissions.