Quantum Algorithms and Learning Theory
Notes and Exercises

Faris Sbahi

March 17, 2018

1 Nielsen & Chuang: Chapter 2

1.1 Postulates of Quantum Mechanics

First, we cover the fundamental postulates of quantum mechanics.

1.1.1 State Space and State Vector

Associated with an isolated physical system is a Hilbert space, $\mathcal{H}$. A Hilbert space is a complete inner-product vector space. Note that completeness holds trivially in a finite-dimensional vector space because we have closure with respect to all sequences (and hence any Cauchy sequence in the vector space must converge to a vector in the same space). Nevertheless, the state space of a physical system may be infinite-dimensional.

A system is completely described by a unit vector $u \in \mathcal{H}$ called the state vector.

For example, consider a system given by a single qubit, which has a two-dimensional state space. Let $|0\rangle$ and $|1\rangle$ be an orthonormal basis for this space. Hence, a state vector in this space is given by

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

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

1.1.2 Evolution

The evolution of a closed quantum system is described by a unitary transformation. Recall that an operator U is unitary iff $U^\dagger U = I = UU^\dagger$ (and hence preserves inner products[1]).

So, let the state of a system at time t_1 be given by $|\psi\rangle$ and $|\psi'\rangle$ at t_2. Hence,

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

---

[1]and furthermore has a spectral decomposition because it is normal

1.1.3 Evolution in Continuous Time

Schrodinger's equation provides the time evolution of the state of a quantum system

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle \tag{1}$$

where H is the (Hermitian) Hamiltonian of the closed system. Because the Hamiltonian is Hermitian it has spectral decomposition

$$H = \sum_E E\,|E\rangle\,\langle E|$$

where E is the energy eigenvalue corresponding to energy eigenstate $|E\rangle$.

For example, consider the Hamiltonian $H = \hbar\omega X$ (recall that $X = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ from 9.1). Hence, we solve for its eigenvalues and eigenvectors

$$\det\left\{\hbar\omega \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix}\right\} = 0$$
$$\lambda^2 - 1^2 = 0$$
$$\lambda = \pm 1$$
$$\Rightarrow E_\pm = \pm\hbar\omega$$
$$\hbar\omega \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}|E_+\rangle = 0$$
$$|E_+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} := |+\rangle$$
$$|E_-\rangle = |-\rangle$$

Onwards, notice that we can solve Schrodinger's equation (1) and have

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle$$

and equivalently from 1.1.2 we can represent this transformation with unitary operator $U = \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]$. This holds in general and so we can consider the two descriptions from 1.1.2 and 1.1.3 interchangeably (the authors prefer the latter).

1.1.4 Quantum Measurement

Quantum measurements are described by a collection of measurements operators $\{M_m\}$ (where the index m refers to the potential measurement outcomes of the experiment) which act on the state space of the system being observed.

Hence, if the pre-measurement state is $|\psi\rangle$, then

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

and the post-measurement state is

$$\frac{M_m\, |\psi\rangle}{\sqrt{p(m)}}$$

Furthermore, $\{M_m\}$ satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I$$

An important example of a measurement is the measurement of a qubit in the computational basis. This is a measurement of a qubit with two outcomes defined by the measurement operators $M_0 = |0\rangle\langle0|$ and $M_1 = |1\rangle\langle1|$.

Now, we see an interesting implication. If we seek to distinguish our physical system from a set of orthogonal states, then we can reliably do so by simply defining each measurement operator to be the outer product of our states of interest. We add a final operator defined to be the remaining complement of the identity in order to satisfy the completeness equation.

On the flipside, two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ necessarily share a parallel component in their orthogonal decomposition. Hence, a measurement outcome that corresponds to the pre-measurement state being $|\psi_1\rangle$ with probability $p > 0$ has a probability $p' > 0$ of having been in state $|\psi_2\rangle$.

1.1.5 Projective Measurements

There exists a special class of quantum measurements known as projective measurements. These measurements can be described by an observable M, a hermitian operator on the state space being observed. M has spectral decomposition

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalues m.

Furthermore, if the pre-measurement state is $|\psi\rangle$, then

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

and the post-measurement state is

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

This simplifies the formula for the expected value of a measurement

$$
\begin{aligned}
\langle M\rangle &= \sum_m mp(m) \\
&= \langle\psi| \left(\sum_m mP_m\right) |\psi\rangle \\
&= \langle\psi| M |\psi\rangle
\end{aligned}
$$

For example, consider projective measurements on the system given by single qubits with observable Pauli matrix Z. Hence, Z has eigenvalues $+1$ and -1 and eigenstates $|0\rangle$ and $|1\rangle$, respectively. So, consider state $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle \Rightarrow p(+1) = \langle+|0\rangle \langle0|+\rangle = \frac{1}{2}$. Similarly, $p(-1) = \frac{1}{2}$.

1.1.6 POVM measurements

POVMs are best viewed as a special case of the general measurement formalism, providing the simplest means to study post-measurement statistics without knowledge of the post measurement state.

From above, $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ so if we define $E_m := M_m^\dagger M_m$ (which is hence positive from 9.3) then these E_m's are sufficient for the purpose of computing probabilities. We denote $\{E_m\}$ as a POVM.

Note that projective operators are the special case of being equivalent to their respective POVM element because $E_m = P_m^\dagger P_m = P_m$.

Nevertheless, the POVM formalism is a useful guide in for our intuition in quantum information. Consider if Alice prepares some state for Bob that is either $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Recall from 1.1.4, Bob can't determine which state was prepared with full certainty (because of the shared orthogonal component $|0\rangle$). Still, we can define a POVM[2]

---

[2] verify that completeness and these being positive operators holds

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} \left|1\right\rangle \left\langle 1\right|$$

$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(\left|0\right\rangle - \left|1\right\rangle)(\left\langle 0\right| - \left\langle 1\right|)}{2}$$

$$E_3 = I - E_1 - E_2$$

Now, notice what happens.

$$\left\langle \psi_1\right| E_1 \left|\psi_1\right\rangle = \left\langle 0\right| \frac{\sqrt{2}}{1+\sqrt{2}} \left|1\right\rangle \left\langle 1|0\right\rangle$$

$$= 0$$

$$\left\langle \psi_2\right| E_1 \left|\psi_2\right\rangle = \frac{\left\langle 0\right| + \left\langle 1\right|}{\sqrt{2}} \frac{\sqrt{2}}{1+\sqrt{2}} \left|1\right\rangle \left\langle 1\right| \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}$$

$$= \frac{\sqrt{2}}{2\sqrt{2}+2} > 0$$

Hence, if we observe E_1 after the measurement described by $\{E_1, E_2, E_3\}$, then Alice must've prepared $\left|\psi_2\right\rangle$. Similarly,

$$\left\langle \psi_1\right| E_2 \left|\psi_1\right\rangle = \left\langle 0\right| \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(\left|0\right\rangle - \left|1\right\rangle)(\left\langle 0\right| - \left\langle 1\right|)}{2} \left|0\right\rangle$$

$$= \frac{\sqrt{2}}{2\sqrt{2}+2} > 0$$

$$\left\langle \psi_2\right| E_2 \left|\psi_2\right\rangle = \frac{\left\langle 0\right| + \left\langle 1\right|}{\sqrt{2}} \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(\left|0\right\rangle - \left|1\right\rangle)(\left\langle 0\right| - \left\langle 1\right|)}{2} \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}$$

$$= 0$$

so if we observe E_2, then Bob concludes that Alice prepared $\left|\psi_1\right\rangle$. Our routine is imperfect because we may observe E_3 and hence would infer nothing of the original state. Still, we would never *incorrectly* guess given that we allow ourselves to abstain when we see E_3.

Exercise 1.1. *(2.64) Suppose Bob is given a quantum state chosen from a set $S = \left|\psi_1\right\rangle, \cdots, \left|\psi_m\right\rangle$ of linearly independent states. Construct a POVM $\{E_1, \cdots, E_{m+1}\}$ such that if outcome E_i occurs, $1 \leq i \leq m$, then Bob knows with certainty that he was given state $\left|\psi_i\right\rangle$.*

To distinguish the states we require $\left\langle \psi_i\right| E_j \left|\psi_i\right\rangle = p_i \delta_{ij}$ where $p_i > 0$ and $1 \leq i, j \leq m$.

So, we can use the Gram-Schmidt process using S as our linearly independent set. This will give us an orthonormal set $U = |\varphi_1\rangle, \cdots, |\varphi_m\rangle$ that spans the same subspace as S. Next, we can represent each $|\psi_i\rangle$ in this orthonormal basis, U. Finally, for each i we can find a vector $|\psi_i'\rangle$ in the span of U that is orthogonal to all $|\psi_j\rangle, j \neq i$. Hence, we can define $E_i = |\psi_i'\rangle \langle \psi_i'|, 1 \leq i \leq m$. Finally, take $E_{m+1} = I - \sum_m E_i$.

Creating an optimal POVM is much trickier (in the sense of minimizing the probability p_{m+1}).

From this exercise, we see that POVMs present a reliable way to distinguish non-orthogonal (but linearly independent) states given that we allow for the slack of an "inconclusive" measurement (E_{m+1}).

1.1.7 Composite Systems

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

Exercise 1.2. *(2.66) Show that the average value of the observable $X_1 Z_2$ (X acting on the first qubit and Z on the second) for a two qubit system measured in the state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is zero.*

Proof. Let observable $M = X_1 Z_2$. Hence,

$$
\begin{aligned}
\langle M \rangle &= \frac{\langle 00| + \langle 11|}{\sqrt{2}} M \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
&= \frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{X_1 |0\rangle Z_2 |0\rangle + X_1 |1\rangle Z_2 |1\rangle}{\sqrt{2}} \\
&= \frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{|1\rangle |0\rangle - |0\rangle |1\rangle}{\sqrt{2}} \\
&= 0
\end{aligned}
$$

$\square$

Interestingly, we can show that a general quantum measurement (as described in 1.1.4) can be implemented as a projective measurement coupled with unitary dynamics.

Consider a quantum system with state space Q and measurements M_m on this system. We can introduce an *ancilla* system M with orthonormal basis $|m\rangle$ which is in one-to-one correspondence with the possible outcomes of the measurement we wish to implement.

So, let $|0\rangle$ be a fixed state of M and define an operator U on $|\psi\rangle |0\rangle$ (with $|\psi\rangle$ as a state of Q) by

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

Hence,

$$\langle\varphi|\,\langle0|\,U^\dagger U\,|\psi\rangle\,|0\rangle = \sum_m\sum_{m'}\langle\varphi|\,M_m^\dagger M_{m'}\,|\psi\rangle\,\langle m|m'\rangle$$

So, because the states $|m\rangle$ are orthonormal

$$= \sum_m\langle\varphi|\,M_m^\dagger M_m\,|\psi\rangle$$

and finally by the completeness of M_m

$$= \langle\varphi|\psi\rangle$$

This tells us that U preserves inner products between states of the form $|\psi\rangle\,|0\rangle$. Furthermore, we can show that U can be extended to a unitary operator on $Q \otimes M$ (exercise).

Hence, consider a projective measurement on the two systems $(U\,|\psi\rangle\,|0\rangle)$ given by projectors $P_m := I_Q \otimes |m\rangle\,\langle m|$. So,

$$\begin{aligned}
p(m) &= \langle\psi|\,\langle0|\,U^\dagger P_m U\,|\psi\rangle\,|0\rangle \\
&= \sum_{m'}\sum_{m''}\langle\psi|\,M_{m'}^\dagger\,\langle m'|\,(I_Q \otimes |m\rangle\,\langle m|)M_{m''}\,|\psi\rangle\,|m''\rangle \\
&= \langle\psi|\,M_m^\dagger M_m\,|\psi\rangle
\end{aligned}$$

which agrees with the general result from 1.1.4. Similarly, the post-measurement state is as expected. Hence, we've shown that unitary dynamics, projective measurements, and ancillary systems can be used together to describe any general measurement.

Exercise 1.3. *(2.68) Prove that $|\psi\rangle \neq |a\rangle\,|b\rangle$ for all single qubit state $|a\rangle$ and $|b\rangle$ where $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.*

Proof. First, decompose the qubit state in their basis, $|a\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$ and $|b\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle$. Now, we prove by contradiction

$$\begin{aligned}
|a\rangle\,|b\rangle &= \alpha_0\beta_0\,|00\rangle + \alpha_0\beta_1\,|01\rangle + \alpha_1\beta_0\,|10\rangle + \alpha_1\beta_1\,|11\rangle \\
&= \frac{|00\rangle + |11\rangle}{\sqrt{2}}
\end{aligned}$$

which would imply that either α_0 or β_1 are zero in order to remove the $|01\rangle$ term. However, this would also remove either the $|00\rangle$ or $|11\rangle$ term, so we have a contradiction. $\square$

A state of a composite system having this property is said to be entangled.

1.2 Superdense Coding

Suppose Alice is in possession of two classical bits of information she wishes to transmit to Bob, but is only allowed to send a single qubit to Bob.

Now, suppose that Alice and Bob initially share a pair of qubits in the entangled state from above

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

where Alice is initially holding the first qubit and Bob the second. She can then apply a particular gate to send a bit string. Below shows the corresponding gate and resulting state

Bit String	Applied gate	Resulting state
00	–	$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
01	Z	$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$
10	X	$\frac{|10\rangle + |01\rangle}{\sqrt{2}}$
11	iY	$\frac{-|10\rangle + |01\rangle}{\sqrt{2}}$

Observe that these are the Bell states (see 9.2). Furthermore, Bell states form an orthonormal basis and hence can be distinguished (as we've discussed in 1.1.6). Hence, Alice needs only to interact with the single qubit to transmit two classical bits of information to Bob.

Exercise 1.4. *(2.70) Suppose E is any positive operator acting on Alices qubit. Show that $\langle\psi| E \otimes I |\psi\rangle$ takes the same value when $|\psi\rangle$ is any of the four Bell states. Suppose some malevolent third party ('Eve') intercepts Alices qubit on the way to Bob in the superdense coding protocol. Can Eve infer anything about which of the four possible bit strings 00, 01, 10, 11 Alice is trying to send? If so, how, or if not, why not?*

Proof.

$$\langle 00| + \langle 11| \, (E \otimes I) \, |00\rangle + |11\rangle = \langle 0| E |0\rangle + \langle 1| E |1\rangle$$
$$\langle 00| - \langle 11| \, (E \otimes I) \, |00\rangle - |11\rangle = \langle 0| E |0\rangle + \langle 1| E |1\rangle$$
$$\langle 10| + \langle 01| \, (E \otimes I) \, |10\rangle + |01\rangle = \langle 0| E |0\rangle + \langle 1| E |1\rangle$$
$$-\langle 10| + \langle 01| \, (E \otimes I) - |10\rangle + |01\rangle = \langle 0| E |0\rangle + \langle 1| E |1\rangle$$

Hence, Eve can't infer anything. The states are only distinguishable if one can perform a measurement that acts on both qubits. $\square$

1.3   The Density Operator

An alternative formulation of quantum mechanics is possible using a tool known as the density operator.

Suppose a quantum system is one of a number of states $|\psi\rangle$ with probability p_i. We call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator is defined

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

Evolution of the density operator (under a unitary transformation) can be derived readily

$$\sum_i p_i U |\psi_i\rangle \langle\psi_i| U^\dagger = U\rho U^\dagger$$

If we perform a measurement with operator M_m with initial state $|\psi_i\rangle$ then

$$p(m \mid i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle$$
$$= \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|\right)$$

using 9.4.

Hence, summing this conditional probability across all initial states we have

$$p(m) = \sum_i p_i \, \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|\right)$$
$$= \mathrm{tr}\left(M_m^\dagger M_m \rho\right)$$

The state after obtaining measurement result m on initial state $|\psi_i\rangle$ is

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}}$$

and so the density operator after result m is given by

$$\rho_m = \sum_i p(i \mid m) |\psi_i^m\rangle \langle\psi_i^m|$$
$$= \sum_i p(i \mid m) \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}$$

Furthermore, from Baye's rule we have that $p(i \mid m) = \frac{p(m|i)p(i)}{p(m)}$ so we can simplify

$$
\begin{aligned}
\rho_m &= \sum_i \frac{p(m \mid i)p(i)}{p(m)} \frac{M_m \left|\psi_i\right\rangle \left\langle\psi_i\right| M_m^\dagger}{\left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle} \\
&= \sum_i \frac{p(i) \left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)} \frac{M_m \left|\psi_i\right\rangle \left\langle\psi_i\right| M_m^\dagger}{\left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle} \\
&= \sum_i \frac{p(i) M_m \left|\psi_i\right\rangle \left\langle\psi_i\right| M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)} \\
&= \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}
\end{aligned}
$$

A quantum state whose state $\left|\psi\right\rangle$ is known exactly is said to be in a pure state. In this case the density operator is simply $\rho = \left|\psi\right\rangle \left\langle\psi\right|$. Otherwise, ρ is in a mixed state.

A pure state satisfies $\mathrm{tr}\left(\rho^2\right) = 1$ and a mixed state $\mathrm{tr}\left(\rho^2\right) < 1$.

Imagine that our record of the result m of a measurement was lost. We would have a quantum system in the state ρ_m with probability $p(m)$ without knowing the actual value of m. Hence, the system would be described as

$$
\begin{aligned}
\rho &= \sum_m p(m)\rho_m \\
&= \sum_m M_m \rho M_m^\dagger
\end{aligned}
$$

We may wish to move away from the interpretation of the density operator as a means of describing ensembles of quantum states.

Theorem 1.5. *An operator ρ is a density operator associated to some ensemble $\{p_i, \left|\psi_i\right\rangle\}$ if and only if it satisfies the conditions*

1. *ρ has trace equal to one*

2. *ρ is a positive operator*

Proof. We show one direction (see the text for the other). Let ρ be a density operator. Hence,

$$
\begin{aligned}
\mathrm{tr}(\rho) &= \sum_i p_i \, \mathrm{tr}(\left|\psi_i\right\rangle \left\langle\psi_i\right|) \\
&= \sum_i p_i = 1
\end{aligned}
$$

10

because $\mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \psi_{i1}^2 + \psi_{i2}^2 + \cdots \psi_{in}^2 = 1$ by normalization.

Furthermore, suppose $|\varphi\rangle$ resides in the vector space

$$\langle\varphi|\,\rho\,|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle \langle\psi_i|\varphi\rangle$$
$$= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \geq 0$$

so we have positivity. $\qquad\qquad\square$

The use of this theorem is that we can define a density operator to be a positive operator with trace one and hence reformulate the postulates of quantum mechanics without speaking of ensembles.

This reformulation shines when describing quantum systems whose state is not known and when describing subsystems a composite quantum system.

Exercise 1.6. *(2.71) Let ρ be a density operator. Show that $\mathrm{tr}\big(\rho^2\big) \leq 1$ with equality iff ρ is a pure state.*

Proof. $\qquad\qquad\square$

Remember that different ensembles of quantum states can give rise to a specific density matrix and hence one must avoid assuming that the eigenvectors and eigenvalues have special significance with regard to the represented ensemble of quantum states.

Nevertheless, there is value in discussing which ensembles give rise to the same density matrix (notably in quantum noise and error correction). Let $\big|\tilde{\psi}_i\big\rangle$ generate ρ i.e. $\rho :=$ $\sum_i \big|\tilde{\psi}_i\big\rangle\big\langle\tilde{\psi}_i\big|$. Note that $\big|\tilde{\psi}_i\big\rangle = \sqrt{p_i}\,|\psi_i\rangle$ is clearly not necessarily normalized. Now, we have the following theorem.

Theorem 1.7. *The sets $\big|\tilde{\psi}_i\big\rangle$ and $|\tilde{\varphi}_j\rangle$ generate the same ρ if and only if*

$$\big|\tilde{\psi}_i\big\rangle = \sum_j u_{ij}\,|\tilde{\varphi}_j\rangle$$

where the matrix with matrix elements u_{ij} is unitary.

Proof. See the text. $\qquad\qquad\square$

Exercise 1.8. *(2.72) Bloch Sphere for mixed states.*

Proof. $\qquad\qquad\square$

As mentioned above, density operators are powerful tools for describing subsystems of composite systems.

Suppose we have physical systems A and B, whose state is described by ρ^{AB}. The reduced density operator for system A is defined by

$$\rho^A := \text{tr}_B(\rho^{AB})$$

where tr_B is a map of operators known as the partial trace over system B which is defined by

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

Hence, consider the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and the reduced density operator of its first qubit

$$\rho = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{\langle 00| + \langle 11|}{\sqrt{2}}$$
$$\rho^1 = \frac{|0\rangle \langle 0| \langle 0|0\rangle + |1\rangle \langle 0| \langle 0|1\rangle + |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 1| \langle 1|1\rangle}{2}$$
$$= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2}$$
$$= \frac{I}{2}$$

Oddly, $\text{tr}\left(\frac{I^2}{4}\right) = 1/2 < 1$ so the first qubit is in a mixed state despite the system as a whole being in a pure state. This is another hallmark of quantum entanglement.

Exercise 1.9. *(2.74) Suppose a composite of systems A and B is in state $|a\rangle |b\rangle$, where $|a\rangle$ is a pure state of system A and $|b\rangle$ is a pure state of system B. Show that the reduced density operator of system A alone is a pure state.*

Proof.

$$\rho = |a\rangle |b\rangle \langle a| \langle b|$$
$$\rho^A = |a\rangle \langle a| \langle b|b\rangle = |a\rangle \langle a|$$

where we were given that $|a\rangle$ is a pure state. □

Exercise 1.10. *(2.75) For each of the four Bell states, find the reduced density operator for each qubit*

Proof. First, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

$$\rho = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{\langle 00| + \langle 11|}{\sqrt{2}}$$

$$\rho^1 = \frac{|0\rangle \langle 0| \langle 0|0\rangle + |1\rangle \langle 0| \langle 0|1\rangle + |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 1| \langle 1|1\rangle}{2}$$

$$= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

$$\rho^2 = \frac{|0\rangle \langle 0| \langle 0|0\rangle + |1\rangle \langle 0| \langle 0|1\rangle + |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 1| \langle 1|1\rangle}{2}$$

$$= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

Next, $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$

$$\rho = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \frac{\langle 00| - \langle 11|}{\sqrt{2}}$$

$$\rho^1 = \frac{|0\rangle \langle 0| \langle 0|0\rangle - |1\rangle \langle 0| \langle 0|1\rangle - |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 1| \langle 1|1\rangle}{2}$$

$$= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

$$\rho^2 = \frac{|0\rangle \langle 0| \langle 0|0\rangle - |1\rangle \langle 0| \langle 0|1\rangle - |0\rangle \langle 1| \langle 1|0\rangle + |1\rangle \langle 1| \langle 1|1\rangle}{2}$$

$$= \frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

The remaining two are similar. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

1.4   Quantum Teleportation

Quantum teleportation is a procedure for sending quantum information from Alice to Bob, given that Alice and Bob share an EPR pair, and have a classic communications channel. Recall that the need for Alice to communicate her result to Bob prevents faster than light communication.

The state to be teleported is $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. We can use the circuit shown in the figure below to perform this telerportation, with inputs $|\psi\rangle |\beta_{00}\rangle$ where $|\beta_{00}\rangle$ is the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Hence,

$$|\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \Big[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle) \Big]$$
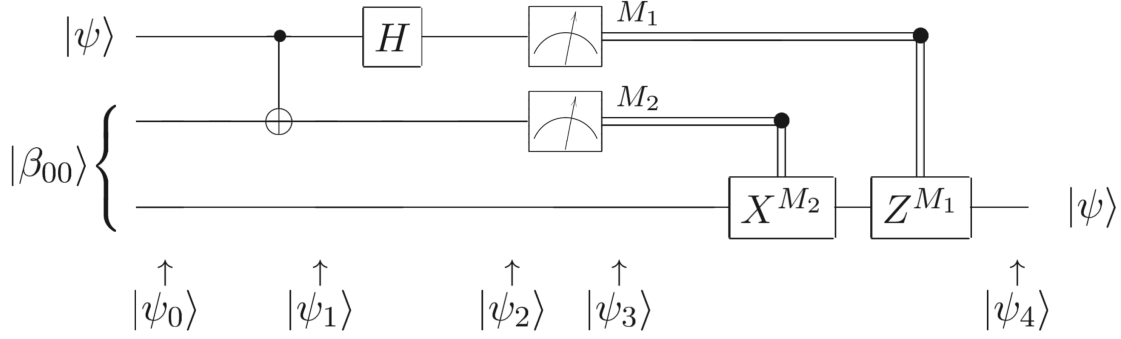
Figure 1: Two top lines are Alice's system and bottom is Bob's

Recall the controlled-NOT (CNOT) takes $|a\rangle |b\rangle$ to $|a\rangle |b \oplus a\rangle$. The other gates in the circuit are summarized in the diagram below.

Figure 2: Basic gates

So, the first two qubits belong to Alice and the third to Bob. Alice sends her qubits through a CNOT obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)\Big]$$

Then, Alice's first qubit is sent through a Hadamard gate which gives

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big]$$
$$= \frac{1}{2}\Big[|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)\Big]$$

Now, observe that each grouping in this expression has Alice's bits in a different state $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$, each of which Alice may observe after a measurement. Curiously, each of these groupings has a unique corresponding state for Bob's qubits. Hence, we know the state of Bob's qubits given knowledge of the outcome of Alice's measurement.

14

Furthermore, note that each of the possible states of Bob's qubits after Alice's measurements can be readily transformed to $|\psi\rangle$. Consider the four cases

1. Alice measures 00. Hence, Bob's state is already $|\psi\rangle$.

2. Alice measures 01. Hence, Bob's state is $\alpha|1\rangle + \beta|0\rangle$. So, just apply the X gate.

3. Alice measures 10. Hence, Bob's state is $\alpha|0\rangle - \beta|1\rangle$. So, just apply the Z gate to flip the second sign.

4. Alice measures 11. Hence, Bob's state is $\alpha|1\rangle - \beta|0\rangle$. So, apply the X gate to flip the bits, then the Z gate to flip the second sign.

So that's what the notation in the circuit above means, we apply X or Z to Bob's qubits to recover $|\psi\rangle$ depending on the outcome of Alice's measurement.

Pretty cool, right? Let's look at this a level deeper using the density operator formalism we've developed. Each of the 4 cases have probability $\frac{1}{4}$ of occurring. Hence, the density operator is given by

$$
\rho = \frac{1}{4}\Big[\, |00\rangle\langle00|\,(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle0| + \beta^*\langle1|) + |01\rangle\langle01|\,(\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle1| + \beta^*\langle0|)
$$
$$
+ |10\rangle\langle10|\,(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle0| - \beta^*\langle1|) + |11\rangle\langle11|\,(\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle1| - \beta^*\langle0|)\,\Big]
$$

So, the reduced density operator of Bob's system is

$$
\rho^B = \frac{1}{4}\Big[\, \langle00|00\rangle\,(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle0| + \beta^*\langle1|) + \langle01|01\rangle\,(\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle1| + \beta^*\langle0|)
$$
$$
+ \langle10|10\rangle\,(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle0| - \beta^*\langle1|) + \langle11|11\rangle\,(\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle1| - \beta^*\langle0|)\,\Big]
$$
$$
= \frac{1}{4}\Big[(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle0| + \beta^*\langle1|) + (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle1| + \beta^*\langle0|)
$$
$$
+ (\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle0| - \beta^*\langle1|) + (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle1| - \beta^*\langle0|)\Big] = \qquad \frac{1}{4}\Big[(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle0|
$$

1.5   EPR and the Bell Inequality

1.6   No-cloning Theorem

2   Nielsen & Chuang: Chapter 4

3   Nielsen & Chuang: Chapter 5

1. Quantum Fourier Transform

2. Quantum Phase Estimation Algorithm

3. Shor's algorithm for Factoring

4 Nielsen & Chuang: Chapter 6

Quantum Search algorithms

5 Algorithms for solving linear systems of equations

`https://arxiv.org/abs/0811.3171`

6 Density Matrix Exponentiation Algorithms

`https://www.nature.com/articles/nphys3029`

7 Review of Quantum Machine Learning

`https://www.nature.com/articles/nature23474`

8 Learnability of Quantum States

1. `https://arxiv.org/abs/quant-ph/0608142`

2. `https://arxiv.org/abs/1711.01053`

3. `https://arxiv.org/abs/1801.05721`

9 Appendix

9.1 Pauli Matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

9.2 Bell States

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

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

9.3 Positive Operators

Let A be a bounded[3] linear operator on complex Hilbert space $\mathcal{H}$. The following conditions are equivalent to A being positive

1. $A = S^\dagger S$ for some bounded operator S on $\mathcal{H}$

2. A is hermitian and $\langle x| A |x\rangle \geq 0$ for every $|x\rangle \in \mathcal{H}$

3. the spectrum of A is non-negative

9.4 Trace of an Operator

Let $\{|i\rangle\}$ be an orthonormal basis for A and so

$$\mathrm{tr}(A) = \sum_i A_{ii}$$

$$= \sum_i \langle i| A |i\rangle$$

Hence, if we extend $|\psi\rangle$ to the orthonormal basis $\{|i\rangle\}$ which includes $|\psi\rangle$ as the first element (for example via the Gram-Schmidt procedure) then

$$\mathrm{tr}(A |\psi\rangle \langle\psi|) = \sum_i \langle i| A |\psi\rangle \langle\psi|i\rangle$$

$$= \langle\psi| A |\psi\rangle$$

by orthonormality.

---

[3] $\|Av\| \leq M\|v\|$ for some $M > 0$ and all $v \in \mathcal{H}$

9.5   Spectral Theorem

Suppose A is a compact[4] hermitian operator (compactness ensures A has eigenvectors) on complex Hilbert space $\mathcal{H}$. Hence, there is an orthonormal basis of $\mathcal{H}$ consisting of eigenvectors of A. Each eigenvalue is in $\mathbb{R}$.

---

[4]the image under A acting on any bounded subset of $\mathcal{H}$ is a compact subset of $\mathcal{H}$