Notes on Quantum Information Processing

Edward Kim

January 10, 2020

1 Quantum Mechanics

1.1 Postulates of Quantum Mechanics

1.2 Density Matrices

Suppose we have an ensemble of states $\{|\psi_1\rangle, ..., |\psi_k\rangle\}$ in a statisitcal mixture in the sense that we know the distribution of the states. Let p_i denote the probability of selecting state $|\psi_i\rangle$ for $1 \leq i \leq k$ where $\sum_i p_i = 1$.

We wish to find a way to calculate the expected value of any observable A on this ensemble. Note that the linear superposition of these states in the form $\sum_{i=1}^{k} p_i |\psi_i\rangle$ is generally not the same as a statistical mixture of the individual states $|\psi_i\rangle$.

From Postulate three, we can calculate the probability that measuring with $A = \sum_i a_i P_i$ will yield outcome a_j:

$$p(j) = \sum_{i=1}^{k} p_i \langle\psi_i| P_j |\psi_i\rangle$$

Note that the $\langle\psi_i| P_j |\psi_i\rangle$ represent the probability of obtaining outcome a_j given the state vector is $|\psi_i\rangle$ as per postulate three. Thus, our expected value for the observable A would objects:

$$\langle A\rangle = \sum_{j=1}^{n} a_j p(j) = \sum_{j=1}^{n} a_i (\sum_{i=1}^{k} p_i \langle\psi_i| P_j |\psi_i\rangle) = \sum_{i=1}^{k} p_i \langle\psi_i| \sum_{i=1}^{n} a_j P_j |\psi_i\rangle = \sum_{i=1}^{k} p_i \langle\psi_i| A |\psi_i\rangle$$

Define the **density matrix** of the ensemble to be

$$\rho = \sum_{i=1}^{k} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$$

and $\langle A\rangle = Tr(\rho A)$. We verify this as follows:

$$Tr(\rho A) = \sum_{j=1}^{n} \langle j| \rho A |j\rangle = \sum_{j=1}^{n} \langle j| (\sum_{i=1}^{k} p_i |\psi_i\rangle \langle\psi_i|) A |j\rangle = \sum_{j=1}^{n}\sum_{i=1}^{k} p_i \langle j|\psi_i\rangle \langle\psi_i| A |j\rangle = \quad (1)$$

$$\sum_{i=1}^{k} p_i \langle\psi_i| A (\sum_{j=1}^{n} |j\rangle \langle j|) |\psi_i\rangle = \sum_{i=1}^{k} p_i \langle\psi_i| A |\psi_i\rangle = \langle A\rangle \quad (2)$$

where the next-to-last equality stems from the completeness criterion: $\sum_i |i\rangle \langle i| = I$. Thus, we have a method to describe expectation and probabilities in terms of operators rather than state vectors. Note that a pure state can be trivially described through the density matrix formalulation by $\rho = |\psi\rangle \langle\psi|$.

The density matrix has the following properties: Let $\{|i\rangle\}$ denote an orthogonal basis of our Hilbert space $\mathcal{H}$:

1. ρ **is Hermitian**: Let

   $$\rho_{ij} = \langle i| \rho |j\rangle = \sum_{m=1}^{k} p_m \langle i|\psi_m\rangle \langle\psi_m|j\rangle = \sum_{m=1}^{k} p_m c_i^{(m)} (c_j^{(m)})^*$$

   Thus,

   $$\rho_{ji}^* = \sum_{m=1}^{k} p_m (c_j^{(m)})^* c_i^{(m)} = \rho_{ij}$$

2. ρ **has unit trace** By our formula above:

   $$Tr(\rho) = \sum_{i=1}^{n} \rho_{ii} = \sum_{i=1}^{n}\sum_{m=1}^{k} p_m c_i^{(m)} (c_i^{(m)})^* = \sum_{m=1}^{k} p_m \sum_{i=1}^{n} |c_i^{(m)}|^2 = \sum_{m=1}^{k} p_m = 1$$

3. ρ **is non-negative**: Let $|\phi\rangle \in \mathcal{H}$. It suffices to prove that $\langle\phi| \rho |\phi\rangle \geq 0$.

1.3 Composite Systems

We can use the density matrix formalism to express statistical measurements in subsystems in the following sense:

Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be the *bipartite* separable system consisting of two subsystems expressed as Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$. By definition of the tensor product if $|\psi\rangle \in \mathcal{H}$, $|\psi\rangle$ has the form:

$$|\psi\rangle = \sum_{i,\alpha} c_i c_\alpha |i\rangle \otimes |\alpha\rangle = \sum_{i,\alpha} c_{i,\alpha} |i\rangle \otimes |\alpha\rangle$$

if we let $\{|i\rangle\}, \{|\alpha\rangle\}$ be sets of orthogonal basis vectors in $\mathcal{H}_1, \mathcal{H}_2$ respectively.

By our definiton in the previous section, the density matrix for our pure state $|\psi\rangle$ will be:

$$\rho = |\psi\rangle \langle\psi| = \sum_{i,\alpha} \sum_{j,\beta} c_{i,\alpha} (c_{j,\beta})^* |i\rangle |\alpha\rangle \langle j| \langle\beta|$$

Suppose we have an observable A_1 for subsystem $\mathcal{H}_1$, and we wish to find $\langle A_1 \rangle$ given $\mathcal{H}$. Let $A_1 \otimes I_B : \mathcal{H} \to \mathcal{H}$ be the unique linear map induced by $A_1 : \mathcal{H}_1 \to \mathcal{H}_1$ and $I_B : \mathcal{H}_2 \to \mathcal{H}_2$.

$$\langle A_1 \otimes I_B \rangle = Tr(\rho(A_1 \otimes I_B)) \tag{3}$$

2 Qubits

A **qubit** $|\Psi\rangle$ is the linear combination of basis elements $|0\rangle$ and $|1\rangle$ interpreted as a superposition of $0, 1$:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \alpha, \beta \in \mathbb{C}$$

Taking n tensor products of $|0\rangle$,$|1\rangle$ yields entangled states of n-qubits:

$$
\begin{gathered}
|0\rangle \otimes |0\rangle \ldots \otimes |0\rangle = |0....0\rangle \\
|0\rangle \otimes |0\rangle \ldots \otimes |1\rangle = |0....1\rangle \\
\ldots \\
|1\rangle \otimes |1\rangle \ldots \otimes |1\rangle = |1....1\rangle
\end{gathered}
$$

Let $\mathbb{C}^2$ be the 2 dimensional $\mathbb{C}$-vector space representing the space of superpostions of a single qubit. Then the n-qubit $\mathcal{H}_n$ can be represented as:

$$\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$$

In other words, if $|\Psi\rangle \in \mathcal{H}_n$, then

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \quad c_i \in \mathbb{C}$$

by definition of the n-tensor product of the 2-dimensional complex vector space.

3 Quantum Gates

Quantum gates are esstentially unitary operators on Hilbert spaces. These unitary operators act on single qubits by rotating them along the Bloch sphere.

3.1 Hadamard Gates

There are many gates that do not have classical analouges. One example is the Hadamard gate $H : \mathbb{C}^2 \to \mathbb{C}^2$

$$
\begin{aligned}
|0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|1\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
$$

which is represented as the matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

We can see from the definition that H takes a qubit and sends it to a superposition between $|0\rangle, |1\rangle$. H is unitary as $H^2 = I$:

$$H^2 = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^2 = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$$

Thus, H also takes superpositions of $|0\rangle, |1\rangle$ to single-state qubits.

We can directly calculate the effect the Hadamard gate has on n-qubits as such:

$$H^{\otimes n} |j_{n-1} ... j_0\rangle = \frac{1}{\sqrt{2^n}} \prod_{l=0}^{n-1} (|0\rangle + e^{i\pi j_l} |1\rangle)$$

where $j_i = \{0, 1\}$ for $0 \leq i \leq n-1$.

Consequently, an *equal* superposition where the probabilities for measuring a given n-qubit state are uniform:

$$H^{\otimes n} |0...0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

This superposition is instrumental in many quantum algorithms such as Grover's algorithm to extract useful information from oracles.

3.2 CNOT Gates

Define the CNOT (Controlled-Not Gate) as the operator which takes a 2-qubit system sends them as follows:

$$\begin{aligned}
|0\rangle|0\rangle &\mapsto |0\rangle|0\rangle \\
|0\rangle|1\rangle &\mapsto |0\rangle|1\rangle \\
|1\rangle|0\rangle &\mapsto |1\rangle|1\rangle \\
|1\rangle|1\rangle &\mapsto |1\rangle|0\rangle
\end{aligned}$$

The qubit on the bottom (target qubit) flips in respect to the value of the top qubit (control qubit). The corresponding matrix representation of $CNOT : \mathbb{C}^2 \to \mathbb{C}^2$ is:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

We can extend this idea to create a set of *generalized* CNOT gates with the following matrices:

4 Quantum Algorithms

4.1 Deutsch-Jozsa Algorithm

Let $f : \{0, 1\} \to \{0, 1\}$ be a boolean function with one-bit input. We would like to ascertain if f is either constant (both inputs have the same value) or balanced (inputs have different values). Through the classical perspective, one would have to query the function twice to determine the state of f as constant or balanced. However, we can leverage quantum mechanics so that f will only have to the queried once.

We will