PHYS 7895: Quantum Information Theory Fall 2015

Lecture 5 — September 13, 2015

Prof. Mark M. Wilde *Scribe: Yifan Yang*

1 Overview

In the last lecture we defined and exploited important properties of a conditionally typical set and obtained a detailed proof of Shannon's channel capacity theorem. We also discussed decoding algorithm and showed the achievability of an $(n, C(\mathcal{N}) - \delta, \varepsilon)$ channel code for all $\delta > 0, \varepsilon \in (0, 1)$, where $C(\mathcal{N})$ is the mutual information of a classical channel $\mathcal{N}$.

In this lecture we review the basics of the noiseless quantum theory: quantum bits, matrix representations, and unitary rotation operations. We discuss the three steps in quantum information processing. A proof of the No-Cloning theorem also will be discussed. Going forward from this lecture, we can see more interesting protocols such as teleportation, super-dense coding, Bell inequalities, quantum data compression, classical communication, quantum error correction, and quantum capacity.

2 The Noiseless Quantum Theory

The Noiseless Quantum Theory applies to closed quantum systems which do not interact with their surroundings and thus are not subject to corruption and information loss. However, quantum noise is inherent in nature and is due to nature, an example of the noise is the "Heisenberg noise," which is the noise resulting from measuring a quantum system.

State preparation, quantum operations, and measurement are three steps of information processing. In a quantum communication protocol, spatially separated parties may execute different parts of the steps, and we are interested in keeping track of the non-local resources needed to implement a communication protocol.

2.1 Quantum Bits

A *qubit* a the simplest two-level quantum system. Quantum states are represented by rays in Hilbert space (we limit our discussion to finite dimensions). A general qubit is an arbitrary *superposition* of states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle \equiv \alpha |0\rangle + \beta |1\rangle , \tag{1}$$

where the coefficients α and β are *probability amplitudes*. They are arbitrary complex numbers with unit norm:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

The unit-norm constraint leads to the *Born rule* (the probabilistic interpretation) of the quantum theory. States $|0\rangle$ and $|1\rangle$ can be represented as the following column vectors:

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \tag{3}$$

$$|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{4}$$

In Dirac notation $|0\rangle$ and $|1\rangle$ are called "kets," and the "bras" $\langle 0|$ and $\langle 1|$ are the matrix conjugate transpose of the kets. The superposition state in (1) then has a representation:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \tag{5}$$

We interpret states as being the same as $e^{i\phi}|\psi\rangle \approx |\psi\rangle$ for some phase ϕ. Furthermore, the dual of a ket is called a bra and is the conjugate transpose of the ket:

$$|\psi\rangle = \alpha^*\,\langle 0| + \beta^*\,\langle 1| \tag{6}$$

where

$$\langle 0| \equiv \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \langle 1| \equiv \begin{bmatrix} 0 & 1 \end{bmatrix}. \tag{7}$$

2.2 Reversible Evolution

2.2.1 Pauli Matrices:

Pauli matrices are the most important matrices for understanding qubits. Classically, there are just two interesting operations for a single bit: do nothing or flip it. Quantumly, we take the computational basis as the *standard basis* for representing physical qubits. There are three interesting principal axes on Bloch sphere and we can perform NOT (flip) operations with respect to each of these axes. There are four Pauli operators when we choose the computational basis as the standard basis:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{8}$$

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{9}$$

It is easy to check that $Y = iXZ$, and for this reason, we can think of the Y operator as a combined bit and phase flip. The four matrices I, X, Y, and Z are special for the manipulation of physical qubits.

- X, Y – flip state on Z axis.
- Y, Z – flip state on X axis..
- X, Z – flip state on Y axis..

2.2.2 Rotation Operators and Bloch Sphere

We now discuss "rotation evolutions" of quantum states which provide a picture of the Bloch sphere. Because of the unit-norm constraint, pure states in quantum theory lie on the surface of a sphere called Bloch sphere. For the qubit state: $\alpha |0\rangle + \beta |1\rangle$, set $\alpha = r_0 e^{i\phi_0}$, $\beta = r_1 e^{i\phi_1}$, then factor out the global phase ϕ_0 we get:

$$r_0 |0\rangle + r_1 e^{i\phi_1} |1\rangle \tag{10}$$

we can express any state in terms of two parameters θ and ϕ : $r_0 = \cos(\frac{\theta}{2})$, $r_1 = \sin(\frac{\theta}{2})$ for $0 \leq \theta \leq \pi$ and $\phi \equiv \phi_0 - \phi_1$.

More generally, the rotation operators $R_X(\phi)$, $R_Y(\phi)$, $R_Z(\phi)$ are functions of the respective Pauli operators X, Y, Z where

$$R_X(\phi) \equiv \exp\{iX\phi/2\}, \tag{11}$$

$$R_Y(\phi) \equiv \exp\{iY\phi/2\}, \tag{12}$$

$$R_Z(\phi) \equiv \exp\{iZ\phi/2\}, \tag{13}$$

and ϕ is some angle such that $0 \leq \phi < 2\pi$. A Hermitian operator A has a spectral decomposition $A = \sum_{i:a_i \neq 0} a_i |i\rangle \langle i|$ for some orthonormal basis $\{|i\rangle\}$. Then the operator $f(A)$ for some function f is defined as follows:

$$f(A) = \sum_{i:a_i \neq 0} f(a_i) |i\rangle \langle i|. \tag{14}$$

Figure 1 provides a more detailed picture of the Bloch sphere since we have now established the Pauli operators and their eigenstates. The computational basis states are the eigenstates of the Z operator and are the north and south poles on the Bloch sphere. For this state in classical theory are at the corners of the simplex. The $+/-$ basis states are the eigenstates of the X operator.

2.2.3 Reversible Evolution

Physical systems evolve as time progresses. *If we do not measure of a closed quantum system, then its evolution is reversible.* With reversibility, the input state of an evolution can be determined with knowledge of the evolution and given output. A closed quantum state evolves according to a unitary operator. Such transformations are known as length-preserving transformations since $U^\dagger U = UU^\dagger = I$ and thus a unitary U preserves the norm of any vector on which it acts.

Consider applying an unitary operator U to the example qubit state $|\psi\rangle$, then $\langle\psi| U^\dagger U |\psi\rangle = \langle\psi| I |\psi\rangle = \langle\psi|\psi\rangle = 1$. This unitary evolution complements the assumption that a vector always has a unit amplitude for being itself.

Suppose a 'NOT' transformation acts on a superposition state: $X(\alpha |0\rangle + \beta |1\rangle)$. By linearity of the quantum theory, the X operator distributes so that the above expression is equal to: $\alpha X |0\rangle + \beta X |1\rangle = \alpha |1\rangle + \beta |0\rangle$. Thus, the NOT gate is reversible and flips the basis states $|0\rangle$ and $|1\rangle$.

There is a big difference with classical probability theory: a continuous unitary transformation gets us from one pure state to another, i.e., we should be able to 'build up' any unitary from many unitaries that each differ from the identity by an infinitesimally small amount.

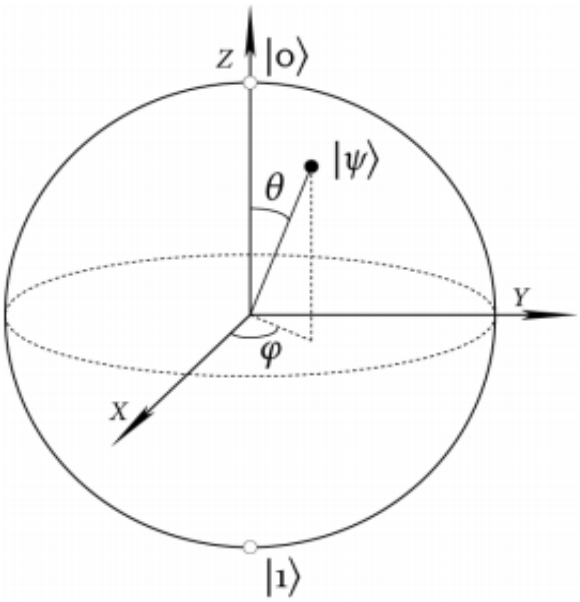

Figure 1: This figure provides more labels for states on the Bloch sphere. The Z axis has its points on the sphere as eigenstates of the Pauli Z operator, the X axis has eigenstates of the Pauli X operator, and the Y axis has eigenstates of the Pauli Y operator. The rotation operators $R_X(\phi)$, $R_Y(\phi)$, and $R_Z(\phi)$ rotate a state on the sphere by an angle ϕ about the respective X, Y, and Z axis.

2.3 Composite Quantum Systems

A composite quantum system is needed in quantum information-processing tasks. Generalizing the case of states of a single system, states of composite systems are rays in a tensor-product Hilbert space.

Consider two classical bits c_0 and c_1. The space of all possible bit values for an ordered pair (c_1, c_0) is the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_2$ of two copies of the set $\mathbb{Z}_2 \equiv \{0, 1\}$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \equiv \{(0,0), (0,1), (1,0), (1,1)\}. \tag{15}$$

However,the Cartesian product is not rich enough to capture the states of multi-particle quantum systems. In quantum theory, any possible linear combination of the set of two-cbit states is a possible two-qubit state:

$$|\xi\rangle \equiv \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle. \tag{16}$$

along with the unit-norm condition $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

The tensor product is the simplest mathematical operation and rich enough to capture this structure. Suppose we have two two-dimensional vectors:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \qquad \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}. \tag{17}$$

The tensor product of these two vectors is

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \equiv \begin{bmatrix} a_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \\ b_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{bmatrix}. \tag{18}$$

Recalling the vector representation of the single-qubit states $|0\rangle$ and $|1\rangle$, the two-qubit basis states can be written with the following vector representations:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{19}$$

Then the vector representation of the superposition state in (16) is

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}. \tag{20}$$

Note that there are actually many different ways that we can write two-qubit states. The tensor product structure is what leads to the phenomenon of entanglement and it explains why Hilbert space is huge : 2^n parameters are needed for n qubits. It does not seem physically reasonable that quantum systems should be able to reach all states in Hilbert space in a reasonable amount of time. Nevertheless, this is our best description (similar issue with classical probability).

Another example of NOT transformation, consider the two-qubit state in (16). We can perform a NOT gate on the first qubit so that it changes to

$$\alpha\,|10\rangle + \beta\,|11\rangle + \gamma\,|00\rangle + \delta\,|01\rangle\,. \tag{21}$$

We can alternatively flip its second qubit:

$$\alpha\,|01\rangle + \beta\,|00\rangle + \gamma\,|11\rangle + \delta\,|10\rangle\,, \tag{22}$$

or flip both at the same time:

$$\alpha\,|11\rangle + \beta\,|10\rangle + \gamma\,|01\rangle + \delta\,|00\rangle\,. \tag{23}$$

These are all reversible operations.

2.4 Measurement

Measurement is another type of evolution that allows us to retrieve classical information from a quantum state. Nature only allows us to measure observables which in the quantum theory as Hermitian operators in part because their eigenvalues are real numbers and every measuring device

outputs a real number. Examples of qubit observables that we can measure are the Pauli operators X, Y, and Z.

The measurement postulate of the quantum theory is that immediate repetition of a measurement gives the same outcome. This leads to the *Born rule*, which states that the system reduces to the state $|0\rangle$ with probability $|\alpha|^2$ and reduces to the state $|1\rangle$ with probability $|\beta|^2$ after measuring in the basis $\{|0\rangle, |1\rangle\}$. The resulting probabilities are the squares of the probability amplitudes.

In any case, for any projective measurement, there is an orthonormal basis for it labeled as $|j\rangle$, we can write any quantum state with respect to this basis: $|\psi\rangle = \sum_j \alpha_j |j\rangle$. α_j is the probability amplitude, indicating that the probability of getting outcome j is $|\alpha_j|^2$.

Consider the Hermitian operator

$$\Pi_0 \equiv |0\rangle \langle 0| . \tag{24}$$

Π_0 is a projection operator because applying it twice has the same effect as applying it once: $\Pi_0^2 = \Pi_0$. It projects onto the subspace spanned by the single vector $|0\rangle$. A similar line of analysis applies to the projection operator

$$\Pi_1 \equiv |1\rangle \langle 1| . \tag{25}$$

The measurement postulate also extends to composite quantum systems. For a two-qubit quantum state $|\xi\rangle \equiv \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle$, the four probability amplitudes are as follows:

$$\langle 00|\xi\rangle = \alpha, \quad \langle 01|\xi\rangle = \beta, \quad \langle 10|\xi\rangle = \gamma, \quad \langle 11|\xi\rangle = \delta. \tag{26}$$

The projection operators corresponding to this measurement are as follows:

$$\Pi_{00} \equiv |00\rangle \langle 00| , \quad \Pi_{01} \equiv |01\rangle \langle 01| , \quad \Pi_{10} \equiv |10\rangle \langle 10| , \quad \Pi_{11} \equiv |11\rangle \langle 11| , \tag{27}$$

and apply the Born rule to determine the probabilities for each result:

$$\langle \xi| \Pi_{00} |\xi\rangle = |\alpha|^2 , \quad \langle \xi| \Pi_{01} |\xi\rangle = |\beta|^2 , \quad \langle \xi| \Pi_{10} |\xi\rangle = |\gamma|^2 , \quad \langle \xi| \Pi_{11} |\xi\rangle = |\delta|^2 . \tag{28}$$

2.4.1 Entanglement

We have briefly talked about entanglement in class which is a unique quantum phenomenon observed by Schrödinger.

Consider a simple, unentangled state that two parties, Alice and Bob, may share :

$$|0\rangle_A |0\rangle_B , \tag{29}$$

where Alice has the qubit in system A and Bob has the qubit in system B. Now, consider the composite quantum state $|\Phi^+\rangle_{AB}$:

$$|\Phi^+\rangle_{AB} \equiv \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) . \tag{30}$$

$|\Phi^+\rangle_{AB}$ is an entangled state : it is a uniform superposition of the joint state $|0\rangle_A |0\rangle_B$ and the joint state $|1\rangle_A |1\rangle_B$, and it is not possible to describe either Alice's or Bob's individual state in the noiseless quantum theory.

Definition 1 (Pure-State Entanglement)**.** *A pure bipartite state $|\psi\rangle_{AB}$ is entangled if it cannot be written as a product state $|\phi\rangle_A \otimes |\varphi\rangle_B$ for any choices of states $|\phi\rangle_A$ and $|\varphi\rangle_B$.*

Figure 2 gives a graphical depiction of entanglement: Alice and Bob are spatially separated and they possess the entangled state after some time. If they share the entangled state in (30), we say that they share one bit of entanglement.

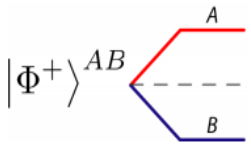

Figure 2: We use the above diagram to depict entanglement shared between two parties A and B. The diagram indicates that a source location creates the entanglement and distributes one system to A and the other system to B. The standard unit of entanglement is the ebit $|\Phi^+\rangle_{AB} \equiv (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$.

2.5 Quantum Information Processing in the Noiseless System

Any QIP protocol can be broken down into three simple parts: state preparation, quantum operations, and measurement. State preparation is the initialization of a quantum system to some beginning state. The input system for state preparation is a classical system, and the output system is quantum.

After initialization, we perform some quantum operations that evolve its state. Finally, the result of the computation is read out with a measurement. The input system for this step is quantum, and the output is classical. Figure 3 depicts all of these steps.

In quantum communication theory, we consider scenarios with spatially separated parties which may execute different parts of these steps. We allow each part an unbounded amount of computation and we only count the rate at which they consume or generate non-local resources such as classical communication channels, quantum communication channels, or shared entanglement.

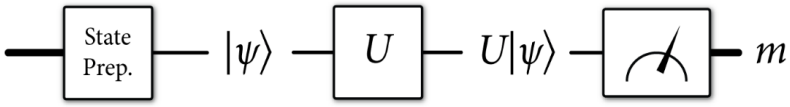

Figure 3: All of the steps in a typical noiseless quantum information processing protocol. A classical control (depicted by the thick black line on the left) initializes the state of a quantum system. The quantum system then evolves according to some unitary operation. The final step is a measurement that reads out some classical data m from the quantum system.

2.6 The No-Cloning Theorem

The No-Cloning theorem states that it is impossible to build a *universal copier* of quantum states. A universal copier would be a device that could copy any arbitrary quantum state that is input to it. A simple proof follows directly from the linearity of quantum mechanics.

Suppose there is a two-qubit unitary operator U acting as a universal copier of quantum information. That is, if we input an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as the first qubit and input an ancilla qubit $|0\rangle$ as the second qubit, such a device should "write" the first qubit to the second qubit slot as follows:

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle && (31)\\ &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) && (32)\\ &= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle . && (33) \end{aligned}$$

The copier is universal, meaning that it copies an arbitrary state. In particular, it also copies the states $|0\rangle$ and $|1\rangle$:

$$\begin{aligned} U|0\rangle|0\rangle &= |0\rangle|0\rangle , && (34)\\ U|1\rangle|0\rangle &= |1\rangle|1\rangle . && (35) \end{aligned}$$

From linearity, the unitary operator acts on a superposition $\alpha|0\rangle + \beta|1\rangle$ as follows:

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle . \quad (36)$$

However, the consequence in (33) contradicts the consequence in (36) because these two expressions do not have to be equal for all α and β:

$$\exists \alpha, \beta : \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \neq \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle . \quad (37)$$

Thus, linearity of the quantum theory contradicts the existence of a universal quantum copier.

But a specific cloner could exist. Observe that (37) is satisfied for $\alpha^2 = \alpha$, $\beta^2 = \beta$, and $\beta\alpha = 0$. Thus, it is satisfied for $\alpha = 1, \beta = 0$ or $\alpha = 0, \beta = 1$, so that we can copy unknown classical states prepared in the basis $|0\rangle, |1\rangle$ (or any other orthonormal basis for that matter). The no-cloning theorem has several applications in quantum information processing. First, it underlies the security of the quantum key distribution protocol because it ensures that an attacker cannot copy the quantum states that two parties use to establish a secret key. It finds application in quantum Shannon theory because we can use it to reason about the quantum capacity of a certain quantum channel known as the erasure channel.