CSE 291 / Math 277A - Quantum Complexity Theory September 22, 2022

Lecture 1

Lecturer: Daniel Grier *Scribe: Jon Stephens*

1 Introduction to the Course

As is the case with complexity courses the goal is to discover the inherent hierarchy of computational problems. With the realization of quantum computers the question of quantum complexity theory naturally becomes a topic of much interest. As is natural when studying complexity theory we ask the following questions. Is there any problem that a quantum computer can solve that no classical computer can solve? Is there any problem that an efficient quantum computer can solve that no efficient classical computer can solve?

The class BQP, Bounded-Error Quantum Polynomial Time, is the collection of problems which take in a classical input, perform a bounded-error polynomial time quantum algorithm that is then measured giving the correct classical output. One question of interest is where does BQP stand in the complexity classes? Is BQP in P, NP, PH, or PSPACE? What about BQP vs P, EXPTIME, or EEXP? For this we must discuss further quantum computation and its freedoms/limitations.

2 Basics of Quantum Bits and Probability

Single qubit In standard computation a bit can take the value 1 or 0. This bit is solidified into this choice when written and it cannot be anything other than it has been designated. In quantum bits we are allowed more freedom. Specifically, a qubit, quantum bit, will be allowed to be a "superposition" of both 0 and 1. This is analogous to a bit being 0 with certain probability and being 1 otherwise in the random computation model. Mathematically, we represent a qubit as a column vector in $\mathbb{C}^2$. For example,

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \cdot i \end{bmatrix}, \tag{1}$$

where the first coefficient is often referred as the "amplitude" for 0 and the second coefficient is the "amplitude" for 1. For convenience, we often write the basis vector as $|0\rangle, |1\rangle$ (commonly referred as the ket, bra notation)

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2}$$

In this notation, we can then rewrite the qubit in Equation (1) as

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}i|1\rangle. \tag{3}$$

The physical meaning of the two coefficients are best illustrated by the outcome of *measuring* the bit. If one were to measure the qubit's value, it would collapse into either the 0 state or the 1 state. Moreover, the probability of collapsing into one of the two states will be exactly the square of the corresponding amplitude, i.e. the outcome will be 0 with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ and the outcome will be 1 with probability $|\frac{1}{\sqrt{2}} \cdot i|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. The above postulate is often referred as the "Born" rule. For this reason, for a vector $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ to represent a valid state, we require its ℓ_2 norm to be exactly 1, i.e. $|\alpha|^2 + |\beta|^2 = 1$.

Multiple qubits We start with two random bits and then discuss how a two-qubit system can be viewed as a natural extension of the random system. Let A, B be two random bits. Each bit is allowed to have its own probability to have a 0 or a 1 and combining the two we can create the probability space associated to AB taking value 00, 10, 01 and 11. As an example we can consider the following two distributions for each bit taking values 0 or 1.

$$A = \begin{bmatrix} 0.3 \\ 0.7 \end{bmatrix}_A \begin{matrix} \leftarrow 0 \\ \leftarrow 1 \end{matrix} \qquad , \qquad B = \begin{bmatrix} 0.6 \\ 0.4 \end{bmatrix}_B \begin{matrix} \leftarrow 0 \\ \leftarrow 1 \end{matrix} \tag{4}$$

Then the associated probability space associated to A and B taking values 0 or 1 would give us the following vector.

$$AB = \begin{bmatrix} 0.18 \\ 0.12 \\ 0.42 \\ 0.28 \end{bmatrix}_{AB} \begin{matrix} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{matrix} \tag{5}$$

Now, let $|\phi\rangle$, $|\psi\rangle$ be two *qubits*.

$$|\phi\rangle = \begin{bmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{bmatrix} \begin{matrix} \leftarrow 0 \\ \leftarrow 1 \end{matrix} \qquad , \qquad |\psi\rangle = \begin{bmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{bmatrix} \begin{matrix} \leftarrow 0 \\ \leftarrow 1 \end{matrix} \tag{6}$$

Then, we can similarly consider the associated joint quantum system formed by ϕ and ψ, which is a superposition of the values 00, 10, 01 and 11. Such a quantum system can be described by a vector in $\mathbb{C}^4$.

$$|\phi\psi\rangle = \begin{bmatrix} \sqrt{0.18} \\ \sqrt{0.12} \\ \sqrt{0.42} \\ \sqrt{0.28} \end{bmatrix}_{AB} \begin{matrix} \leftarrow |00\rangle \\ \leftarrow |01\rangle \\ \leftarrow |10\rangle \\ \leftarrow |11\rangle \end{matrix} \tag{7}$$

The probability of getting different outcomes after measuring the system is still given by the square of the corresponding amplitude. This makes sense as one can see that the ℓ_2 norm of the vector $|\phi\psi\rangle$ is still 1. Besides, one can see that the vector of the joint system is exactly the *Tensor product* of the two vectors representing ϕ and ψ.

$$|\phi\psi\rangle = \begin{bmatrix} \sqrt{0.18} \\ \sqrt{0.12} \\ \sqrt{0.42} \\ \sqrt{0.28} \end{bmatrix}_{AB} = \begin{bmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{bmatrix} \otimes \begin{bmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{bmatrix} = |\phi\rangle \otimes |\psi\rangle.$$

In general, we may have a n-qubit system, which is described by 2^n different amplitude coefficients.

$$\text{1-qubit:} \quad \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \quad \text{with} \quad \sum_i |\alpha_i|^2 = 1. \tag{8}$$

$$\text{2-qubits:} \quad \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} \quad \text{with} \quad \sum_i |\alpha_i|^2 = 1. \tag{9}$$

$$\vdots$$

$$\text{n-qubits:} \quad \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n} \end{pmatrix} \quad \text{with} \quad \sum_i |\alpha_i|^2 = 1. \tag{10}$$

3 Quantum Operation and Unitary Matrices

As we have discussed before, a quantum system made up of n qubits can be mathematically represented as a vector in $|\phi\rangle \in \mathbb{C}^{2^n}$. Now, we would like to have some gate acting on qubits which can transform the system from one quantum state to another. One such example is the CNOT gate. The classical meaning of such a gate is clear: it acts on a two-qubit system and flips the second bit if and only if the first bit is 1.

$$\begin{gathered} 00 \to 00 \\ 01 \to 01 \\ 10 \to 11 \\ 11 \to 10 \end{gathered}$$

Its quantum extension can be viewed as a matrix/linear transformation that acts on vectors in $\mathbb{C}^4$.

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

In particular, the matrix is the unique linear operator which "respects" the mapping of the basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

In general, the gate allowed in the world of quantum computation can all be represented as linear operators acting on $\mathbb{C}^{2^n}$. More specifically, they are what we call the unitary matrix U satisfying the property

$$UU^\dagger = \mathbb{I}\,,$$

where by $U^\dagger$ we denote the conjugate transpose of U. To see why we need the operator to be unitary, we will need to digress a bit and refer back to probability theory. In the theory of stochastic process, we have stochastic matrices which map one probabilistic vector to another. Importantly, these matrices preserve the ℓ_1 norm of the input vector. In the quantum world, in order to map one valid quantum state to another, we instead require the operator to preserve the ℓ_2 norm. It turns out unitary matrices are exactly the family of linear operations that preserve the ℓ_2 norm.

Understanding these unitary matrices and their properties will be integral in understanding quantum computation. These matrices are invertible, meaning that any operations performed will be reversible. For any state $|\psi\rangle$ we can apply the unitary U to $|\psi\rangle$ to get $U|\psi\rangle$. By then applying U's conjugate transpose we get

$$U^\dagger(U|\psi\rangle) = (U^\dagger U)|\psi\rangle = |\psi\rangle \tag{11}$$

Hence, information is always recoverable if we use unitary matrices. Recall that, to describe a quantum system with two qubits, we simply use the tensor product between the two qubits.

$$|0\rangle_A \otimes |1\rangle_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_B = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{matrix} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{matrix} \tag{12}$$

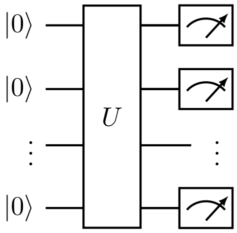
It is perfectly valid if one wants to apply two different gates U_A, U_B on the two qubits. In that case, similar to how we represent the state of the joint system, we can represent the "joint gate" itself also as a tensor product $U_A \otimes U_B$.

$$\text{If } U_A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad \text{then} \quad U_A \otimes U_B = \begin{pmatrix} a_{11}U_B & a_{12}U_B \\ a_{21}U_B & a_{22}U_B \end{pmatrix}. \tag{13}$$

Furthermore, it is worth noticing the following distributive property of tensor product.

$$(U_A \otimes U_B)|0\rangle_A \otimes |1\rangle_B = (U_A|0\rangle_A) \otimes (U_B|1\rangle_B). \tag{14}$$

In general, if we want to act on an n-qubit system using our Unitary matrices we know that U will have dimensions $2^n \times 2^n$. A common paradigm of quantum computation is simply to perform some unitary transformation on the qubits in the system and then measure the outcome of each of the qubit.



Altogether, there are as many as 2^n different outcomes, over which only some outcomes are desired. When we measure we get the result $i \in 2^n$ with probability $|\alpha_i|^2$. So if we want a consistent result then we must have some sort of probability condensation around one specific i.

4 Entanglement, Product, Density Matrix

Entanglement A state is *entangled* if it cannot be represented as a tensor product. Specifically, for two qubits, this means there is a selection of $\alpha, \beta, \gamma, \delta$ for which

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \neq (\alpha'|0\rangle + \beta'|1\rangle) \otimes (\gamma'|0\rangle + \delta'|1\rangle) \tag{15}$$

for any choice of $\alpha', \beta', \gamma', \delta'$. The CNOT gate mentioned before is a very common gate that is used to entangle qubits.

Inner Product and Outer Product For a collection of k states we may want to see how close one state is to another. Similarly, we may want to know how close all the states are to one another. One way to do so is via the dot product defined for the space $\mathbb{C}^n$. For that, we need the conjugate transpose of a vector. We refer to the notation $|\psi\rangle$ as a “Ket”. And we refer to $\langle\psi|$, the conjugate transpose of ψ as a “Bra”. Together they are a ”Bra-Ket” or ”Bracket”, $\langle\phi|\psi\rangle$, Whenever we write $\langle\phi|\psi\rangle$ we are taking the inner product between $|\phi\rangle$ and $|\psi\rangle$. Specifically, if we have two n dimensional column vectors $|\phi\rangle$ and $|\psi\rangle$, their inner product is then given by

$$\langle\phi|\psi\rangle = \begin{bmatrix} \bar{\phi_1} & \bar{\phi_2} & \dots & \bar{\phi_n} \end{bmatrix} \cdot \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{bmatrix} = \sum_{i=1}^{n} \bar{\phi}_i \psi_i. \tag{16}$$

We can also look at the “Ket-Bra” product and get an $n \times n$ matrix.

$$|\phi\rangle\langle\psi| = \begin{bmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{bmatrix} \cdot \begin{bmatrix} \bar{\psi_1} & \bar{\psi_2} & \dots & \bar{\psi_n} \end{bmatrix} = \begin{bmatrix} a_{ij} \end{bmatrix}_{i,j\in[n]} \text{ where } a_{ij} = \phi_i \bar{\psi_j}. \tag{17}$$

Density Matrix The states we have described so far are called *pure* states. More generally, we may have a statistical mixture (or an ensemble) of pure states. This states are referred to as the *mixed* states. In particular, if we have a collection of pure states, $|\psi_i\rangle$ for $i \in [k]$, and associated probabilities, p_i for each of the state, we can construct the mixed state such that the state is $|\psi_i\rangle$ with probability p_i. Alternatively, the mixed state can be interpreted as the result of the following process

1. One uses a random number generator to get $i \in [k]$ with probability p_i.

2. Then, one uses a quantum circuit to prepare the pure state $|\psi_i\rangle$.

It turns out different ensembles of pure states may result in mixed states that are impossible to be distinguished through any experiment (or quantum algorithm). For this reason, what really "defines" a mixed state is actually the following concept of the "Density Matrix"

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i|. \tag{18}$$

If two mixed states have identical density matrix, they are information theoretically impossible to be distinguished. On the other hand, if two states have different density matrices, then they can be distinguished with some nonzero bias. Below, we give an example of an even statistical mixture of the state $|0\rangle$ and $|1\rangle$.

$$0.5|0\rangle\langle 0| + 0.5|1\rangle\langle 1| = 0.5 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} + 0.5 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \end{pmatrix} = 0.5 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 0.5 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0.5 \cdot \mathbb{I}. \tag{19}$$

If one were to perform a measurement of the system, one would observe $0, 1$ each with probability exactly $1/2$. One may wonder then how the system is different from the pure state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ as the probability distribution induced after measurement will be exactly the same. However, it turns out one can actually distinguish the two states. In particular, if one to perform any unitary transformation on the mixed state, the resulting density matrix will be invariant. In particular, the density matrix of the mixed state after any unitary transformation will be

$$U 0.5 \cdot \mathbb{I} \xrightarrow{ConjU} U \cdot 0.5\mathbb{I} \cdot U^\dagger = 0.5 \cdot \mathbb{I}.$$

However, for the pure state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, there is some unitary operation which can map it to the state $|0\rangle$. If one first applies the unitary operation and then performs a measurement, one would consistently observe $|0\rangle$ if the starting state were the pure state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. On the other hand, if the starting state were the mixed state, the unitary would do nothing and the measurement still yields $|0\rangle$ or $|1\rangle$ each with probability $1/2$.