COS 597A: Quantum Cryptography — Princeton University
Lecture 2 (September 18, 2018)
Lecturer: Mark Zhandry — Scribe: Benjamin Kuykendall

Notes for Lecture 2

Today we will define a mathematical model of quantum computing. We looked at the basics of this model last week, as well as some of the motivating quantum physics. But in this lecture and moving forward, we will drop the physics and work within the model we define.

1 Complex Numbers

A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + bi$$

for $a, b \in \mathbb{R}$ and a number i such that $i^2 = -1$. Thus a complex number is a point on a plane where the reals lie on the horizontal axis and the real multiples of i on the vertical. This is given in Figure 1.

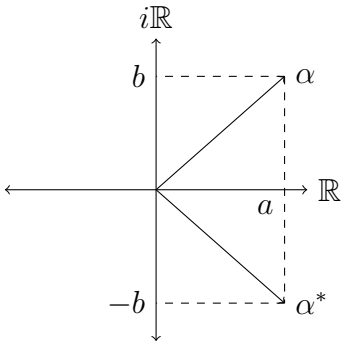

Figure 1: The points $\alpha = a + bi$ and $\alpha^* = a - bi$ in $\mathbb{C}$.

In addition to addition and multiplication, we can define some new operations on complex numbers:

Conjugate the conjugate of α is

$$\alpha^* := a - bi.$$

Graphically, this corresponds to flipping α about the horizontal axis.

Norm given by

$$|\alpha| := \sqrt{a^2 + b^2} = \sqrt{\alpha^* \alpha}.$$

This corresponds to the usual Euclidean distance in the picture below.

1.1 Linear Algebra over $\mathbb{C}$

Further, we can consider linear algebra over $\mathbb{C}$. Define two vectors $\phi, \psi \in \mathbb{C}^n$ and a square matrix $U \in \mathbb{C}^{n \times n}$:

$$\phi = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{pmatrix}, \quad \psi = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}, \quad U = \begin{pmatrix} U_{00} & U_{01} & \dots & U_{0n} \\ U_{10} & U_{11} & \dots & U_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ U_{n0} & U_{n1} & \dots & U_{nn} \end{pmatrix}.$$

In addition to the usual operations of linear algebra, we can define the following:

Inner product given by

$$\langle \phi | \psi \rangle := \sum_{j \in [n]} \phi_j^* \psi_j.$$

Inner products are sometimes denoted $\phi \cdot \psi$ or $\langle \phi, \psi \rangle$, but we will use this notation for reasons that will later become clear.

This inner product corresponds to the ℓ^2-norm: $\|\phi\|^2 = |\langle \phi | \phi \rangle| = \sum_{j \in [n]} |\phi_i|^2$.

Matrix conjugate is a transpose followed by component-wise complex conjugation:

$$\left(U^\dagger\right)_{ij} := (U_{ji})^*.$$

We also define two special types of matrices:

Hermitian matrix U such that $U = U^\dagger$.

Unitary transformation U such that $U^\dagger U = I$.

We will further explore the properties of unitary matrices. First note that U is unitary $\iff UU^\dagger = I \iff U^\dagger = U^{-1}$. These alternate characterizations follow easily by rearranging the definition. Further, note that U is unitary $\iff$ the columns of U are orthonormal vectors. This follows as:

$$\left(U^\dagger U\right)_{ij} = \sum_{k \in [n]} \left(U^\dagger\right)_{ik} \left(U\right)_{kj} = \sum_{k \in [n]} (U_{ki})^* U_{kj}.$$

2 Quantum States

Let B be a finite set of classical basis states. This can be any finite set. For example:

$B = \{\texttt{top-slit}, \texttt{bottom-slit}\}$ as in the double slit example.

$B = \{0, 1, 2, 3, 4\}$ or any arbitrary finite set.

$B = \{0, 1\}$ which is called a *qubit*.

$B = \{0, 1\}^n$ the bitstrings of length n.

Once we have chosen B, we can define a quantum state.

Definition 1 (Quantum state)**.** *A* quantum state *is a unit vector in* $\mathbb{C}^{|B|}$.

Thus to specify a quantum state it suffices to give $|B|$ complex numbers. We call these numbers the *amplitudes* associated with each $b \in B$. We can write states as column vectors. In order to manipulate vectors more easily, we introduce a new syntax for linear algebra called *bra-ket* notation:

Column vector ϕ written as $|\phi\rangle$ using the "ket" symbol.

Row vector $\phi^\dagger$ written as $\langle\phi|$ using the "bra" symbol.

Inner product $\phi \cdot \psi$ written as $\langle\phi|\psi\rangle$ a whole "bra-ket".

Using this syntax, we can introduce a special set of states. If $B = \{0, \ldots, n-1\}$ consider the vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Note that these states are classical states. Further, they form an orthonormal basis; we call it the *computational basis*. Thus, we can write any quantum state as a complex combination of the classical states:

$$|\phi\rangle = \phi_0 |0\rangle + \phi_1 |1\rangle + \cdots + \phi_{n-1} |n-1\rangle .$$

We call such combinations *superpositions*. More formally,

Definition 2 (Superposition)**.** *A state* $|\phi\rangle$ *is* in superposition *if there does not exist* $z \in \mathbb{C}$ *and* $i \in B$ *such that* $|\phi\rangle = z\,|i\rangle$.

The degree of freedom given by z in this definition might be unexpected. It appears here because overall phase-shifts in the state (i.e. replacing $|\phi\rangle$ with $e^{\pi i\theta}\,|\phi\rangle$) are not physically meaningful. For example, the states $|1\rangle$ and $i\,|1\rangle$ are equivalent for our purposes and both are considered classical non-entangled states.

3 Operations

Now that we have quantum states, we should specify what do to with them. There are two types of operations.

3.1 Unitary Transformations

If U is a unitary matrix, we can transform

$$|\phi\rangle \mapsto U|\phi\rangle .$$

Remember, the reason we are restricted to unitary matrices is in order to ensure the state remains a unit vector. We now have the tools to prove that this is the case.

Theorem 3. *If U is a unitary transformation then it preserves norm.*

Proof. In bra-ket notation

$$\|U\phi\|^2 = \langle U\phi|U\phi\rangle = \left\langle \phi\middle|U^\dagger U\phi\right\rangle = \langle\phi|I\phi\rangle = \langle\phi|\phi\rangle = \|\phi\|^2.$$

The second equality may be unclear; so far, we have no rules for moving things between the bra and ket. In order to justify this step, we can temporarily revert to linear algebra notation. Note that $(Ax)^\dagger = x^\dagger A^\dagger$ giving

$$\left\langle x\middle|A^\top y\right\rangle = x^\dagger A^\dagger y = (Ax)^\dagger y = \langle Ax|y\rangle . \qquad \square$$

Unitary transformations allow us to change one quantum state to another. We now need an operation to get usable classical information out of a quantum state.

3.2 Measurement

As we discussed last class, if you observe a photon exiting the two slits, you will see a classical result: the photon will go through either the top slit or the bottom slit. You both learn the classical information of which slit it went through and perturb the system, collapsing it into a classical state.

This example translates easily to our formal model. Let $|\phi\rangle$ be the state of a qubit, i.e. $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then upon measurement, we get one of the following results:

With probability $|\alpha|^2$: observe 0 and state collapses to $|0\rangle$.

With probability $|\beta|^2$: observe 1 and state collapses to $|1\rangle$.

This easily generalizes to a quantum state over B. For each $j \in B$:

With probability $|\langle j|\phi\rangle|^2$: observe j and state collapses to $|j\rangle$.

Thus, with these two types of operations defined, we can now write quantum procedures as a series of unitaries and measurements.

4 Classical vs. Quantum

Last class, we compared quantum procedures to randomized classical procedures. In summary: classical randomized procedures have states (i.e. probability distributions) with unit ℓ^1-norm (i.e. $\sum \alpha_i = 1$) and their operations (stochastic matrices) preserve ℓ^1-norm. Quantum procedures have states with unit ℓ^2-norm (i.e. $\sum |\alpha_i|^2 = 1$) and their operations (unitary transformations) preserve ℓ^2-norm.

Although we only made this transition due to the nature of quantum physics, we can try to generalize without physical motivation. To this end, what happens when we transition to ℓ^p-norm for arbitrary p? It turns out there is a mathematical reason why an ℓ^p-based computer would be undesirable.

Theorem 4. *For $p \notin \{0, 1\}$ the set of ℓ^p-norm preserving linear transformations is generated by*

1. *Phase-shifts of single coordinates: for some $j \in [n]$ and $\theta \in [0, 2\pi]$*
$$U|i\rangle = \begin{cases} e^{2\pi i\theta}|i\rangle & \text{if } i = j \\ |i\rangle & \text{otherwise.} \end{cases}$$
2. *Permutations of coordinates: for some permutation π on $[n]$:*
$$U|i\rangle = |\pi(i)\rangle .$$

This class of transformations is uninteresting: much less powerful than the ℓ^1-based or ℓ^2-based computations we are familiar with. Of course, we could consider non-linear transformations as well, but the resulting models are unusual in other ways which we will not explore.

5 Joint Systems

Stepping back to our model, consider a world with two qubits:

$$|\phi_0\rangle = \alpha_0|0\rangle + \beta_0|1\rangle$$
$$|\phi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle .$$

To describe the whole system, we take $B = \{0, 1\} \times \{0, 1\}$ in order to match the set of classical outcomes. Thus the computational basis of the joint state is

$$|0\rangle \otimes |0\rangle , \quad |0\rangle \otimes |1\rangle , \quad |1\rangle \otimes |0\rangle , \quad |1\rangle \otimes |1\rangle .$$

For brevity, we almost always omit the $\otimes$ and often simply write $|0\rangle|0\rangle = |00\rangle$. We can use distributivity to express $|\phi\rangle := |\phi_0\rangle|\phi_1\rangle$ in the computational basis.

$$\begin{aligned} |\phi_0\rangle|\phi_1\rangle &= (\alpha_0|0\rangle + \beta_0|1\rangle)(\alpha_1|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle . \end{aligned}$$

5.1 Entanglement

Consider another joint state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Note that $|\psi\rangle$ cannot be written as a tensor product of two qubits (to prove this, we can note that the matrix $\left(\begin{smallmatrix}\psi_{00} & \psi_{01}\\ \psi_{10} & \psi_{11}\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ has rank 2). Operationally, this means that the system cannot be described fully by two separate qubits. We call this *entanglement*. More precisely:

Definition 5 (Entanglement)**.** *A system of two qubits $|\phi\rangle$ is* entangled *when it cannot be written as the tensor product of qubits $|\phi_0\rangle$ and $|\phi_1\rangle$.*

Entanglement lets us create much more interesting quantum systems.

5.2 Partial measurement

Now that we have systems with multiple qubits, we want a way to measure one qubit but not the others. This follows from the same principles as before in the un-entangled case. Again let $|\phi\rangle = |\phi_0\rangle\,|\phi_1\rangle$. Then, a measurement of the first qubit leaves the second qubit the same.

With probability $|\alpha_0|^2$: observe 0 and state collapses to $|0\rangle\,|\phi_1\rangle$.

With probability $|\beta_0|^2$: observe 1 and state collapses to $|1\rangle\,|\phi_1\rangle$.

In the entangled case, we retain the same intuition, but writing out the result of measurement gets more complicated. Whenever we observe the first qubit in $|0\rangle$, all of the terms where the first qubit is in $|1\rangle$ must be dropped for the system to be consistent with our observations. To achieve this, we simply "cross out" the inconsistent terms from the state and re-normalize. More explicitly, when we measure the first qubit of $|\psi\rangle = \psi_{00}\,|00\rangle + \psi_{01}\,|01\rangle + \psi_{10}\,|10\rangle + \psi_{11}\,|11\rangle$,

With probability $\|\psi_{00}\|^2 + \|\psi_{01}\|^2$: observe 0 and state collapses to $\frac{\alpha_{00}|00\rangle+\alpha_{01}|01\rangle}{\sqrt{\|\psi_{00}\|^2+\|\psi_{01}\|^2}}$.

With probability $\|\psi_{10}\|^2 + \|\psi_{11}\|^2$: observe 1 and state collapses to $\frac{\alpha_{10}|10\rangle+\alpha_{11}|11\rangle}{\sqrt{\|\psi_{10}\|^2+\|\psi_{11}\|^2}}$.

This formalization agrees with our computation for the un-entangled case and allows us to partially measure any joint state.

5.3 Example

Consider the first qubit of $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as an example. Then:

With probability 1/2: observe 0 and state collapses to $|00\rangle$.

With probability 1/2: observe 1 and state collapses to $|11\rangle$.

Imagine we now measure the second qubit: we will always observe the same value in both measurements. This is the manner in which entanglement connects the values of two quantum states; the first measurement told us something about the second.

This setup allows for an interesting experiment: imagine we prepare two qubits in $|\psi\rangle$ and give them to different parties. The parties may travel some massive distance apart, and then simultaneously measure their respective qubits. The parties will always observe the same values, despite the distance; there is no speed-of-light delay. This is not a violation of causality because the parties cannot transmit information using it. However, it is still an unintuitive result of entanglement.

6 No-Cloning

It is easy to write a classical program that takes input x and outputs $x||x$. However, performing the equivalent task with qubits is impossible.

Theorem 6 (No-cloning)**.** *No quantum procedure transforms $|\phi\rangle \mapsto |\phi\rangle\,|\phi\rangle$ for all ϕ.*

We will prove a weaker version of this theorem: that no unitary transformation can clone a state. To prove the full version, you would need to consider measurements as well. Also, recall that unitaries are square matrices, so we need to add an "auxiliary qubit" to make the input and output the same size.

Theorem 7 (No-cloning (weakened))**.** *There is no unitary transformation such that $U\,|\phi\rangle\,|0\rangle = |\phi\rangle\,|\phi\rangle$ for all ϕ.*

Proof. Suppose we have such a U. Then using $U^\dagger U = I$ we have for any ψ, ϕ

$$\begin{aligned}
\langle\psi|\phi\rangle &= \langle 0|0\rangle\,\langle\psi|\phi\rangle \\
&= \langle\psi|\,\langle 0|\phi\rangle\,|0\rangle \\
&= \langle\psi|\,\langle 0|U^\dagger U|\phi\rangle\,|0\rangle \\
&= \langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle \\
&= |\langle\psi|\phi\rangle|^2.
\end{aligned}$$

Thus taking ψ, ϕ neither orthogonal nor equal we reach a contradiction. □

We have in fact proved something stronger: given any two ψ, ϕ that are neither orthogonal nor equal, there is no unitary matrix such that $U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ and $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$.

The no-cloning theorem can be seen as a limitation. Using similar techniques, we can show that one cannot learn with certainty what an arbitrary quantum state is. Intuitively, we would like to clone a state and then independently measure each copy. However, this approach is prohibited by the no-cloning theorem.

Alternatively, it can be seen as a cryptographic guarantee. In a classical channel, an eavesdropper can always copy the bits going through the channel and read them. However, in a quantum channel carrying qubits, the no-cloning theorem prevents this. If the eavesdropped party learns anything about the qubits, it must disturb the quantum state. This disturbance can be detected by the communicating parties.

This non-clonability can also be used to implement digital currency. It is desirable that a bank note cannot be copied; thus, perhaps a quantum state should serve as money.