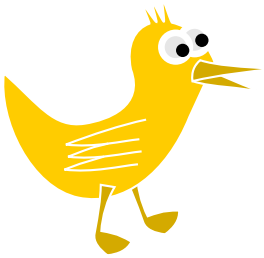
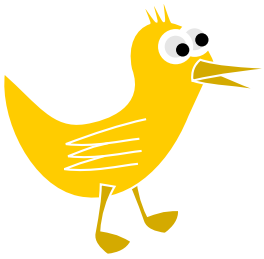


Lecture 2

In which we describe the quantum analogs of product distributions, independence, and conditional probability, and we describe the process of quantum teleportation, which is precisely what the name suggests.

Chapter 1



Measurements

Let Ω be our set of possible states (for example, $\{0,1\}^m$, if we are studying a computing device that has m bits of storage).

In the setting of probability, an event is a subset $E \subseteq \Omega$; for example we could have $\Omega = \{0,1\}^m$ and E be the set of binary strings where the first bit is one. If $p \in \mathbb{R}^\Omega$ is a probability distribution over Ω, then the probability, according to p, that a event E holds is

$$\mathbb{P}[E] := \sum_{a \in E} p_a$$

and the probability that E does not hold is

$$\mathbb{P}[\Omega - E] := \sum_{a \notin E} p_a$$

If we know that a certain system has a state that is distributed according to distribution p, and then we are told that even E holds, then the knowledge that E holds changes our distribution to the conditional distribution of p given E. This new distribution, let's call it p' is such that

- $p'_a = 0$ if $a \notin E$
- $p'_a = \frac{p_a}{\sum_{b \in E} p_b}$ if $a \in E$

Similarly, if we are told that E does not hold, our new distribution will be p' such that

- $p'_a = \frac{p_a}{\sum_{b \notin E} p_b}$ if $a \notin E$
- $p'_a = 0$ if $a \in E$

The rationale for the above rules is very natural: if we know that the event E happened, then clearly this makes the probability of any state outside of E to be zero. For the states inside E, the information that E happened does not change our estimate for their relative likelihood, and their probability should add up to one, and the only way to satisfy these two constraints is to multiply each probability by $1/\sum_{a \in E} p_a$.

In the quantum setting, if $q \in \mathbb{C}^\Omega$ is a pure quantum state over the state space Ω, a binary measurement is defined by a subset $E \subseteq \Omega$. The outcome of the measurement is one bit of information, that tells us whether our state is an element of E or not. For concreteness, we can think of $\Omega = \{0,1\}^m$ and E being the set of m-bit strings where the first bit is one. Then if $q \in \mathbb{C}^{\{0,1\}^m}$ is an m-qubit quantum state, measuring q according to E can be thought of as measuring the first of the m qubits.

The probability that the outcome of the measurement is "element of E" is

$$\sum_{a \in E} |q_a|^2$$

and the probability that the outcome of the measurement is "not element of E" is

$$\sum_{a \notin E} |q_a|^2$$

If the outcome of the measurement is "element of E," then we are left with a modified quantum state, in which states not in E have amplitude zero, and the other states maintain their relative amplitudes while still having the squares of the amplitudes summing to 1. Similarly to the rules for conditional probability, the new quantum state q' is such that

- $q'_a = 0$ if $a \notin E$
- $q'_a = \frac{q_a}{\sqrt{\sum_{b \in E} |q_b|^2}}$ if $a \in E$.

Similarly, if the outcome of the measurement is "not element of E," then the new quantum state after the measurement is

- $q'_a = \frac{q_a}{\sqrt{\sum_{b \notin E} |q_b|^2}}$ if $a \notin E$.
- $q'_a = 0$ if $a \in E$

For example, suppose that we have a 2-qubit quantum state $q \in \mathbb{C}^{\{0,1\}^2}$ such that

$$q = \begin{pmatrix} \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{3}} \end{pmatrix}$$

where the rows of q are indexed, top to bottom, by $00, 01, 10, 11$.

If we measure the first bit of the quantum state (corresponding to the event $\{10, 11\}$), then the outcome of the measurement will be 1 with probability $2/3$ and 0 with probability $1/3$.

If the outcome is 1, then the residual state will be

$$q = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

If the outcome is 0, then the residual state will be

$$q = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix}$$

In a more general type of measurement, we have a quantum state $q \in \mathbb{C}^{\Omega}$ and a partition $S_1, \ldots, S_k$ of Ω. In this case the outcome of the measurement is an element of $\{1, \ldots, k\}$; for each $i \in \{1, \ldots, k\}$, the probability that the outcome of the measurement is i is

$$\sum_{a \in S_i} |q_a|^2$$

and if the outcome of the measurement is i then the residual quantum state becomes the vector q' such that

- $q'_a = 0$ if $a \notin S_i$

- $q'_a = \frac{q_a}{\sqrt{\sum_{b \in S_i} |q_b|^2}}$ if $a \in S_i$

There is an equivalent and more linear-algebraic way of giving the above definitions. Suppose that $S_1, \ldots, S_k$ is a partition of Ω, and for each i let $M_i \in \mathbb{C}^{\Omega \times \Omega}$ be the projection matrix such that for every vector x we have $(M \cdot x)_a = x_a$ if $a \in S_i$ and $(M \cdot x)_a = 0$ if $a \notin S_i$. (That is, M_i is the matrix such that $M_{i,a,b} = 1$ if $a = b$ and $a \in S_i$ and $M_{i,a,b} = 0$ otherwise.) Then we have that

- For every i, the probability that the measurement of a quantum state q gives the outcome i is

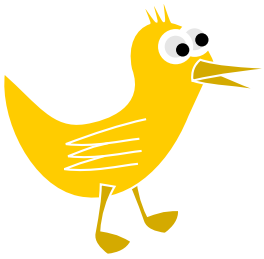
$$||M_i \cdot q||^2$$

- If the outcome of the measurement is i, then the residual state is

$$\frac{1}{||M_i \cdot q||} \cdot M_i \cdot q$$

The definition of measurement could be further generalized by considering an arbitrary collection of orthogonal projection matrices that sum to the identity (as described in the textbook) but the above level of generality will suffice for all applications.

Chapter 2



Ket notation

It is common in linear algebra to denote vectors with an overhead arrow, as in $\vec{v}$. In quantum mechanics, if v is a label chosen to represent a quantum state, then $|v\rangle$ is the notation for the corresponding vector. In particular, if Ω is a state space, then it is common, for every $a \in \Omega$, to use $|a\rangle$ to denote the vector in $\mathbb{C}^\Omega$ that has a 1 in the a-th coordinate and 0s everywhere else. (Such a vector corresponds to the "classical state a" in which a has amplitude one and all other states have amplitude zero.) Every pure quantum state can be written as a linear combination of vectors $|a\rangle$, usually resulting in a more readable expression than writing the vector as a $1 \times |\Omega|$ array. For example, the quantum state over $\Omega = \{0,1\}^2$ that we used as an example above can be written as

$$\frac{1}{\sqrt{6}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle - \frac{1}{\sqrt{3}}|11\rangle$$

which expresses much more clearly which states has which amplitudes compared with the notation

$$\begin{pmatrix} \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{3}} \end{pmatrix}$$

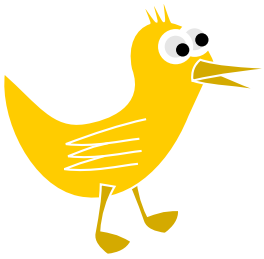
If $|v\rangle \in \mathbb{C}^\Omega$ is a vector, then $\langle v|$ denotes the conjugate transpose of v. With this

notation, the inner product between two vectors $|v\rangle$ and $|w\rangle$ can be written as the matrix product

$$\langle v| \cdot |w\rangle$$

(where the dot is usually omitted) which is suggestive of the standard notation $\langle v, w\rangle$.

Chapter 3



Tensor Products

Going back to the setting of probability, suppose that we have a sample space A and a probability distribution $p_A \in \mathbb{R}^A$ defined over A, and a sample space B and a probability distribution $p_B \in \mathbb{R}^B$ defined over B. Then we can define a probability distribution p over the product space $\Omega := A \times B$ by setting $p_{a,b} := p_a \cdot p_b$ (it is easy to verify that p is indeed a probability distribution) which corresponds to the probabilistic process of sampling an element from A according to p_A and, independently, an element from B according to p_B, thus selecting a pair in $A \times B$.

In linear algebra, if $x \in \mathbb{C}^A$ and $y \in \mathbb{C}^B$ are vectors, then their tensor product $x \otimes y \in \mathbb{C}^{A \times B}$ is defined as the vector such that $(x \otimes y)_{a,b} := x_a \cdot x_b$. This means that the above way of combining a distribution p_A over A and a distribution p_B over B to get a distribution over $A \times B$ is precisely the tensor product of p_A and p_B.

The quantum analog is as follows. If $q_A \in \mathbb{C}^A$ is a pure quantum state over the state space A and $q_B \in \mathbb{C}^B$ is a pure quantum state over the state space B, then the vector $q_A \otimes q_B \in \mathbb{C}^{A \times B}$ is a pure quantum state over the product space $A \times B$ (this can be easily verified), and it corresponds to the quantum state in which the part of the state encoded by A is in a superposition described by q_A, the part of the state encoded by B is in a superposition described by q_B, and the two parts are "independent," or, in the quantum terminology, not entangled. In general, if we can write a quantum state $q \in \mathbb{C}^{A \times B}$ as a tensor product $q_A \otimes q_B$ of two quantum states $q_A \in \mathbb{C}^A$ and $q_B \in C^B$, then we say that the information in A and the information in B of q are not entangled, otherwise we say that they are entangled.

For examples, returning to a quantum state that we already used in a previous example, consider the 2-qubit state

$$\frac{1}{\sqrt{6}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle - \frac{1}{\sqrt{3}}|11\rangle$$

it can be written as

$$\left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

and so it is a 2-qubit quantum state in which the two qubits are not entangled.

The quantum state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

instead, is an example of a 2-qubit quantum state in which the two qubits are entangled. (More about this state in the next subsection.)

A tensor product can also be defined for matrices. If $M_A \in \mathbb{C}^{A\times A}$ and $M_B \in \mathbb{C}^{B\times B}$ are matrices, then their tensor product is the matrix $M = M_A \otimes M_B$ such that

$$M_{(a,b),(a',b')} := M_{A,a,a'} \cdot M_{B,b,b'}$$

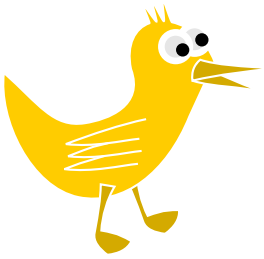
If $M_A \in \mathbb{R}^{A\times A}$ is a stochastic matrix that describes a probabilistic process over elements of A, and $M_B \in \mathbb{R}^{B\times B}$ is a stochastic matrix that describes a probabilistic process over elements of B, then $M = M_A \otimes M_B$ is a stochastic matrix (prove it) that describes a probabilistic process over pairs in $A \times B$; specifically, it is the process that operates on the first element of the pair according to M_A and, independently, on the second element of the pair according to M_B.

If $U_A \in \mathbb{C}^A$ and $U_B \in \mathbb{C}^B$ are unitary matrices, then their tensor product $U = U_A \otimes U_B$ is also a unitary matrix (prove it), and it corresponds to the quantum operator over the state space $A \times B$ that operates according to U_A on the first element of a state and according to U_B on the second element. For example, if we have a 4-qubit state space $\{0,1\}^5$, the operation that applies $U \in \mathbb{C}^{4\times 4}$ to the first two qubits and leaves the other three qubits unchanged is the operation $U \otimes I_8$, where I_8 is the 8×8 identity matrix.

Note that if $M_A \in \mathbb{C}^{A\times A}$ and $M_B \in \mathbb{C}^{B\times B}$ are matrices and $x \in \mathbb{C}^A$ and $y \in \mathbb{C}^B$ are vectors, then we have

$$(M_A \otimes M_B) \cdot (x \otimes y) = (M_A \cdot x) \otimes (M_B \cdot y)$$

Chapter 4



EPR Pairs

The quantum state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

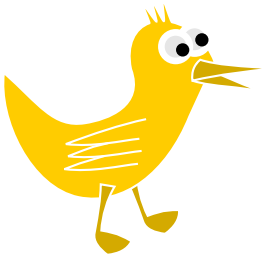
is called an EPR pair, because it was studied in a paper by Einstein, Podolsky and Rosen. The paper highlighted properties of such a quantum state that seemed to contradict physical intuition and to point to gaps in the theory of quantum mechanics. Later experiments have confirmed that EPR pairs can be generated in a laboratory and their behavior does obey the prediction of quantum mechanics.

The perceived problem with EPR pairs is as follows: particles do have binary properties, for example spin, and so it is possible to have to particles whose respective spins form the 2-qubit quantum state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Suppose now that these two particles with entangled spins are separated by a very large distance, say that we keep one particle in Palo Alto and move the other particle to New York. Now suppose that we measure the spin of the particle in Palo Alto. Because of the way, described above, in which measurements work, we will measure with probability 1/2 a spin 0 and with probability 1/2 a spin 1. No matter the outcome of the measurement, after we perform it, the spin of the particle in New York becomes determined, and equal to the spin that we measured in Palo Alto. This means that: (1) the quantum state of the particle in New York changed as an effect of the measurement we performed in Palo Alto, and (2) the quantum state of the particle in New York changed in a way that depends on the outcome of the measurement in Palo Alto. Einstein made fun

of prediction (1) as "spooky action at a distance," and the counterintuitive nature of prediction (2) is that the state of the particle in New York changes instantaneously after the experiment, even though information can never travel faster than the speed of light.

In any event, experiments have shown that EPR pairs can be created and behave according to the theory. We will not discuss the interesting question of how to interpret this prediction, and of how to develop a physical intuition for such phenomena.

Chapter 5



Unitary Transformations from Classical Bijective Functions

Suppose that $f : \Omega \to \Omega$ is a bijective function. Then we use f to define a unitary matrix U_f in the following way:

- $U_{f,a,b} = 1$ if $f(b) = a$
- $U_{f,a,b} = 0$ otherwise.

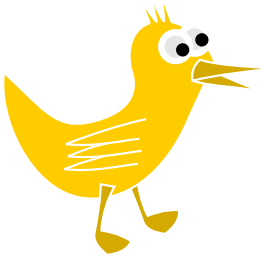
The matrix U_f is a unitary matrix because $U_f \cdot x$ is essentially the same vector as x, except that the coordinates of x are permuted according to f. In particular, the Euclidean norm of $U_f \cdot x$ and of x are the same.

It is easy to see that for every $a \in \Omega$ we have

$$U_f \cdot |a\rangle = |f(a)\rangle$$

That is, U_f is the matrix that, applied to a classical state, simply applies $f(\cdot)$ to the state. When U_f is applied to a more general quantum state it simply permutes the amplitudes according to f.

Chapter 6



Quantum Teleportation

Consider the following scenario: we are on the surface of a planet and we have found an object a that in a quantum superposition of two possible states, $|a\rangle = \alpha|0\rangle + \beta|1\rangle$. We also have a bit b that is half of an EPR pair $|bc\rangle$, while the other bit c is on a spaceship orbiting around the planet. We would like to teleport the quantum state a to the spaceship using only the ability to communicate classical messages between the surface of the planet and the spaceship. (As usual, teleporting an object means that the object at the source is destroyed and an identical copy is reconstituted at the destination.) One of the most remarkable things about this process is that the quantum state $|a\rangle$ is specified by two complex numbers, and thus it cannot be encoded with any finite number of classical bits, yet only two bits of classical information are exchanged between the planet and the spaceship.

Here is the "algorithm" for teleportation:

1. [On the planet] Apply the unitary transformation U_{CNOT} to the qubits a, b.
2. [On the planet] Apply the unitary transformation H to a.
3. [On the planet] Measure the qubits a, b and send the outcome of the measurement to the spaceship
4. [On the spaceship] If the outcome of the b measurement is 1, apply the unitary transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to c, else do nothing

5. [On the spaceship] If the outcome of the a measurement is 0, apply the unitary transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ to c, else do nothing.

We are going to prove that at the end of this algorithm, the bit a is in a classical state (hence it's "destroyed" as a quantum state) and the bit c has the same quantum state as a had at the beginning.

At the beginning, the three bits are in the quantum state s_0

$$|s_0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$
$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Applying the operator U_{CNOT} to the first two bits while doing nothing on the third bit corresponds to applying the operator $U_{CNOT} \otimes I_1$ to the whole state. The result can be computed by applying $U_{CNOT} \otimes I_1$ to each of the basis elements. For example,

$$(U_{CNOT} \otimes I_1) \cdot |000\rangle = (U_{CNOT} \otimes I_1) \cdot (|00\rangle \otimes |0\rangle)$$
$$= (U_{CNOT} \cdot |00\rangle) \otimes (I_1 \cdot |0\rangle)$$
$$= |00\rangle \otimes |0\rangle = |000\rangle$$

In general, applying $U_{CNOT} \otimes I_1$ to a basis state $|x_1x_2x_3\rangle$ gives the basis state $|CNOT(x_1, x_2)x_3\rangle$. So after the first step we have the state

$$|s_1\rangle = (U_{CNOT} \otimes I_1) \cdot |s0\rangle$$
$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

In the second step, we apply the transformation H to the first bit, that is, we apply the transformation $H \otimes I_2$ to the state s_1. For every basis vector of the form $|0x_2x_3\rangle$, we have

$$(H \otimes I_2) \cdot |0x_2x_3\rangle = \frac{1}{\sqrt{2}}|0x_2x_3\rangle + \frac{1}{\sqrt{2}}|1x_2x_3\rangle$$

and for every vector of the form $|1x_2x_3\rangle$ we have

$$(H \otimes I_2) \cdot |1x_2x_3\rangle = \frac{1}{\sqrt{2}}|0x_2x_3\rangle - \frac{1}{\sqrt{2}}|1x_2x_3\rangle$$

so at the second step we have the state

$$s_2 = (H \otimes I_2) \cdot |s_1\rangle$$
$$= \frac{1}{2}\left(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\right)$$

In the third step, we measure the first two bits. The measurement has four possible outcomes, and we continue the analysis by considering what happens in each case

- Outcome 00. This outcome happens with probability $\frac{1}{4}\alpha^2 + \frac{1}{4}\beta^2 = \frac{1}{4}$.

  If the measurement has outcome 00, then the residual quantum state is

  $$s_3 = \alpha|000\rangle + \beta|001\rangle = (|00\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

  which means that the bits on the planet are not entangled with the bits on the spaceship (and are, in fact, just the classical bits 00), while the bit on the spaceship has the exact state that the bit a had at the beginning.

- Outcome 01. This outcome happens with probability $\frac{1}{4}\alpha^2 + \frac{1}{4}\beta^2 = \frac{1}{4}$.

  If the measurement has outcome 01, then the residual quantum state is

  $$s_3 = \alpha|011\rangle + \beta|010\rangle = (|01\rangle) \otimes (\alpha|1\rangle + \beta|0\rangle)$$

  At this point, on the spaceship, we apply the transformation $U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ while we apply no operation to the bits on the planet, after which we have the state

  $$s_4 = (I_2 \otimes U_{NOT}) \cdot s_3 = (|01\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

  which means that the bits on the planet are not entangled with the bits on the spaceship (and are, in fact, just the classical bits 01), while the bit on the spaceship has the exact state that the bit a had at the beginning.

- Outcome 10. This outcome happens with probability $\frac{1}{4}\alpha^2 + \frac{1}{4}\beta^2 = \frac{1}{4}$.

  If the measurement has outcome 10, then the residual quantum state is

  $$s_3 = \alpha|100\rangle - \beta|101\rangle = (|10\rangle) \otimes (\alpha|0\rangle - \beta|1\rangle)$$

  At this point, on the spaceship, we apply the transformation $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ while we apply no operation to the bits on the planet, after which we have the state

$$s_4 = (I_2 \otimes Z) \cdot s_3 = (|10\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

which means that the bits on the planet are not entangled with the bits on the spaceship (and are, in fact, just the classical bits 10), while the bit on the spaceship has the exact state that the bit a had at the beginning.

- Outcome 11. This outcome happens with probability $\frac{1}{4}\alpha^2 + \frac{1}{4}\beta^2 = \frac{1}{4}$.

  If the measurement has outcome 11, then the residual quantum state is

  $$s_3 = \alpha|111\rangle - \beta|110\rangle = (|11\rangle) \otimes (\alpha|1\rangle - \beta|0\rangle)$$

  In the next step, on the spaceship, we apply the $U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, getting the state

  $$s_4 = (I_2 \otimes U_{NOT}) \cdot s_3 = (|11\rangle) \otimes (\alpha|0\rangle - \beta|1\rangle)$$

  The last step is to apply, on the spaceship, the transformation $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ while we apply no operation to the bits on the planet, after which we have the state

  $$s_5 = (I_2 \otimes Z) \cdot s_4 = (|11\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

  which means that the bits on the planet are not entangled with the bits on the spaceship (and are, in fact, just the classical bits 11), while the bit on the spaceship has the exact state that the bit a had at the beginning.