

APMA 1930W: Probabilities in Quantum Mechanics

Milan Capoor

Fall 2023

Lecture 1: Sept 6

Outline of the course:

1. A single particle
 - Probabilities
 - Waves
2. Entanglement (multiple particles)
3. Applications and consequences
 - Bell's theorem
 - Teleportation
 - Free will (Conway-Kochen theorem)
 - Encryption
 - Quantum computing

Lecture 2: Sept 8

The 2-Slit Experiment

A wave: we can imagine a 1-color wave at a single frequency

$$A \cos(\omega t - kx + \phi)$$

where

- ω is the frequency (rad/s) which describes the speed of vertical oscillation
- k is rad/m which describes speed of horizontal movement
- ϕ is the phase shift
- A is the amplitude

(the goal of the kx term is to grow proportionally with the ωt term to create a constant value without oscillation to send through the detector)

This wave can be decomposed:

$$A \cos(\omega t - kx + \phi) = A \cos \phi \cos(\omega t - kx) - A \sin \phi \sin(\omega t - kx)$$

Proof:

Using Euler's identity, $e^{iz} = \cos z + i \sin z$,

$$\begin{aligned} \Re(A \cos(\omega t - kx + \phi)) &= \Re(Ae^{i(\omega t - kx + \phi)}) \\ &= \Re(Ae^{i\phi}(\cos(\omega t - kx) + i \sin(\omega t - kx))) \\ &= \Re(A(\cos \phi + i \sin \phi)(\cos(\omega t - kx) + i \sin(\omega t - kx))) \\ &= A \cos \phi \cos(\omega t - kx) - A \sin \phi \sin(\omega t - kx) \end{aligned}$$

The Experiment: We imagine a variable with two narrow slits bombarded by the wave $\tilde{A} \cos(\omega t - kx)$.

Our goal is to find the equation of the wave impacting a detector at $x = 1$ after the diffusion effect of the variable. Because there are two slits, the waves (ψ_1, ψ_2) from each slit will interfere (linear sum) to create a new wave on the detector at a specific point $\psi(x, y, t)$ after traveling a distance r_1 or r_2 respectively. Thus,

$$\psi(x, y, t) = \psi_1(x, y, t) + \psi_2(x, y, t) = A_1 \cos(\omega t - kr_1) + A_2 \cos(\omega t - kr_2)$$

where $A_1 = \tilde{A}/\sqrt{r_1}$ and $A_2 = \tilde{A}/\sqrt{r_2}$ to take into account fading intensity over time.

All of this together will give us the amplitude of composite waves at the point on the screen which we square to get the intensity ($I \propto A^2$)

Calculated across the entire screen this will give a distribution of intensities which **perfectly** matches the distribution of collision locations of single-particles over a long period of time.

Lecture 3: Sept 11

Stern-Gerlach Experiment

We set up two non-symmetric magnets on top of each other with North pole facing South pole and a gap between them. We send an electron through and it will either go up or down to land on two specific points on the detector, indicating that each electron has a magnetic moment of exactly $\hbar/2$ or $-\hbar/2$.

Important findings:

1. This happens for ANY orientation of the machine
2. The result is definite. If we put a second S-G device at the detector point, ALL the particles that went up the first time will also go up the second time (and the same for down). That is,

$$\mathbb{P}(\lambda_n(t+1) = 1 | \lambda_n(t) = 1) = 1, \quad \mathbb{P}(\lambda_n(t+1) = 1 | \lambda_n(t) = -1) = 0$$

where λ_n is the state of the particle after going through the device ($\lambda_n : t \mapsto \{-1, 1\}$)

If we now send the particle through a new “m-machine” characterized by a new orientation $n, m \in \mathbb{R}_1^3 = \{v \in \mathbb{R}^3 : |v| = 1\} = S^2$, then the corresponding probabilities for a particle prepared in the n -direction is

$$\begin{aligned} \mathbb{P}(\lambda_m(t+1) = 1 | \lambda_n(t) = 1) &= \frac{1 + m \cdot n}{2} \\ \mathbb{P}(\lambda_m(t+1) = 1 | \lambda_n(t) = -1) &= \frac{1 - m \cdot n}{2} \end{aligned}$$

Now we create a new experiment. A stream of N $\lambda_x = 1$ particles go through an orthogonal z -detector such that $\mathbb{P}(\lambda_z = 1) = N/2$ and $\mathbb{P}(\lambda_z = -1) = N/2$. If we

magnetically bend these two back through the same x -detector so the input is $1/2 \lambda_z = 1$ and $1/2 \lambda_z = -1$, we still see $\mathbb{P}(\lambda_x = 1) = N$.

But! If we do not bend these into the same detector but place another x -detector after the z -detector we find that $\mathbb{P}(\lambda_x = 1 | \lambda_z = 1) = N/4$ and $\mathbb{P}(\lambda_x = -1 | \lambda_z = -1) = N/4$ – exactly what would have happened regardless of the earlier x -detector

Lecture 4: Sept 13

Feynman's Version: Using three machines in series, we are able to take an input, split it, and put it back together regardless of preparation. Using the normal process, we prepare $\lambda_x = 1$ then send it through one z -Feynman machine with the bottom blocked (so $\mathbb{P}(\lambda_z = 1) = N/2$) then through a x -Feynman machine with the top blocked so the final output is $\mathbb{P}(\lambda_x = -1) = N/4$

Now we set up a new experiment: send $\lambda_x = 1$ through a z -Feynman machine with no block then through a x -Feynman machine with the top blocked. The output is 0.

Conclusion: bending the streams back together is as if we never sent it through a machine at all because the particle is now in both states.

Derivation of State

Recall the Two-slit: we use complex variables to account for phase and model linear interference (See Lecture 2)

$$\psi(y, t) = \Re(y) e^{i\psi(y, t)} = A_1(y) e^{-ikr_1(y)} + A_2(y) e^{-ikr_2(y)}$$

In the Two-Slit Experiment the outcomes fall into \mathbb{R}^2 but in the Stern-Gerlach Experiment, there are only two possible outcomes.

Lecture 5: Sept 15

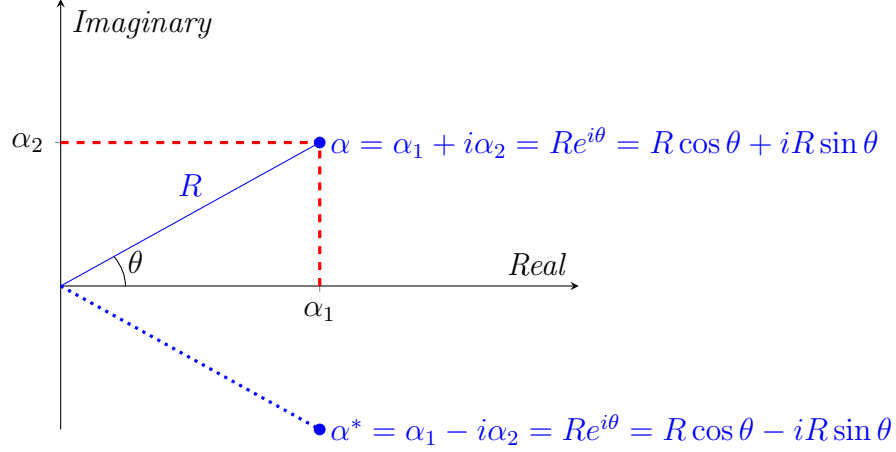
A Complex-valued Vector Space

(The complex-values conveniently handle phase while the vector space accounts for linear interference)

Our first task is to determine the dimensionality needed. From the experiment itself, we saw that \mathbb{R}_1^3 was sufficient to completely determine the system. Thus we do not

need a higher dimensional space than \mathbb{R}^3 . In mapping to the complex numbers, though, we observe that \mathbb{C}^2 already provides more degrees of freedom than we need.

Notation:



This gives us several identities:

$$\mathbb{R}^2 = \alpha_1^2 + \alpha_2^2 = |\alpha|^2 = \alpha^* \alpha = (\alpha_1 - i\alpha_2)(\alpha_1 + i\alpha_2)$$

From these, we see for $a \in \mathbb{C}^2$

$$\begin{aligned} a &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_1 + i\alpha_2 \\ \beta_1 + i\beta_2 \end{pmatrix} \\ \implies |a|^2 &= |\alpha|^2 + |\beta|^2 \\ &= \alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 \\ &= (\alpha^* \alpha) + (\beta^* \beta) \\ &= (\alpha_1 + i\alpha_2 \quad \beta_1 + i\beta_2)^* \begin{pmatrix} \alpha_1 + i\alpha_2 \\ \beta_1 + i\beta_2 \end{pmatrix} \quad (= a^\dagger a) \\ &= \alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 \\ &= \left| \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right|^2 \end{aligned}$$

($a^\dagger a$ is the composition of element-wise conjugate and transpose.)

Dirac Notation

For $\psi \in \mathbb{C}^2$ we use $\langle\psi|$ to designate the state of the particle corresponding to ψ .

Then we define

$$|\psi\rangle := \langle\psi|^\dagger = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger = (\alpha^*, \beta^*)$$

So

$$\langle\psi|\psi\rangle = \psi^\dagger\psi = |\psi|^2$$

Lecture 6: Sept 18

A Better State Space

Shortcomings of \mathbb{R}_1^3 :

- Nonlinear
- Arbitrary subset of a vector space
- No amplitudes
- Phase is difficult

Complex Space: $\mathbb{C} = \{\alpha_1 + i\alpha_2 | \alpha_1, \alpha_2 \in \mathbb{R}\}$

Which gives us a probability,

$$|\alpha|^2 = \alpha_1^2 + \alpha_2^2 = \alpha^* \alpha$$

2-Space: $\mathbb{C}^2 = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}$

For which we introduce Dirac notation (Bra-Ket notation):

$$|a\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

so

$$||a\rangle|^2 = \langle a|a\rangle = |a\rangle^\dagger |a\rangle = (\alpha^* \quad \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2$$

More generally:

$$|a\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} \delta \\ \gamma \end{pmatrix} \longrightarrow \langle a|b\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger \begin{pmatrix} \delta \\ \gamma \end{pmatrix} = \alpha^* \delta + \beta^* \gamma$$

We call $\langle a|b\rangle$ the **inner product** in \mathbb{C}^2 .

Rules of the Inner Product

Let $\eta_1, \eta_2 \in \mathbb{C}$ and $a_1, a_2, b \in \mathbb{C}^2$. Then

1. $\langle b|\eta_1 a_1 + \eta_2 a_2\rangle = \eta_1 \langle b|a_1\rangle + \eta_2 \langle b|a_2\rangle$ (Linearity in Ket)
2. $\langle a|b\rangle^* = \langle b|a\rangle$
3. $\langle \eta_1 a_1 + \eta_2 a_2|b\rangle = \eta_1^* \langle a_1|b\rangle + \eta_2^* \langle a_2|b\rangle$ (Conjugate linear in Bra)

Moving between the two formulations

Recall:

$$m, n \in \mathbb{R}_1^3 \implies \mathbb{P}(\lambda_n = 1 | \lambda_m = 1) = \frac{1 + m \cdot n}{2} = \cos^2\left(\frac{\theta}{2}\right)$$

Define:

$$\begin{aligned} |n^+\rangle &\in \mathbb{C}^2 \equiv \lambda_n = 1 \\ |n^-\rangle &\in \mathbb{C}^2 \equiv \lambda_n = -1 \equiv \lambda_{-n} = 1 \end{aligned}$$

So with $|n^*\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $|\alpha|^2 \propto$ probability of one outcome and $|\beta|^2 \propto$ the probability of the other outcome.

Then we limit \mathbb{C}^2 to

$$\mathbb{C}_1^2 = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} : \alpha, \beta \in \mathbb{C} \mid |\alpha|^2 + |\beta|^2 = 1 \right\}$$

So at last we have a probability formulation

$$|\langle m^+ | n^+ \rangle|^2 = \frac{1 + m \cdot n}{1} = \mathbb{P}(\lambda_m = 1 | \lambda_n = 1) = \mathbb{P}(\lambda_m = 1 \mid |\psi\rangle = |n^+\rangle)$$

Lecture 7: Sept 20

Goal: find the mapping $n \in \mathbb{R}_1^3 \rightarrow |n^+\rangle \in \mathbb{C}_1^2$ such that

$$\mathbb{P}(\lambda_m = 1 | |\psi\rangle = |n^+\rangle) = |\langle m^+ | n^+ \rangle|^2 = \frac{1 + m \cdot n}{2}$$

Remark: the product $\langle \psi | \phi \rangle$ is often called the *overlap* and is (basically) proportional to the degree of which one predicts the other

The Cardinal Directions

1. Up ($|u\rangle$)
2. Down ($|d\rangle$)
3. Left ($|l\rangle$)
4. Right ($|r\rangle$)
5. In ($|i\rangle$)
6. Out ($|o\rangle$)

By convention and arbitrarily, we begin by choosing a coordinate system and denoting

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Then with $|d\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$,

$$\langle u | d \rangle = 0 \implies \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha = 0$$

$$|d\rangle = \begin{pmatrix} 0 \\ \beta \end{pmatrix}$$

$$|\beta|^2 = 1 \implies \beta = e^{i\phi} \implies |e^{i\phi}|^2 = |e^{-i\phi} e^{i\phi}| = 1$$

$$|d\rangle = \begin{pmatrix} 0 \\ e^{i\phi} \end{pmatrix} = e^{i\phi} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \stackrel{\phi=0}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(ϕ can be arbitrary because only the relative phase matters)

Again, we begin

$$|r\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

From the Stern-Gerlach experiment, we know that

$$\begin{cases} |\langle u|r \rangle|^2 = \frac{1}{2} \\ |\langle d|r \rangle|^2 = \frac{1}{2} \end{cases} \implies \begin{cases} |\alpha|^2 = \frac{1}{2} \\ |\beta|^2 = \frac{1}{2} \end{cases} \implies \begin{cases} \alpha = \frac{1}{\sqrt{2}}e^{i\phi_1} \\ \beta = \frac{1}{\sqrt{2}}e^{i\phi_2} \end{cases} \implies |r\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}}e^{i\phi_1} \\ \frac{1}{\sqrt{2}}e^{i\phi_2} \end{pmatrix}$$

Again arbitrarily, we say $\phi_1 = \phi_2 = 0$ so

$$|r\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

This gives us three sets of constraints for $|l\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$:

$$\begin{aligned} \langle u|l \rangle &= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \\ \langle d|l \rangle &= \beta \\ \langle r|l \rangle &= \frac{1}{\sqrt{2}}\alpha + \frac{1}{\sqrt{2}}\beta \\ |\langle u|l \rangle|^2 &= \frac{1}{2} \\ |\langle d|l \rangle|^2 &= \frac{1}{2} \\ |\langle r|l \rangle|^2 &= 0 \end{aligned}$$

From all of this,

$$\begin{cases} \alpha^2 = \frac{1}{2} \implies \alpha = e^{i\phi_1} \frac{1}{\sqrt{2}} \\ \beta^2 = \frac{1}{2} \implies \beta = e^{i\phi_2} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}\alpha + \frac{1}{\sqrt{2}}\beta = \frac{1}{\sqrt{2}}e^{i\phi_1} + \frac{1}{\sqrt{2}}e^{i\phi_2} = 0 \implies e^{i\phi_1} = -e^{i\phi_2} \end{cases}$$

so

$$|l\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}}e^{i\phi_1} \\ \frac{1}{\sqrt{2}}e^{i\phi_2} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}e^{i\phi_1} \\ -\frac{1}{\sqrt{2}}e^{i\phi_1} \end{pmatrix}$$

We choose $\phi_1 = 0$ so

$$|l\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Lecture 8: Sept 22

Review

States:

\mathbb{R}_1^3	z	$-z$	x	$-x$	y	$-y$
Dirac \mathbb{C}_1^2	$ u\rangle$	$ d\rangle$	$ r\rangle$	$ l\rangle$	$ i\rangle$	$ o\rangle$
Linear Alg \mathbb{C}_1^2	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$

Generically,

$$n \in \mathbb{R}_1^3 \rightarrow |n^+\rangle \in \mathbb{C}_1^2$$

so

$$\mathbb{P}(\lambda_m = 1 | \lambda_n = 1) = \mathbb{P}(\lambda_m = 1 | |\psi\rangle = |n^+\rangle) = \frac{1 + m \cdot n}{2} = \cos^2 \frac{\theta}{2} = |\langle m^+ | n^+ \rangle|^2$$

Remarks:

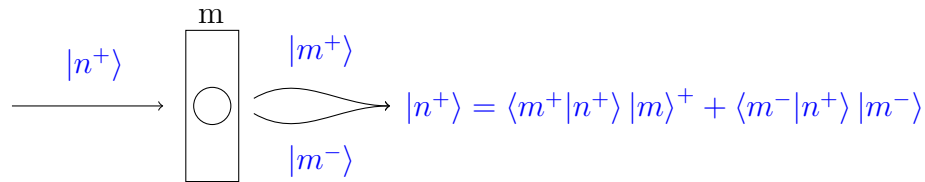
1. The representation in \mathbb{C}_1^2 is not unique.

$$\forall |\psi\rangle \in \mathbb{C}_1^2 : e^{i\phi} |\psi\rangle = |\psi\rangle$$

The Feynman Machine

We imagine $|n^+\rangle$ through an m -oriented Feynman S-G machine such that the up and down states are bent back together. We can say

$$|n^+\rangle = \langle m^+ | n^+ \rangle |m^+\rangle + \langle m^- | n^+ \rangle |m^-\rangle$$



Expectations

$$\begin{aligned}\mathbb{E}[\lambda_n | \psi\rangle = |m^+\rangle] &= |\langle n^+ | m^+ \rangle|^2 - |\langle n^- | m^+ \rangle|^2 \\ &= \frac{1 + m \cdot n}{2} - \frac{1 - m \cdot n}{2} \\ &= m \cdot n\end{aligned}$$

Or

$$\begin{aligned}\mathbb{E}[N \mathbb{1}_{\lambda_n=1} | \psi\rangle = |m^+\rangle] &= N \cdot \mathbb{E}[\mathbb{1}_{\lambda_n=1} | \psi\rangle = |m^+\rangle] \\ &= N |\langle m^+ | n^+ \rangle|^2\end{aligned}$$

Lecture 9: Sept 25

Mixtures and Superposition

By now, we have

$$|r\rangle = \frac{1}{\sqrt{2}} |u\rangle + \frac{1}{\sqrt{2}} |d\rangle$$

We want to calculate $\mathbb{E}[\lambda_x | \psi\rangle = |r\rangle]$

Mixture interpretation

We assume that because $|u\rangle$ and $|r\rangle$ are orthogonal, putting an $|\psi\rangle = |r\rangle$ prepared vector through an x machine will show it go up half the time and down half the time:

$$\begin{aligned}\mathbb{E}[\lambda_x | \psi\rangle = |r\rangle] &= \frac{1}{2} \mathbb{E}[\lambda_x | \psi\rangle = |u\rangle] + \frac{1}{2} \mathbb{E}[\lambda_x | \psi\rangle = |d\rangle] \\ &= \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 0 \\ &= 0\end{aligned}$$

But in reality,

$$\mathbb{E}[\lambda_x | \psi\rangle = |r\rangle] = \mathbb{P}(\lambda_x = 1 | \psi\rangle = |r\rangle) - \mathbb{P}(\lambda_x = -1 | \psi\rangle = |r\rangle) = 1$$

So $|r\rangle$ is NOT a mixture of $|u\rangle$ and $|d\rangle$. It is both at the same time.

Measurements

Hermitian Adjoint:

$$A \in \mathbb{C}^{m \times n} : A^\dagger = (A')^* = (A^*)'$$

Example:

$$A = \begin{pmatrix} i & 2 \\ 1+i & 1-i \\ 3 & 2i \end{pmatrix} \implies A^\dagger = \begin{pmatrix} -i & 1-i & 3 \\ 2 & 1+i & -2i \end{pmatrix}$$

Hermitian Matrix/Operator/Transform:

$$A \in \mathbb{C}^{n \times n} : A^\dagger = A$$

Example:

$$A = \begin{pmatrix} 3+2i & 1-i \\ 1-i & 2+i \end{pmatrix} \implies A^\dagger = \begin{pmatrix} 3-2i & 1+i \\ 1+i & 2-i \end{pmatrix} \implies A \neq A^\dagger \text{ so } A \text{ is not Hermitian}$$

$$A = \begin{pmatrix} 7 & 1+i \\ 1-i & 8 \end{pmatrix} \implies A^\dagger = A \text{ so } A \text{ is Hermitian}$$

Spectral Theorem:

$A \in \mathbb{C}^{n \times n}$ is a Hermitian matrix if and only if A has the form

$$A = \sum_{k=1}^n \lambda_k e_k e_k^\dagger = \sum_{k=1}^n \lambda_k |e_k\rangle \langle e_k|$$

where

- $\lambda_1, \dots, \lambda_n \in \mathbb{R}$
- $e_1, \dots, e_n \in \mathbb{C}^n$
- (The vectors are orthonormal:)

$$\langle e_k | e_l \rangle = e_k^\dagger e_l = \delta_{kl} = \begin{cases} 1 & \text{if } k = l \\ 0 & \text{if } k \neq l \end{cases}$$

(i.e. e_1, \dots, e_n are orthonormal eigenvectors with eigenvalues $\lambda_1, \dots, \lambda_n$)

Lecture 10: Sept 27

Examples of the Spectral Theorem

Example 1:

$$H = \begin{pmatrix} 3 & -i \\ i & 3 \end{pmatrix}$$

By the Spectral Theorem,

$$\begin{aligned} H &= \lambda_1 e_1 e_1^\dagger + \lambda_2 e_2 e_2^\dagger \\ &= 2 \begin{pmatrix} \frac{1+i}{2} \\ \frac{1-i}{2} \end{pmatrix} \begin{pmatrix} \frac{1+i}{2} \\ \frac{1-i}{2} \end{pmatrix}^\dagger + 4 \begin{pmatrix} \frac{1+i}{2} \\ \frac{-1+i}{2} \end{pmatrix} \begin{pmatrix} \frac{1+i}{2} \\ \frac{-1+i}{2} \end{pmatrix}^\dagger \end{aligned}$$

How do we check this?

Answer:

$$H e_1 = 2 e_1 \quad H e_2 = 4 e_2$$

(the action of the matrix on two orthogonal vectors defines the matrix)

Proof of the Spectral Theorem

Lemma: For a Hermitian matrix,

$$H = \sum_{k=1}^n \lambda_k e_k e_k^\dagger,$$

the values $\lambda_k \in \mathbb{R}$.

Proof:

Let λ be an eigenvalue with eigenvector e . Then

$$\begin{aligned} \lambda &= e^\dagger H e \\ \lambda^* &= \lambda^\dagger = (e^\dagger H e)^\dagger \\ &= e^\dagger H^\dagger e \\ &= e^\dagger H e \\ &= \lambda \end{aligned}$$

so λ is real.

Remark: the collection of eigenvalues λ_k are called the “spectrum”

Lecture 11: Sept 29

Motivating Hermitian Operators

Needing matrices becomes natural when we view state space as hilbert space and the matrices as linear operators on hilbert space.

Goal: find an operator o that maps a wave function to a particular state.

One potential is $|\psi\rangle \rightarrow |n^+\rangle$ using the **projection operators**:

$$|n^+\rangle\langle n^+|, \quad |n^-\rangle\langle n^-|$$

If we imagine σ_n as a particular state, then

$$\begin{aligned}\sigma_n |n^+\rangle &= \frac{\hbar}{2} |n^+\rangle \\ \sigma_n |n^-\rangle &= -\frac{\hbar}{2} |n^-\rangle\end{aligned}$$

So we note that there is a distinction between states ($\in \mathbb{C}_1^2$) and values (in \mathbb{R})

Actually working it out,

$$\begin{aligned}\sigma_n &:= |n^+\rangle\langle n^+| - |n^-\rangle\langle n^-| \\ \sigma_s |n^+\rangle &= |n^+\rangle\langle n^+ | n^+\rangle - |n^-\rangle\langle n^- | n^+\rangle \\ &= |n^+\rangle(1) - |n^-\rangle(0) = |n^+\rangle\end{aligned}$$

Observables

Definition: a Hermitian operator $\sum_i \lambda_i |e_i\rangle\langle e_i|$ with eigenvectors corresponding to states after measurement $|e_i\rangle$ and eigenvalues λ_i corresponding to the physical values we measure ($\{\pm\frac{\hbar}{2}\} \mapsto \{\pm 1\}$).

This also suggests that $|\langle e_i | \psi \rangle|^2$ is the probability of collapse onto a particular state $|e_i\rangle$

Computing spin states

$$\begin{aligned}
 \sigma_z &= |z^+\rangle \langle z^+| - |z^-\rangle \langle z^+| \\
 &\quad + (1 \ 0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} - (0 \ 1) \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
 \end{aligned}$$

Which we notice is a diagonal matrix with eigenvalues ± 1 .

In the same process,

$$\begin{aligned}
 |x^\pm\rangle &= \frac{1}{\sqrt{2}}(|z^+\rangle \pm |z^-\rangle) \\
 |y^\pm\rangle &= \frac{1}{\sqrt{2}}(|z^+\rangle \pm i|z^-\rangle) \\
 \sigma_x &= |x^+\rangle \langle x^+| - |x^-\rangle \langle x^+| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
 \end{aligned}$$

However, these matrices tell us nothing about the states or eigenvalues. To take any probabilities $|\langle z^+ | x^+ \rangle|^2$ we would need to know the explicit form of both vectors. But! We can *diagonalize* a given matrix to find the probability for any matrix.

Taken together, these three basis matrices are the *Pauli Matrices*:

$$\boxed{
 \begin{aligned}
 \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
 \sigma_x &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
 \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
 \end{aligned}
 }$$

Expected Value

$$A = \sum_i \lambda_i |e_i\rangle \langle e_i|$$

From probability theory, the expected value is just the sum of the probability times the value:

$$\begin{aligned}\mathbb{E}(A \mid |\psi\rangle) &= \sum_i |\langle e_i \mid \psi \rangle|^2 \lambda_i \\ &= \sum_i \langle \psi \mid e_i \rangle \langle e_i \mid \psi \rangle \lambda_i \\ &= \langle \psi \mid \left(\sum_i |e_i\rangle \langle e_i| \lambda_i \right) \mid \psi \rangle \\ &= \langle \psi \mid A \mid \psi \rangle\end{aligned}$$

Lecture 12: Oct 2

Recall

We can represent a particular observation by the Hermitian matrix H :

$$H = \sum_{k=1}^n \lambda_k |e_k\rangle \langle e_k|$$

where the vectors e_k form a complete orthonormal set and $\lambda_k \in \mathbb{R}$.

Then, given the starting state $|\psi\rangle$, the probability of the random result of making the observation represented by H , is

$$\mathbb{P}(\lambda_H = \lambda_k \mid |\psi\rangle) = |\langle e_k \mid \psi \rangle|^2$$

This leads to the formula for expected value:

$$\begin{aligned}\mathbb{E}[\lambda_H \mid |\psi\rangle] &= \sum_{k=1}^n \lambda_k \mathbb{P}(|e_k\rangle) \\ &= \sum_{k=1}^n |\langle e_k \mid \psi \rangle|^2 \lambda_k \\ &= \langle \psi \mid H \mid \psi \rangle\end{aligned}$$

Multiple measurements

Example: $H_1 = \sigma_x$ and $H_2 = -\sigma_x$ with $|\psi\rangle = |r\rangle$. Then $\lambda_1 = 1$ and $\lambda_2 = -1$ (deterministically).

In general, if H_1 and H_2 share eigenvectors, then order is “independent”:

$$|\psi\rangle \xrightarrow[\lambda_k^1]{H_1} |e_k^1\rangle \xrightarrow[\lambda_l^2]{H_2} |e_l^2\rangle$$

Question: When is $A = H_2 \cdot H_1$ a measurement? (i.e. when is it Hermitian?)

Answer: If and only if H_1 and H_2 are both hermitian and share the same eigenvectors:

$$H_1 = \sum_{k=1}^n \lambda_k^1 |e_k\rangle \langle e_k|$$
$$H_2 = \sum_{k=1}^n \lambda_k^2 |e_k\rangle \langle e_k|$$

(the eigenvalues can be different but the eigenvectors are the same)

Definition: The *commutator* of AB is

$$[AB] = AB - BA$$

so A and B commute iff $[AB] = 0$

Lecture 13: Oct 6

Lecture 14: Oct 11

The Schrodinger Equation: Moves state forward in time deterministically based on state, environment, and time

Setup

We want a transformation U that maps

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Two options are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

Notice the second resultant is in the equivalence class of $|d\rangle$ with respect to phase.

Notation: $|\psi(t)\rangle = U_t |\psi(0)\rangle$

Derivation

Desiderata:

1. Linearity:

$$U_t(|\psi_1(0)\rangle + |\psi_2(0)\rangle) = U_t |\psi_1(0)\rangle + U_t |\psi_2(0)\rangle = |\psi_1(t)\rangle + |\psi_2(t)\rangle$$

2. Conservation of Probability (i.e. $|\psi(t)\rangle \in \mathbb{C}_1^2$)

$$\langle \psi(t) | \psi(t) \rangle = 1 \quad \forall t$$

Already from these properties, we have a vector space and linearity so U_t has a matrix representation: $U_t \in \mathbb{C}^{2 \times 2}$.

Then from the second condition, by substitution,

$$\begin{aligned} |\psi(t)\rangle &= U_t |\psi(0)\rangle \\ \langle \psi(t) | \psi(t) \rangle &= 1 \\ (U_t |\psi(0)\rangle)^\dagger (U_t |\psi(0)\rangle) &= 1 \\ \langle \psi(0) U_t^\dagger U_t | \psi(0) \rangle &= 1 \end{aligned}$$

But since $(U^\dagger U)^\dagger = U^\dagger U$, we know $U^\dagger U$ is Hermitian. So we can write

$$U_t^\dagger U_t = \sum_{k=1}^n \lambda_k |e_k\rangle \langle e_k|$$

Plugging back in,

$$\left\langle \psi \left| \sum_{k=1}^n \lambda_k |e_k\rangle \langle e_k| \right| \psi \right\rangle = 1 \quad \forall \psi$$

But as this is true *for all* states, we can arbitrarily choose $\psi = e_l$ so

$$\left\langle e_l \left| \sum_{k=1}^n \lambda_k |e_k\rangle \langle e_k| \right| e_l \right\rangle = \lambda_l = 1$$

Hence, all the eigenvalues are 1. Further, $U^\dagger U = I$

Unitary: a matrix $U : \mathbb{C}_1^n \rightarrow \mathbb{C}_1^n$ such that

$$U^\dagger U = U U^\dagger = I$$

All together,

$$\left\langle \psi(0) \mid U_t^\dagger U_t \mid \psi(0) \right\rangle = \langle \psi(0) \mid I \mid \psi(0) \rangle = \langle \psi(0) \mid \psi(0) \rangle = \langle \psi(t) \mid \psi(t) \rangle$$

More generally,

$$\langle \psi_1(0) \mid \psi_2(0) \rangle = \left\langle \psi_1(0) \mid U_t^\dagger U \mid \psi_2(0) \right\rangle = \langle \psi_1(t) \mid \psi_2(t) \rangle$$

So U_t preserves overlap.

Lecture 15: Oct 13

Unitary Matrices

Definition: if a matrix $U : \mathbb{C}_1^n \rightarrow \mathbb{C}_1^n$ and

$$U^\dagger U = U U^\dagger = 1$$

Examples:

- $R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ is unitary but not Hermitian
- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ is unitary and Hermitian

Schrodinger Derivation (Continued)

Recall: by demanding linearity and conservation of probability we have shown that for any starting states,

$$\langle \psi_1(0) | \psi_2(0) \rangle = \langle \psi_1(0) | U_t^\dagger U | \psi_2(0) \rangle = \langle \psi_1(t) | \psi_2(t) \rangle$$

Now we introduce another condition:

3. State:

$$U_{t+s} = U_t U_s$$

so

$$|\psi(t+s)\rangle = U_{t+s} |\psi(0)\rangle = U_t |\psi(s)\rangle$$

4. Continuity:

$$\lim_{s \rightarrow 0} U_{t+s} |\phi\rangle = U_t |\phi\rangle$$

Concretely,

$$\lim_{s \rightarrow 0} |\psi(t+s)\rangle = |\psi(t)\rangle$$

Stone's Representation Theorem: If $U_{t \geq 0}$ satisfies linearity, unitarity, and continuity then there exists a Hermitian operator $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$ such that

$$U_t = e^{iAt}$$

Interlude: Functions of Hermitian Operators

Recall that if A is Hermitian, then

$$A = \sum_{k=0}^n \lambda_k |e_k\rangle \langle e_k|$$

and

$$A^2 = \sum_k \sum_l \lambda_k \lambda_l |e_k\rangle \langle e_k | e_l\rangle \langle e_l| = \sum_{k=0}^n \lambda_k^2 |e_k\rangle \langle e_k|$$

If we let $f(x) = x^2$ then

$$f(A) = \sum_{k=0}^n f(\lambda_k) |e_k\rangle \langle e_k|$$

From analysis you can generalize to all powers, then all polynomials (by linearity), then eventually continuity.

Back to Stone's:

In particular, if $f(x) = e^{itx}$ then

$$f(A) = e^{itA}$$

so by Stone's theorem

$$|\psi(t)\rangle = U_t |\psi(0)\rangle = e^{itA} |\psi(0)\rangle$$

Now taking the derivative, we get Schrodinger's Equation:

$$\boxed{\frac{d}{dt} |\psi(t)\rangle = iA e^{itA} |\psi(0)\rangle = iA |\psi(t)\rangle}$$

Now applying the state definition,

$$|\psi(t)\rangle = \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix} \in \mathbb{C}^2$$

and

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

so

$$\begin{cases} \dot{\alpha} = ia_{11} \alpha(t) + ia_{21} \beta(t) \\ \dot{\beta} = ia_{21} \alpha(t) + ia_{22} \beta(t) \end{cases}$$

Lecture 16: Oct 16

Tensor Product Space

Notation: with $V = \mathbb{C}^n$ and $W = \mathbb{C}^m$, two vector spaces containing a particle in each. We let $V \otimes W$ is the state space of pairs of particles V and W . We make the natural assumptions:

1. $V \otimes W$ is a complex vector space
2. It has an inner product $(|\psi\rangle, |\phi\rangle) \in V \otimes W \implies \langle \psi | \phi \rangle \in \mathbb{C}$ which is linear in $|\phi\rangle$ and conjugate-linear in $|\psi\rangle$

Construction (Ansatz):

1. (Assumption) Minimal elements: $\forall |v\rangle \in V, |w\rangle \in W$ assume that the independent pair (designated $|v w\rangle$) is in $V \otimes W$.
2. Overlap: with $|\psi\rangle, |\phi\rangle \in V \otimes W$,

$$\mathbb{P}(|\psi\rangle \xrightarrow{A} |\phi\rangle) = \left| \langle \psi | \phi \rangle_{V \otimes W} \right|^2$$

3. Independence: if we have two experiments $|v\rangle \xrightarrow{A} |\tilde{v}\rangle$ and $|w\rangle \xrightarrow{B} |\tilde{w}\rangle$ with the pair in A being independent from the pair in B, then

$$\begin{aligned} \left| \langle vw | \tilde{v}\tilde{w} \rangle_{V \otimes W} \right|^2 &= \mathbb{P}(|vw\rangle \rightarrow |\tilde{v}\tilde{w}\rangle) \\ &= \mathbb{P}([|v\rangle \xrightarrow{A} |\tilde{v}\rangle] \cap [|w\rangle \xrightarrow{B} |\tilde{w}\rangle]) \\ &= \mathbb{P}(|v\rangle \xrightarrow{A} |\tilde{v}\rangle) \cdot \mathbb{P}(|w\rangle \xrightarrow{B} |\tilde{w}\rangle) \\ &= \left| \langle v | \tilde{v} \rangle_V \right|^2 \left| \langle w | \tilde{w} \rangle_W \right|^2 \end{aligned}$$

4. Existence of nm orthonormal states in $V \otimes W$: Let $|e_1\rangle, \dots, |e_n\rangle \in V$ and $|f_1\rangle, \dots, |f_m\rangle \in W$ be orthonormal sets. Then $\forall 1 \leq i \leq n, 1 \leq j \leq m$ $|e_i f_j\rangle \in V \otimes W$ and

$$\langle e_i f_j | e_k f_l \rangle_{V \otimes W} = \langle e_i | e_k \rangle_V \otimes \langle f_j | f_l \rangle_W = \delta_{ik} \delta_{jl}$$

so $\{|e_i f_j\rangle\}$ is an orthonormal set in $V \otimes W$. This immediately tells us that all linear combinations of these vectors is in the space:

$$\left\{ \sum_{i=0}^n \sum_{j=0}^m \gamma_{ij} |e_i f_j\rangle \mid \gamma_{ij} \in \mathbb{C} \right\} \subseteq V \otimes W$$

Is this enough to form a full basis for the space?

5. Occam's Razor: We assume that the basis described above *is* sufficient to form a basis for $V \otimes W$

Lecture 17: Oct 18

Review of the Tensor Space

We have two particles $w \in W$ and $v \in V$ where $V \in \mathbb{C}^n$ and $W \in \mathbb{C}^m$ are state spaces.

We define $V \otimes W$ as a vector inner-product space such that

1. $\forall |\psi\rangle, |\phi\rangle \in V \otimes W, \quad \langle \psi | \phi \rangle \in \mathbb{C}$
2. We assume that $V \otimes W$ contains an element for all pair of states $|v\rangle \in V, |w\rangle \in W$ which we designate as

$$|vw\rangle = |v\rangle \otimes |w\rangle \in V \otimes W$$

3.

$$\langle vw | \tilde{v}\tilde{w} \rangle_{V \otimes W} = \langle v | \tilde{v} \rangle \langle w | \tilde{w} \rangle$$

4. Given orthonormal basis sets $\{|e_1\rangle, \dots, |e_n\rangle\}$ for V and $\{|f_1\rangle, \dots, |f_m\rangle\}$ for W ,

$$V \otimes W = \left\{ \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |e_i f_j\rangle \mid \gamma_{ij} \in \mathbb{C} \right\}$$

5. If $|\psi\rangle = \sum_{i,j} \alpha_{ij} |e_i f_j\rangle$ and $|\phi\rangle = \sum_{k,l} \beta_{kl} |e_k f_l\rangle$, then

$$\langle \psi | \phi \rangle = \sum_{ij} \alpha_{ij}^* \beta_{ij}$$

Remarks:

- $\{|e_i f_j\rangle \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is orthonormal of size mn so it is a basis.
- Construction is independent of basis (because of linear algebra and the inner product)
- Condition 4 is actually redundant and arises naturally from the inner product

Independence: If $|\psi\rangle = |vw\rangle = |v\rangle \otimes |w\rangle$ for some $|v\rangle \in V, |w\rangle \in W$ then v and w are *independent*. Otherwise, they are *entangled*.

Now we might wonder if we can go the other way: When is $|\psi\rangle = \sum_{ij} \gamma_{ij} |e_i f_j\rangle$ the state of a pair of independent particles?

Theorem: $|\psi\rangle$ consists of two independent states if and only if

$$\exists a_1, \dots, a_n \in C, b_1, \dots, b_m \in C$$

such that $\gamma_{ij} = a_i b_j$

This leads to another property: If $\sum a_i |e_i\rangle \in \mathbb{C}_1^n$ and $\sum b_j |f_j\rangle \in \mathbb{C}_1^m$, then

$$\sum_{i=1}^n \sum_{j=1}^m |a_i b_j|^2 = 1$$

or

$$\sum_{ij} a_i b_j |e_i f_j\rangle \in \mathbb{C}_1^{n \times m} = \mathbb{C}_1^n \otimes \mathbb{C}_1^m$$

Example: the “singlet state”

In $\mathbb{C}^2 \otimes \mathbb{C}^2$, if we have one particle

$$|\psi\rangle = \frac{1}{\sqrt{2}} |ud\rangle - \frac{1}{\sqrt{2}} |du\rangle$$

and we measure one of the two, then we immediately know the state of the other

Which gives us a few known probabilities:

$$\begin{aligned} \mathbb{P}(\lambda_z^{(1)} = 1 \mid |\psi\rangle) &= \frac{1}{2} \\ \mathbb{P}(\lambda_z^{(1)} = \lambda_z^{(2)} \mid |\psi\rangle) &= 0 \\ \mathbb{P}(\lambda_x^{(1)} = 1 \mid |\psi\rangle) &= \frac{1}{2} \end{aligned}$$

This is the weirdness of QM! There is no way to define the state of either particle. Only the probabilities.

Lecture 18: Oct 20

Two Particles

Let us have two particles, 1 and 2 and two machines $A \in V, B \in W$. How do we measure $\lambda_A^{(1)}, \lambda_B^{(1)}, \lambda_A^{(2)}, \lambda_B^{(2)}$?

Consider

$$\mathbb{E}[\lambda_A^{(1)} \lambda_B^{(2)} \mid |\psi\rangle] = \langle \psi \mid A \otimes B \mid |\psi\rangle \rangle_{V \otimes W}$$

If we can define this on arbitrary basis elements, then we have successfully defined it for every possible operator.

Let $e_i f_j$ and define $(A \otimes B) |e_i f_j\rangle = |Ae_i, Bf_j\rangle$. More generally

$$(A \otimes B) |vw\rangle = |Av, Bw\rangle$$

Lecture 19: Oct 23

Generally

We have two state spaces $V = |e_i\rangle \ 1 \leq i \leq n$ and $W = |f_j\rangle \ 1 \leq j \leq m$. Then

$$V \otimes W = \left\{ \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |e_i f_j\rangle : \gamma_{ij} \in \mathbb{C} \right\} = \left\{ \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |e_i\rangle \otimes |f_j\rangle : \gamma_{ij} \in \mathbb{C} \right\}$$

as expected.

Further, if

$$\psi = \sum_{i,j} \alpha_{ij} |e_i f_j\rangle \tag{1}$$

$$\phi = \sum_{k,l} \beta_{kl} |e_k f_l\rangle \tag{2}$$

Then

$$\langle \psi \mid \phi \rangle_{V \otimes W} = \sum_{i,j} \alpha_{ik}^* \beta_{jl}$$

(because $\langle e_i f_j \mid e_k f_l \rangle = \delta_{ik} \delta_{jl}$)

Heuristic: this is a generalization of $n \cdot m = n_x m_x + n_y m_y + n_z m_z$

An Example

Now, suppose we have a particular system $V, W \in \mathbb{C}_1^2$ and

$$T_2 = \frac{1}{\sqrt{2}} |uu\rangle + \frac{1}{\sqrt{2}} |dd\rangle \tag{3}$$

$$S = \frac{1}{\sqrt{2}} |ud\rangle - \frac{1}{\sqrt{2}} |du\rangle \tag{4}$$

Then

$$\begin{aligned}\langle T_2 | S \rangle &= \left\langle \frac{1}{\sqrt{2}} |uu\rangle + \frac{1}{\sqrt{2}} |dd\rangle \mid \frac{1}{\sqrt{2}} |ud\rangle - \frac{1}{\sqrt{2}} |du\rangle \right\rangle \\ &= 0 |uu\rangle + 0 |ud\rangle + 0 |ud\rangle + 0 |du\rangle + 0 |dd\rangle \\ &= 0\end{aligned}$$

Something is wrong here. Line three should be a scalar. Do something with the coeffs of the kets?

Aside: T_1, T_2, T_3, S are eigenvectors of

$$\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z$$

Independence

Given a state

$$|\psi\rangle = \sum \gamma_{ij} |e_i f_j\rangle$$

are particles (1) and (2) independent?

Definition: if two particles $|v\rangle = \sum_{i=1}^n a_i |e_i\rangle$ and $|w\rangle = \sum_{j=1}^m b_j |f_j\rangle$ are *independent*, we write them $|vw\rangle$ and

$$|vw\rangle = \sum_{ij} \gamma_{ij} |e_i f_j\rangle$$

with $\gamma_{ij} = a_i b_j$

Showing consistency: By definition of the tensor product,

$$\begin{aligned}|vw\rangle &= |v\rangle \otimes |w\rangle \\ &= \sum_{i=1}^n a_i |e_i\rangle \otimes \sum_{j=1}^m b_j |f_j\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^m a_i b_j |e_i\rangle \otimes |f_j\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^m a_i b_i |e_i f_j\rangle\end{aligned}$$

$\implies v, w$ are independent

Lecture 20: Oct 25

Independence in $\mathbb{C}^2 \otimes \mathbb{C}^2$

Example 1:

From earlier work, we have a basis $|u\rangle, |d\rangle$. Given a state,

$$|\psi\rangle = \gamma_{11} |uu\rangle + \gamma_{12} |ud\rangle + \gamma_{21} |du\rangle + \gamma_{22} |dd\rangle$$

What conditions on γ for the particles to be independent?

Answer: Homework

Hint: $\gamma_{11}\gamma_{22} - \gamma_{12}\gamma_{21} = 0 \iff 1 \text{ and } 2 \text{ are independent}$ (though this formula does not even generalize to \mathbb{C}^3 !)

Example 2:

With $|\psi\rangle = \frac{1}{\sqrt{2}}(|ll\rangle - |rr\rangle)$, are particles (1) and (2) independent?

We know that

$$\begin{aligned} |l\rangle &= \frac{1}{\sqrt{2}} |u\rangle - \frac{1}{\sqrt{2}} |d\rangle \\ |r\rangle &= \frac{1}{\sqrt{2}} |u\rangle + \frac{1}{\sqrt{2}} |d\rangle \end{aligned}$$

so

$$\begin{aligned} |ll\rangle &= \frac{1}{\sqrt{2}}(|u\rangle - |d\rangle) \otimes \frac{1}{\sqrt{2}}(|u\rangle - |d\rangle) \\ &= \frac{1}{2} |uu\rangle - \frac{1}{2} |ud\rangle - \frac{1}{2} |du\rangle + \frac{1}{2} |dd\rangle \\ |rr\rangle &= \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle) \otimes \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle) \\ &= \frac{1}{2} |uu\rangle + \frac{1}{2} |ud\rangle + \frac{1}{2} |du\rangle + \frac{1}{2} |dd\rangle \end{aligned}$$

$$\frac{1}{\sqrt{2}}(|ll\rangle - |rr\rangle) = -\frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) = \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle)$$

(the last equality follows from the equivalence classes)

Since they are in \mathbb{C}^2 , we can say

$$0 - \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \neq 0$$

so they are not independent!

Alternatively, show that these coefficients cannot be factored.

Basic states:

$$\begin{aligned} |S\rangle &= \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle) \\ |T_1\rangle &= \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) \\ |T_2\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \\ |T_3\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle - |dd\rangle) \end{aligned}$$

These are all eigenvectors of

$$\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z$$

where

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

General case

Let A and B be Hermitian operators. Then we can define $A \otimes B$ operating on $\mathbb{C}^n \otimes \mathbb{C}^m$ by

$$A \otimes B |e_i f_j\rangle = |Ae_i Bf_j\rangle \implies A \otimes B |vw\rangle = |Av Bw\rangle = |Av\rangle \otimes |Bv\rangle$$

For any $A \in V$, $B \in W$,

$$(A \otimes B)^\dagger = (A^\dagger \otimes B^\dagger)$$

Proof: HW

Hint: Consider $\langle e_i f_j | A \otimes B | e_k f_l \rangle$

Theorem: $A \otimes B$ is Hermitian iff A, B are Hermitian

In fact, for any Hermitian operator on $H \in V \otimes W$, there exists a representation

$$H = \sum_{k=1}^N A_k \otimes B_k$$

where all A_k, B_k are hermitian.

Lecture 21: Oct 27

Preparation for Bell's Theorem

Consider the singlet $|S\rangle = \frac{1}{\sqrt{2}} |ud\rangle - \frac{1}{\sqrt{2}} |du\rangle$

Then because they are entangled, they cannot both be up-up or down-down. So generally,

$$\mathbb{P}(\lambda_n^{(1)} = 1, \lambda_n^{(2)} = 1 \mid |\psi\rangle = |S\rangle) = 0$$

Further, $\forall q, r \in \mathbb{R}_1^3$,

$$\mathbb{P}(\lambda_q^{(1)} = 1, \lambda_r^{(2)} = 1 \mid |s\rangle) = \frac{1}{2} \sin^2 \frac{\theta}{2}$$

where θ is the angle between q and r .

Bell's Theorem

We are looking for an event space \mathcal{H} with a probability $P_{\mathcal{H}}(h)$ such that

$$\lambda_r^{(1)} = \lambda_r^{(1)}(h), \quad \lambda_q^{(2)} = \lambda_q^{(2)}(h)$$

i.e., the λ s are random variables $\lambda_r^{(1)}, \lambda_q^{(2)} : \mathcal{H} \rightarrow \{-1, 1\}$. In a sense, h is a “hidden-variable” that, if known, would reduce everything to a deterministic system.

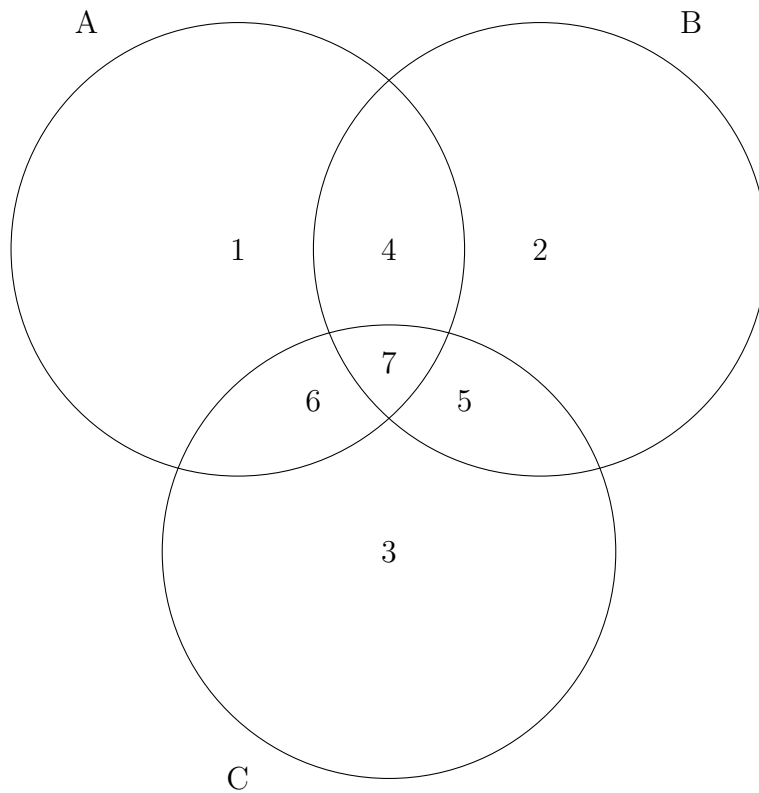
So we need to find lambdas that satisfy

$$P_{\mathcal{H}}(\{h \in \mathcal{H} : \lambda_1^{(1)}(h) = 1, \lambda_r^{(2)}(h) = 1\}) = \frac{1}{2} \sin^2\left(\frac{\theta}{2}\right)$$

(Imagine the event as two dice rolls with h being their sum – perhaps 7 – known and their probability telling us what state each die was in)

Bell's Theorem: there are no functions λ . It is impossible to find two random variables on the event space that satisfy that equation.

Interlude: Probability



$$\begin{aligned}
 P(A \cap B') &= P(1) + P(6) \\
 &\leq P(1) + P(6) + p(3) + P(4) \\
 &= P(A \cap C') + P(C \cap B')
 \end{aligned}$$

With $n, m, l \in \mathbb{R}_1^3$:

$$\begin{cases} A = \{h : \lambda_n^{(1)} = 1\} \\ B = \{h : \lambda_m^{(1)} = 1\} \\ C = \{h : \lambda_l^{(1)} = 1\} \end{cases} \implies \begin{cases} B' = \{h : \lambda_m^{(2)} = 1\} \\ C' = \{h : \lambda_l^{(2)} = 1\} \end{cases}$$

Lecture 22: Oct 30

Review

$$|s\rangle = \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle)$$

We want to find functions (random variables) $\lambda_n^{(1)}, \lambda_m^{(2)}$ such that

$$\mathbb{P}(\{h \in \mathcal{H} : \lambda_n^{(1)}(h) = 1, \lambda_m^{(2)}(h) = 1 \mid |\psi\rangle = |S\rangle\}) = \frac{1}{2} \sin^2 \frac{\theta_{nm}}{2}$$

Bell's Theorem: We *cannot* choose $\mathcal{H}, \mathbb{P}, \lambda_n(h), \lambda_m(h)$ to satisfy that formula.

Proof of Bell's Theorem

Consider the sets

$$A = \{h \in \mathcal{H} : \lambda_n^{(1)}(h) = 1\}$$

$$B = \{h \in \mathcal{H} : \lambda_m^{(1)}(h) = 1\}$$

$$C = \{h \in \mathcal{H} : \lambda_l^{(1)}(h) = 1\}$$

where n, l, m are three vectors in \mathbb{R}_1^3 with $\angle m, l = \theta$, $\angle l, m = \theta$, $\angle n, m = 2\theta$.

Now we see consider the complements:

$$\overline{B} = \{h \in \mathcal{H} : \lambda_m^{(2)}(h) = 1\}$$

$$\overline{C} = \{h \in \mathcal{H} : \lambda_l^{(2)}(h) = 1\}$$

Observe that

$$\underbrace{\mathbb{P}(A \cap \overline{B})}_{\text{(a)}} \leq \underbrace{\mathbb{P}(A \cap \overline{C})}_{\text{(b)}} + \underbrace{\mathbb{P}(C \cap \overline{B})}_{\text{(c)}}$$

Considering the quantum mechanical probabilities given the singleton,

$$\mathbb{P}(\textcircled{a}) = \mathbb{P}(\lambda_n^{(1)}, \lambda_m^{(2)} = 1 \mid |S\rangle) = \frac{1}{2} \sin^2\left(\frac{2\theta}{2}\right) = \frac{1}{2} \sin^2 \frac{\theta}{2}$$

$$\mathbb{P}(\textcircled{b}) = \mathbb{P}(\lambda_n^{(1)}, \lambda_l^{(2)} = 1 \mid |S\rangle) = \frac{1}{2} \sin^2\left(\frac{\theta}{2}\right)$$

$$\mathbb{P}(\textcircled{b}) = \mathbb{P}(\lambda_l^{(1)}, \lambda_m^{(2)} = 1 \mid |S\rangle) = \frac{1}{2} \sin^2\left(\frac{\theta}{2}\right)$$

So

$$\frac{1}{2} \sin^2 \theta \leq \sin^2 \frac{\theta}{2}$$

but

$$\begin{aligned} \lim_{\theta \rightarrow 0} \frac{\frac{1}{2} \sin^2 \theta}{\theta^2} &\leq \lim_{\theta \rightarrow 0} \frac{\sin^2 \frac{\theta}{2}}{\theta^2} \\ \lim_{\theta \rightarrow 0} \frac{1}{2} \frac{\sin \theta}{\theta} \cdot \frac{\sin \theta}{\theta} &\leq \lim_{\theta \rightarrow 0} \frac{\sin \frac{\theta}{2}}{\theta} \cdot \frac{\sin \frac{\theta}{2}}{\theta} \\ \frac{1}{2} \cdot 1 \cdot 1 &\leq \frac{1}{2} \cdot \frac{1}{2} \\ \frac{1}{2} &\leq \frac{1}{4} \end{aligned}$$

So contradiction!!

Conclusion: We used only the most basic properties of modern (Kolmogorovian/Measure theory) probability to create the equation $\mathbb{P}(A \cap \overline{B}) \leq \mathbb{P}(A \cap \overline{C}) + \mathbb{P}(C \cap \overline{B})$. But this shows that there is a contradiction. Thus, probability as we understand it *is insufficient to describe quantum mechanics*.

Lecture 23: Nov 1

Marginals and Mixtures

Say we have two random variables: $X \in \{1, 2, 3\}$, $Y \in \{1, 2\}$. With the following joint probabilities

		Y	
		1	2
X	1	2/12	2/12
	2	5/12	1/12
	3	1/12	1/12

So we have a joint probability $p(X, Y)$ with values e.g. $p(3, 2) = 1/12$ or $p(2, 1) = 5/12$.

Definition: the *marginal distribution* on X is

$$p_X(x) = \sum_y p(x, y)$$

and we say “we marginalized out Y ”.

Examples:

- $p_X(1) = \frac{4}{12}$
- $p_X(2) = \frac{6}{12}$
- $p_X(3) = \frac{2}{12}$
- $p_Y(1) = \frac{2}{3}$
- $p_Y(2) = \frac{1}{3}$

Definition: When we write a distribution (say p_X) in the form

$$p_X(x) = \sum_{k=1}^n p_k q_k(x)$$

where p_k is a probability on $1, 2, \dots, n$ and $q_k(x)$ is a PDF on X , then we say X has a *mixture distribution* with p_1, \dots, p_n the mixing probabilities and $q_1(x), \dots, q_n(x)$ the probability distributions that are mixed.

In fact,

$$p_X(x) = \sum_y p_y p(x | y)$$

where

$$p(x | y) = \frac{p(x, y)}{\sum_{\tilde{x}} p(\tilde{x}, y)}$$

Examples:

•

$$q_1 = \frac{1}{p_Y(1)} \begin{pmatrix} 2/12 \\ 5/12 \\ 1/12 \end{pmatrix} = \frac{3}{2} \begin{pmatrix} 2/12 \\ 5/12 \\ 1/12 \end{pmatrix} = \begin{pmatrix} 6/24 \\ 15/24 \\ 3/24 \end{pmatrix} = \begin{pmatrix} 2/8 \\ 5/8 \\ 1/8 \end{pmatrix}$$

•

$$q_2 = 3 \begin{pmatrix} 2/12 \\ 1/12 \\ 1/12 \end{pmatrix} = \begin{pmatrix} 2/4 \\ 1/4 \\ 1/4 \end{pmatrix}$$

Mixtures are convenient because

$$\mathbb{E}[X] = \sum_{k=1}^n p_k \mathbb{E}_{q_k}[X]$$

Expectation with Mixtures

We go back to our standard state

$$|\psi\rangle = \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |e_i f_j\rangle \in V \otimes W$$

Let A be a measurement on (1) so

$$\mathbb{E}[\lambda^{(A)} \mid |\psi\rangle] = \langle \psi \mid A \otimes I \mid \psi \rangle$$

Our goal is to write this as a mixture expected value. To this end,

$$p_k = \sum_{i=1}^n |\gamma_{ij}|^2$$

is just the marginal on particle (2) ($|\gamma_{ij}|^2 = |\langle \psi \mid e_i f_j \rangle|^2$)

So

$$\begin{aligned} \langle \psi \mid A \otimes I \mid \psi \rangle &= \left\langle \psi \mid \sum_{i,j} \gamma_{ij} |A e_i f_j\rangle \right\rangle \\ &= \left\langle \sum_{k,l} \gamma_{kl} |e_k f_l\rangle \mid \sum_{i,j} \gamma_{ij} |A e_i f_j\rangle \right\rangle \\ &= \sum_j \left\langle \sum_k \gamma_{kj} |e_k\rangle \mid \sum_{i,j} \gamma_{ij} |A e_i\rangle \right\rangle \quad (\text{because } \langle e_k f_l \mid A e_i f_j \rangle = \delta_{l,j} \langle e_k f_l \mid A e_i f_j \rangle) \\ &= \sum_j p_j \cdot \langle v_j \mid A \mid v_j \rangle \end{aligned}$$

Lecture 24: Nov 3

Recall

If we have a state

$$|\psi\rangle = \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |e_i f_j\rangle \in V \otimes W$$

and a hermitian matrix $A \in V$, then

$$\mathbb{E}[\lambda^{(A)} \mid |\psi\rangle] = \langle \psi \mid A \otimes I \mid \psi \rangle = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^n \sum_{l=1}^m \gamma_{kl}^* \gamma_{ij} \langle e_k \mid A \mid e_i \rangle \langle f_l f_j \rangle$$

And we have a mixture distribution

$$p_X(x) = \sum_y p_Y(y) p(x \mid y) = \sum_y p_Y(y) q_y(x)$$

In the expectation, the $\langle f_l \mid f_j \rangle$ reduces to $\delta_{l,j}$ so we can get rid of the l -summation:

$$\begin{aligned} \mathbb{E}[\lambda^{(A)} \mid |\psi\rangle] &= \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^n \gamma_{kl}^* \gamma_{ij} \langle e_k \mid A \mid e_i \rangle \\ &= \sum_{j=1}^m \left\langle \sum_{k=1}^n \gamma_{kj} |e_k\rangle \mid A \mid \sum_{i=1}^n \gamma_{ij} |e_i\rangle \right\rangle \end{aligned}$$

And these are really the exact same vector labelled by different indices!

But, we can equivalently look at the expected value from the mixture distribution:

$$\mathbb{E}[X] = \sum_y p_Y(y) \mathbb{E}_{q_y}[X]$$

So now we need to express the quantum expectation in terms of the marginal expectations which we can do by introducing an arbitrary constant into the last equation above:

$$\mathbb{E}[\lambda^{(A)} \mid |\psi\rangle] = \sum_{j=1}^m p_j \sum_{i=1}^n \left\langle \sum_{k=1}^n \frac{\gamma_{kj}}{\sqrt{p_j}} |e_k\rangle \mid A \mid \sum_{i=1}^n \frac{\gamma_{ij}}{\sqrt{p_j}} |e_i\rangle \right\rangle$$

Intuitively, we would like p_j to be a probability of being in a particular state

$$p_j := \sum_{i=1}^n |\gamma_{ij}|^2$$

which is a joint distribution on the transition probability and which sums to 1 by the properties of probabilities.

Thus,

$$|v_i\rangle = \sum_{j=1}^n \frac{\gamma_{ij}}{\sqrt{p_j}} |e_i\rangle$$

is a normalized vector in $V = \mathbb{C}_1^n$.

All together,

$$\mathbb{E}[\lambda_A^{(1)} | |\psi\rangle] = \sum_{j=1}^m p_j \mathbb{E}[\lambda_A^{(1)} | |v_j\rangle]$$

hence, it is a mixture over the states of the second.

Conclusion: the mixture state of particle 1,

$$M^{(1)} = \sum_{j=1}^m p_j \delta_{|v_j\rangle}$$

so we call it a *mixed state in V* (where δ is the dirac delta).

Lecture 25: Nov 6

3 sided coin

Say we have three options:

#	\mathbb{P}
1	1/6
2	3/6
3	2/6

Now pretend that based on the coin flip results, God

puts some particles in $|u\rangle, |d\rangle, |r\rangle$ based on the results.

We have a mixture:

$$M = \frac{1}{6}\delta_{|u\rangle} + \frac{3}{6}\delta_{|d\rangle} + \frac{2}{6}\delta_{|r\rangle}$$

which allows us to calculate expected values:

$$\begin{aligned}\mathbb{E}[\lambda_{\sigma_z} | M] &= \frac{1}{6} \cdot \mathbb{E}[|u\rangle | |u\rangle] + \frac{3}{6} \cdot \mathbb{E}[|u\rangle | |d\rangle] + \frac{2}{6} \cdot \mathbb{E}[|u\rangle | |r\rangle] \\ &= \frac{1}{6} \cdot 1 + \frac{3}{6} \cdot (-1) + \frac{2}{6} \cdot (0) = -\frac{2}{6}\end{aligned}$$

Equivalently,

$$\mathbb{E}_M[\lambda_{\sigma_z}] = \frac{1}{6} \langle u | \sigma_z | u \rangle + \frac{1}{2} \langle d | \sigma_z | d \rangle + \frac{1}{3} \langle r | \sigma_z | r \rangle$$

General case: for $M^{(1)} = \sum_{j=1}^m p_j \delta_{|v_j\rangle}$,

$$\mathbb{E}[\lambda_A^{(1)} | M^{(1)}] = \sum_{j=1}^m p_j \langle v_j | A | v_j \rangle$$

Alice and Bob

Alice and Bob generate two particles (1) and (2) in a state

$$|\phi_0\rangle_{AB} = \frac{1}{\sqrt{2}}(|uu\rangle_{AB} + |dd\rangle_{AB})$$

(the AB subscripts mean Alice and Bob)

Say Bob takes 100 trillion of particle (2) to Pluto.

Charlie is a particle

$$|C\rangle_C = \alpha |u\rangle + \beta |d\rangle$$

We assume that Charlie is independent from Alice and Bob's particles. We have a joint state

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \otimes (\alpha |u\rangle + \beta |d\rangle)$$

Bell's Basis:

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \\
|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) \\
|\phi_2\rangle &= \frac{i}{\sqrt{2}}(|ud\rangle - |du\rangle) \\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle - |dd\rangle)
\end{aligned}$$

and it provides a basis for $A \otimes B$.

This allows us to write the independent states in terms of the basis:

$$\begin{aligned}
|uu\rangle &= \frac{1}{\sqrt{2}}(|\phi_0\rangle + |\phi_3\rangle) \\
|dd\rangle &= \frac{1}{\sqrt{2}}(|\phi_0\rangle - |\phi_3\rangle) \\
|ud\rangle &= \frac{1}{\sqrt{2}}(|\phi_1\rangle - i|\phi_2\rangle) \\
|du\rangle &= \frac{1}{\sqrt{2}}(|\phi_1\rangle + i|\phi_3\rangle)
\end{aligned}$$

So we can write

$$\begin{aligned}
|\psi\rangle_{ABC} &= \frac{\alpha}{\sqrt{2}}|uuu\rangle_{ABC} + \frac{\beta}{\sqrt{2}}|uud\rangle_{ABC} + \frac{\alpha}{\sqrt{2}}|ddu\rangle_{ABC} + \frac{\beta}{\sqrt{2}}|ddd\rangle_{ABC} \\
&= \frac{\alpha}{\sqrt{2}}|uuu\rangle_{ACB} + \frac{\beta}{\sqrt{2}}|udu\rangle_{ACB} + \frac{\alpha}{\sqrt{2}}|dud\rangle_{ACB} + \frac{\beta}{\sqrt{2}}|ddd\rangle_{ACB} \\
&= \frac{\alpha}{\sqrt{2}}|uu\rangle_{AC} \otimes |u\rangle_B + \frac{\beta}{\sqrt{2}}|ud\rangle_{AC} \otimes |u\rangle_B + \frac{\alpha}{\sqrt{2}}|du\rangle_{AC} \otimes |d\rangle_B + \frac{\beta}{\sqrt{2}}|dd\rangle_{AC} \otimes |d\rangle_B \\
&= \frac{\alpha}{2}(|\phi_1\rangle + |\phi_3\rangle) \otimes |u\rangle_B + \frac{\beta}{2}(|\phi_1\rangle - i|\phi_2\rangle) \otimes |u\rangle_B \\
&\quad + \frac{\alpha}{2}(|\phi_1\rangle + i|\phi_2\rangle) \otimes |d\rangle_B + \frac{\beta}{2}(|\phi_0\rangle - |\phi_3\rangle) \otimes |d\rangle_B
\end{aligned}$$

Finally,

$$\begin{aligned}
|\psi\rangle_{ABC} = & \frac{1}{2} |\phi_0\rangle_{AC} \otimes (\alpha |u\rangle_B + \beta |d\rangle_B) \\
& + \frac{1}{2} |\phi_1\rangle_{AC} \otimes (\alpha |d\rangle_B + \beta |u\rangle_B) \\
& + \frac{i}{2} |\phi_2\rangle_{AC} \otimes (\alpha |d\rangle_B - \beta |u\rangle_B) \\
& + \frac{1}{2} |\phi_3\rangle_{AC} \otimes (\alpha |u\rangle_B - \beta |d\rangle_B)
\end{aligned}$$

But notice!! $\alpha |u\rangle_B + \beta |d\rangle_B$ in the first line is precisely Charlie!! So if we measure the state of AC, and apply a unitary operator to rotate any of the other three states to the first one, we have Charlie back on Pluto!

Lecture 26: Nov 8

Teleportation

Bell's Basis:

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \\
|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|ud\rangle + |du\rangle) \\
|\phi_2\rangle &= \frac{i}{\sqrt{2}}(|ud\rangle - |du\rangle) \\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|uu\rangle - |dd\rangle)
\end{aligned}$$

Spin operators:

$$\begin{aligned}
\sigma_x |u\rangle &= |d\rangle, & \sigma_x |d\rangle &= |u\rangle \\
\sigma_y |u\rangle &= i |d\rangle, & \sigma_y |d\rangle &= -i |u\rangle \\
\sigma_z |u\rangle &= |u\rangle, & \sigma_z |d\rangle &= -|u\rangle
\end{aligned}$$

Setup: Alice and Bob prepare

$$|\phi_0(k)\rangle_{AB} = \frac{1}{\sqrt{2}} |u(k)u(k)\rangle_{AB} + \frac{1}{\sqrt{2}} |d(k)d(k)\rangle_{AB} \quad (1 \leq k \leq n)$$

And we have Charlie in state

$$|C\rangle = \alpha |u\rangle + \beta |d\rangle$$

Step 1 (Algebra): We send Bob to Pluto and have Charlie enter the scene at $k = 1$, creating a joint state

$$\begin{aligned} |\psi\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|uu\rangle + |dd\rangle) \otimes (\alpha |u\rangle + \beta |d\rangle) \\ &= \frac{\alpha}{\sqrt{2}} |uuu\rangle_{ABC} + \frac{\beta}{\sqrt{2}} |uud\rangle_{ABC} + \frac{\alpha}{\sqrt{2}} |ddu\rangle_{ABC} + \frac{\beta}{\sqrt{2}} |ddd\rangle_{ABC} \end{aligned}$$

Interchanging B and C , isolating B , and rewriting AC with Bell's Basis, we get

$$\begin{aligned} |\psi\rangle_{ABC} &= \frac{1}{2} |\phi_0\rangle_{AC} \otimes (\alpha |u\rangle_B + \beta |d\rangle_B) \\ &\quad + \frac{1}{2} |\phi_1\rangle_{AC} \otimes (\alpha |d\rangle_B + \beta |u\rangle_B) \\ &\quad + \frac{i}{2} |\phi_2\rangle_{AC} \otimes (\alpha i |d\rangle_B - \beta i |u\rangle_B) \\ &\quad + \frac{1}{2} |\phi_3\rangle_{AC} \otimes (\alpha |u\rangle_B - \beta |d\rangle_B) \end{aligned}$$

The first term $(\alpha |u\rangle_B + \beta |d\rangle_B)$ is Bob's particle and yet it is indistinguishable from Charlie. i.e., if we measure Bob's particle, then with probability 1/4 it will be Charlie!

Step 2 (Demise of Charlie): We now need to measure Charlie. Construct a Hermitian operator

$$H = k_0 |\phi_0\rangle \langle \phi_0| + k_1 |\phi_1\rangle \langle \phi_1| + k_2 |\phi_2\rangle \langle \phi_2| + k_3 |\phi_3\rangle \langle \phi_3|$$

The result is that AC is entangled and in $|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$ (each with probability 1/4)

Step 3 (Send the Results): If she gets $\lambda = 0$, send 00. $\lambda = 1 \rightarrow 01$, $\lambda = 2 \rightarrow 10$, $\lambda = 3 \rightarrow 11$

Step 4 (Receiving the Results): If Bob gets 00, he applies the identity operator to his one particle. If he gets 01, he applies σ_x . $10 \rightarrow \sigma_y$, $11 \rightarrow \sigma_z$. No matter what, the result of applying the operator to $|\psi\rangle$ is $|C\rangle$.

Lecture 27: Nov 10

A Footnote on Teleportation

Recall that during teleportation, we get a state

$$\begin{aligned} |\psi\rangle_{ABC} = & \frac{1}{2} |\phi_0\rangle_{AC} \otimes (\alpha |u\rangle_B + \beta |d\rangle_B) \\ & + \frac{1}{2} |\phi_1\rangle_{AC} \otimes (\alpha |d\rangle_B + \beta |u\rangle_B) \\ & + \frac{i}{2} |\phi_2\rangle_{AC} \otimes (\alpha i |d\rangle_B - \beta i |u\rangle_B) \\ & + \frac{1}{2} |\phi_3\rangle_{AC} \otimes (\alpha |u\rangle_B - \beta |d\rangle_B) \end{aligned}$$

and then by sending only two bits of information, we select an operator and recover Charlie. However, this means that we only need to bits to uniquely describe a continuum of values: $|C\rangle = \alpha |u\rangle + \beta |d\rangle$ and $\alpha, \beta \in \mathbb{C}_1^2$.

Bob's mixture is given by

$$M^B = \frac{1}{2} \delta_{|u\rangle} + \frac{1}{2} \delta_{|d\rangle}$$

so it makes sense that two bits will be enough!

No Cloning Theorem

Special Unitary Operator: $U : \mathbb{C}_1^2 \otimes \mathbb{C}_1^2 \rightarrow \mathbb{C}_1^2 \otimes \mathbb{C}_1^2$

Let $|R\rangle$ be raw material and $|C\rangle$ be a customer such that

$$U |CR\rangle \rightarrow |CC\rangle$$

Theorem: U does not exist.

Proof: Suppose $|C'\rangle$ is another customer. Then

$$U |C'R\rangle = |C'C'\rangle$$

Consider

$$\begin{aligned}
\langle C | C' \rangle^2 &= \langle C | C' \rangle \langle C' | C \rangle \\
&= \langle CR | U^\dagger U | C'R \rangle \\
&= \langle CR | C'R \rangle \\
&= \langle C | C' \rangle \langle R | R \rangle \\
&= \langle C | C' \rangle \\
&= \{0, 1\}
\end{aligned}$$

But C and C' were different customers so they should be independent.

Lecture 28: Nov 13

Encryption and the Singlet State

Assume Alice has a message.

$$(M_1, M_2, \dots, M_M) \in \{0, 1\}^M$$

We prepare $(A_K, B_K) \sim |\psi_k\rangle = \frac{1}{\sqrt{2}}(|ud\rangle_{AB} + |du\rangle_{AB})$ and define new random variables from a measurement that showed $\lambda_K^{(A)}$ and $\lambda_K^{(B)}$ were in the same direction:

$$\gamma_k^{(A)} = \begin{cases} 0 & \text{if } \lambda_K^{(A)} = 1 \\ 1 & \text{if } \lambda_K^{(A)} = -1 \end{cases}, \quad \gamma_k^{(B)} = \begin{cases} 0 & \text{if } \lambda_K^{(B)} = 1 \\ 1 & \text{if } \lambda_K^{(B)} = -1 \end{cases}$$

(with $l \leq K \leq M$) and Alice encodes her message as

$$e_k = M_k \oplus \gamma_K^{(A)}$$

(where \oplus is the XOR operator)

Bob decodes the message by

$$M_k = e_k \oplus \gamma_K^{(A)} = M_k \oplus (1 - \lambda_K^{(B)})$$

The Process

Preparation: $(A_k, B_k) \sim |S\rangle$ independently samples with $1 \leq k \leq n$ and very large n . Bob takes the B_k particles and we would like to make sure the message cannot be determined by an outside observer.

Measurement Direction & Broadcast: Alice and Bob each independently choose a direction

$$\begin{cases} d_k^{(A)} \stackrel{iid}{\sim} (x, y) \\ d_k^{(B)} \stackrel{iid}{\sim} (x, y) \end{cases}$$

and broadcast the directions publicly.

Security Check: Has the particle received by Bob been intercepted on the way?

Let $\mathcal{I} = \{1 \leq k \leq n : d_k^{(A)} = d_k^{(B)}\}$ (a set of indices) to make notation easier. Let $\mathcal{S} \subseteq \mathcal{I}$ be a random subset of \mathcal{I} such that $|\mathcal{S}| \approx \frac{|\mathcal{I}|}{2}$ and $\mathcal{M} = \mathcal{I} \setminus \mathcal{S}$.

For all $k \in \mathcal{I}$, Alice and Bob broadcast $\gamma_k^{(A)} + \gamma_k^{(B)}$. Is $\gamma_k^{(A)} + \gamma_k^{(B)} = 1$?

If not, the channel is unsecure and they should not send the message.

Lecture 29: Nov 15

Recall

Alice wants to send a message to Bob. They prepare $(A, B) \sim |S\rangle$ and define

$$\gamma^{(A)} = \begin{cases} 1 & \lambda^{(A)} = -1 \\ 0 & \lambda^{(A)} = 1 \end{cases}$$

Bob takes the B particles and we would like to make sure the message

$$(m_1, \dots, m_M) \in \{0, 1\}^M$$

sent to him cannot be determined by an outside observer.

Step 1 - Prep: We choose $(A_i, B_i) \stackrel{iid}{\sim} |S\rangle$ for $1 \leq i \leq n$ and large $n > m$.

Step 2: Send an encrypted key $\{B_1, \dots, B_n\}$ to Bob. Charlie would like to intercept B_k by guessing the correct direction d to measure and then transmitting a new B_k on towards Bob.

Step 3 - Broadcast: Broadcast the measurement directions $d_1^{(A)}, \dots, d_n^{(A)} \stackrel{iid}{\sim} \{x, y\}$ and $d_1^{(B)}, \dots, d_n^{(B)} \stackrel{iid}{\sim} \{x, y\}$.

Step 4 - Security Check: Let $\mathcal{I} = \{k \in \{1, \dots, n\} : d_k^{(A)} = d_k^{(B)}\}$ and $S \subseteq \mathcal{I}$ such that $|S| = \frac{|\mathcal{I}|}{2}$. Finally let $\mathcal{M} = \mathcal{I} \setminus S$.

Now Alice measures $\{\gamma_k^{(A)}\}_{k \in S}$ and Bob measures $\{\gamma_k^{(B)}\}_{k \in S}$ from the broadcast.

If $\gamma_k^{(A)} + \gamma_k^{(B)} \neq 1$, the particles are not entangled – because Charlie intercepted them – and the channel is insecure.

If Charlie does intercept the particles, he has a $\frac{1}{2}$ chance of guessing the k -th particle's direction correctly and a $\frac{1}{2} \cdot \frac{1}{2}$ chance of getting the direction wrong but measuring correctly. Thus, for each particle, Charlie has a $\frac{3}{4}$ chance of intercepting the particle undetected.

Step 5: Encrypt the Message Alice encrypts the message

$$e_k = M_k \oplus \gamma_K^{(A)}$$

(where \oplus is the XOR operator)

Bob decodes the message by

$$M_k = e_k \oplus \gamma_K^{(A)} = M_k \oplus (1 - \lambda_K^{(B)})$$

Lecture 29: Nov 17

Free Will

Alice is going to make a measurement. She chooses a direction $D \in \mathbb{R}_1^3$. Let h_A be her “history” or her unique light cone at the time of her decision.

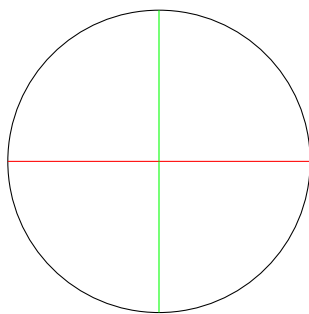
Light cone: From special relativity, *nothing* can travel faster than the speed of light. If we imagine a point in space-time, then the light cone is the set of all points that can reach that point (because their spatial distance in the cone is less than the distance light can travel in the time it takes to reach the point). Thus, the light cone is also a map of causality because no thing outside the boundary of the cone could possibly have an effect on the point.

If $\exists d(h_A) : D = d(h_A)$, then Alice's decision is determined by her history and there is no free will. If no such function exists, there is “free will.”

A Painting Lemma: Consider a circle and the set of all lines through its center. Now let O be the set of all pairs of lines (l_1, l_2) through the center such that l_1 and l_2 are perpendicular. In each pair, paint one of the lines red and the other green.

Each line will create two points on the circle assigned either red or green depending on the color of their generating line. Can we paint every point on the circle red or green?

Of course. Draw one line red and its orthogonal pair green. Then we will have two red points opposite each other and two green points opposite each other and separated 90 degrees from the red points. To color the whole circle, just rotate the red line through an arc of 90 degrees and each of the four quadrants will be painted.



Now consider the 3d space. $O = \{(l_1, l_2, l_3) : l_1 \perp l_2, l_2 \perp l_3, l_1 \perp l_3\}$. Suppose for every triple in O , we paint one line red and the other two green. Can we paint every point in space red or green?

No! It is impossible.

Proof: Let

$$L = \{33 \text{ specifically chosen lines}\} \subset \{\text{the set of lines through the origin in } \mathbb{R}^3\}$$

and

$$O = \{(l_1, l_2, l_3) : l_1, l_2, l_3 \in L, l_1 \perp l_2, l_2 \perp l_3, l_3 \perp l_1\}$$

(Note that $|O| = 16$). Finally, let $A = \{(1, 1, 0), (1, 0, 1), (0, 0, 1)\}$. Our problem thus reduces to showing that for this very particular subset of \mathbb{R}^3 , $\nexists m : O \rightarrow A$.

3 Spin States

Basis: We create a new basis for \mathbb{C}_1^3 :

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |n\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |d\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Such that any $|\psi\rangle \in \mathbb{C}_1^3$ can be written

$$|\psi\rangle = \alpha |u\rangle + \beta |n\rangle + \delta |d\rangle$$

with $|\alpha|^2 + |\beta|^2 + |\delta|^2 = 1$.

Measurements: We define the spin operators by

$$\sigma_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \sigma_y = \frac{i}{\sqrt{2}} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \sigma_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Expected values: as before,

$$\mathbb{E}[\lambda_{\sigma_z}^2 \mid |\psi\rangle] = \mathbb{E}[\lambda_{\sigma_z^2} \mid |\psi\rangle] = 1^2 |\langle\psi \mid u\rangle|^2 + 0^2 |\langle\psi \mid n\rangle|^2 + (-1)^2 |\langle\psi \mid d\rangle|^2$$

(the coefficients are the eigenvalues of the operator so squaring just squares the eigenvalues).

And by analogy, we get the mean squared spin states by $\sigma_x^2, \sigma_y^2, \sigma_z^2$:

$$\sigma_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \sigma_y^2 = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}, \quad \sigma_x^2 = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

This is very useful because while the spin operator matrices do not commute, the squared spin operator matrices do!

$$[\sigma_x^2, \sigma_y^2] = [\sigma_x^2, \sigma_z^2] = [\sigma_y^2, \sigma_z^2] = 0$$

so there exists a common set of 3 eigenvectors:

$$|e_1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |e_2\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \end{pmatrix}, \quad |e_3\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \end{pmatrix}$$

Which lets us create a table to read off the corresponding eigenvalues:

	σ_x^2	σ_y^2	σ_z^2
$ e_1\rangle$	1	1	0
$ e_2\rangle$	1	0	1
$ e_3\rangle$	0	1	1

Conclusion: These are precisely the pairs in A ! Results are not defined until they are measured. There does not exist a hidden h such that $\forall l \in L, \lambda_l = l(h)$.

This is precisely the same conclusion as we got from Bell's without using probabilities at all.

Lecture 30: Nov 27

Background in \mathbb{C}_1^3

A combinatorial result:

L is a particular set of lines through the origin with $|L| = 33$. O is the set of triples of lines in L which are mutually perpendicular. $A = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$.

Kochen-Specker Theorem: There does not exist a function $m : L \rightarrow \{0, 1\}$ for which

$$(m(l_1), m(l_2), m(l_3)) \in A \quad \forall (l_1, l_2, l_3) \in O$$

Spin 2 State Space: We have basis vectors

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |n\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |d\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

leading to arbitrary states

$$|\psi\rangle = \alpha |u\rangle + \beta |n\rangle + \delta |d\rangle \in \mathbb{C}_1^3$$

We can also calculate spin operators,

$$\sigma_x = \begin{pmatrix} 0 & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i/\sqrt{2} & 0 \\ i/\sqrt{2} & 0 & -i/\sqrt{2} \\ 0 & i/\sqrt{2} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

whose eigenvalues are all in $\{-1, 0, 1\}$

We also have squared operators $\sigma_x^2, \sigma_y^2, \sigma_z^2$ which correspond to measuring $\lambda_x^2, \lambda_y^2, \lambda_z^2 \in \{0, 1\}$.

As in the spin 1 case, these squared operators commute if and only if there exists a common set of eigenvectors:

$$|e_1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |e_2\rangle = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad |e_3\rangle = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

Using these eigenvectors, we create a chart of eigenvalues for the squared operators:

	σ_x^2	σ_y^2	σ_z^2	
$ e_1\rangle$	1	1	0	
$ e_2\rangle$	1	0	1	
$ e_3\rangle$	0	1	1	

The No-Go Theorem

Because of the Kochen-Specker Theorem and rotational invariance for all $(l_1, l_2, l_3) \in O$, we have a problem: If measurements could be known before hand (e.g. by knowing a hidden variable $h \in H$ a la Einstein's belief), then we could say the eigenvalues were functions of h that took a value in $\{(1, 1, 0), (1, 0, 1), (0, 0, 1)\}$. But this is impossible!

This is a *stronger* result than Bell's Theorem because it does not make use of probability. So we have yet another no-go on hidden variables.

A way out: There is still a way hidden variables could work though! Suppose $h \rightarrow h \times h_a$ for a particle a .

Consider the singlet in \mathbb{C}_1^3 :

$$|S\rangle = \frac{1}{\sqrt{3}}(|ud\rangle + |nn\rangle - |du\rangle)$$

For this state, we have six measurements that are very easy to calculate. Furthermore, they all commute with each other and share the same eigenvectors:

	$ e_1e_1\rangle$	$ e_2e_2\rangle$	$ e_3e_3\rangle$
$\sigma_x^2 \otimes I$	1	1	0
$\sigma_y^2 \otimes I$	1	0	1
$\sigma_z^2 \otimes I$	0	1	1
$I \otimes \sigma_x^2$	1	1	0
$I \otimes \sigma_y^2$	1	0	1
$I \otimes \sigma_z^2$	0	1	1

This leads to the *TWIN* property: particle 2 is clearly a twin of particle 1.

What if the particles are very far apart? Imagine the light cones from the two particles. If there is a hidden particle, then the state of b depends on $h \times h_b$. But we can arrange the light cones so that h_b is outside the light cone of a and h_a is outside the light cone of b . By special relativity, we can make it such that Bob chooses h_b in Alice's future. Thus, Alice's choice of h_a cannot depend on Bob's choice of h_b . But similarly, Alice chooses in Bob's future.

Lecture 31: Nov 29

Overview of Quantum Computing

1. We have a sequence of n particles in energy wells. We can represent the state of the system as a vector in $\mathbb{C}^{2^{\otimes n}} = \underbrace{\mathbb{C}_1^2 \otimes \mathbb{C}_1^2 \otimes \cdots \otimes \mathbb{C}_1^2}_n$.
2. Initialize $|\psi_0\rangle \in \mathbb{C}_1^{2^{\otimes n}}$
3. Perform a sequence of unitary operators with the goal of finding a $|g\rangle \in \mathbb{C}_1^{2^{\otimes n}}$ such that $g \iff x \in \{0,1\}^n$ ($x = x_1, x_2, \dots, x_n \in 2^n$)
4. Iterate operators until $|\psi_t\rangle \approx |g\rangle$ (i.e. $\forall \varepsilon > 0 : \mathbb{P}(|\psi\rangle \rightarrow |g\rangle) > 1 - \varepsilon$)
5. Readout: measure $|\psi\rangle$ by measuring each coordinate (so that all measurements commute)

Essential Background

Unitary Operator: $UU^\dagger = U^\dagger U = I$ (reflections and rotations)

Every unitary operator U can be realized (by a physical machine)

Evolution of a physical system is accomplished through unitary operators (because of preservation of total probability mass)

$$|\psi(t)\rangle = U_t |\psi_0\rangle \implies \frac{d\psi}{dt} = -i\hbar H |\psi(0)\rangle \iff |\psi(t)\rangle = e^{-\frac{i}{\hbar} H t} |\psi(0)\rangle$$

And the spectral representation of unitary operators is given by

$$U = \sum_{k=1}^m e^{i\theta_k} |e_k\rangle \langle e_k|$$

which implies a Hamiltonian operator with real values

$$H = \sum_{k=1}^m \theta_k |e_k\rangle \langle e_k|$$

Conclusion: for any unitary operator, we can find a Hamiltonian representing a real physical state/environment for which we can build a machine that will induce that state. Thus, we can build a machine that will perform any unitary operator by running long enough.

Notation:

- $|u\rangle \leftrightarrow |0\rangle$
- $|d\rangle \leftrightarrow |1\rangle$
- $X = (X_1, \dots, X_n) \in \{0, 1\}^n \leftrightarrow |x\rangle \in \mathbb{C}_1^{2^n}$
- $|\psi\rangle = \sum_{x_1, x_2, \dots, x_n} \gamma_{x_1, x_2, \dots, x_n} |x_1, x_2, \dots, x_n\rangle = \sum_x \gamma_x |x\rangle$ where x is all sequence of 2^n zeros and ones

Example:

$$\begin{aligned} |\psi\rangle &= \left(\frac{1}{\sqrt{2}}\right)^3 \sum_x |x\rangle \in \mathbb{C}_1^{(2^{\otimes 3})} \\ &= \left(\frac{1}{\sqrt{2}}\right)^3 (|uuu\rangle + |uud\rangle + |udu\rangle + |duu\rangle + |udd\rangle + |dud\rangle + |ddu\rangle + |ddd\rangle) \\ &= |r\rangle \otimes |r\rangle \otimes |r\rangle \end{aligned}$$

In fact, this makes a very good initial state because it is “neutral” with respect to the up and down directions.

How do we measure $|\psi\rangle$? Say we have $|\psi(T)\rangle$ and we want to measure it. We know

$$\mathbb{P}(|\psi\rangle \rightarrow |g\rangle) > 1 - \varepsilon$$

but in general,

$$\mathbb{P}(|\psi\rangle \rightarrow x) = |\langle x | \psi \rangle|^2$$

and

$$A \otimes B = (A \otimes I)(I \otimes B) = B \otimes A$$

Lecture 32: Dec 01

Quantum Computing

We have a data structure called the *register*

$$x = (x_1, x_2, \dots, x_n) \in \{0, 1\}^n \leftrightarrow |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle \in \mathbb{C}^{2^n}$$

with $x_k = 1 \leftrightarrow |d\rangle$, $x_k = 0 \leftrightarrow |u\rangle$

Basis: $B = \{|x\rangle : (x_1, x_2, \dots, x_n) \in \{0, 1\}^n\}$ with

$$|\psi\rangle = \sum_{x_1} \sum_{x_2} \dots \sum_{x_n} \gamma_{x_1, \dots, x_n} |x_1\rangle \otimes \dots \otimes |x_n\rangle = \sum_{x \in B} \gamma_x |x\rangle$$

Generic operator:

$$\sum_{i=1}^m \gamma_i \gamma_i A_1 \otimes A_2 \otimes \dots \otimes A_n$$

Example in $\mathbb{C}^2 \otimes \mathbb{C}^2$: $A_1 \otimes B_1 + A_2 \otimes B_2$

Readout: we measure each particle in the register independently using

$$\sigma_{z_i} = \underbrace{I \otimes \dots \otimes I}_{i-1} \otimes \sigma_z \otimes \underbrace{I \otimes \dots \otimes I}_{n-i-1}$$

And since for all i , the σ_{z_i} s commute, we can measure in any order.

Goal (Boolean Satisfiability): Given a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, find $g \in \{0, 1\}^n$ such that $f(g) = 1$. We assume that there is a unique g that satisfies this property.

The best known classical algorithm for this search problem is $O(2^n)$ (i.e. brute force).

Grover's Algorithm does it in $O(2^{n/2})$.

Boolean function Example (XOR/CNOT):

$$\begin{cases} \{0,1\} \rightarrow 1 \\ \{1,0\} \rightarrow 1 \\ \{0,0\} \rightarrow 0 \\ \{1,1\} \rightarrow 0 \end{cases} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Grover's Algorithm

1. **Prepare the register.** Notice that $(-1)^{f(x)} |x\rangle$ is a unitary operator on $|x\rangle$. Further, by uniqueness of g ,

$$(-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle & x = g \\ |x\rangle & x \neq g \end{cases}$$

Because it is unitary, we can build a machine to create it via Schrodinger and the Hamiltonian. But also, we can prepare the register in such a way that all the elements are entangled which means that they are in a superposition of all possible states in the space – one of which must be g .

Thus, we initialize the register

$$|\psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle = \frac{1}{\sqrt{2}} |r\rangle \otimes |r\rangle \otimes \cdots \otimes |r\rangle$$

Lecture 33: Dec 4

Setup

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a boolean function with a unique g such that $f(g) = 1$.

We designate a basis by the set

$$\{|x\rangle = |x_1, \dots, x_n\rangle : (x_1, \dots, x_n) \in \{0,1\}^n\}$$

And let the state space be

$$V = \left\{ \sum_{x=x_1}^{x_n} \gamma_x |x\rangle \mid \sum_x |\gamma_x|^2 = 1 \right\}$$

And prepare the register of particles x_1, \dots, x_n by

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle = |r\rangle \otimes |r\rangle \otimes \dots \otimes |r\rangle$$

Suppose we are given an “oracle” which evaluates $f(x)$.

Thus, we are searching the state space \mathbb{V} for the input which the oracle evaluates to 1.

Lastly, we define

$$|\psi'\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq g} |x\rangle$$

and a subspace

$$S = \{x \in \mathbb{V} : |x\rangle = \alpha |g\rangle + \beta |\psi'\rangle, \alpha^2 + \beta^2 = 1, \alpha, \beta \in \mathbb{R}\}$$

Notice that \mathbb{V} is a space of dimension 2^n and S is a linear space of two real dimensions.

The Process

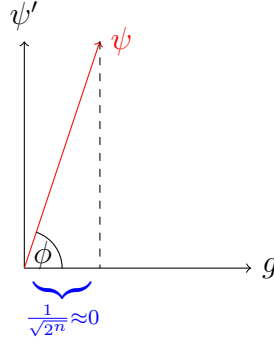
Notice that

1. $\langle g | \psi' \rangle = 0$
2. $|g\rangle, |\psi\rangle, |\psi'\rangle$ are all linear combinations of $|g\rangle$ and $|\psi'\rangle$ with real coefficients:

$$\begin{aligned} |g\rangle &= 1 |g\rangle + 0 |\psi'\rangle \\ |\psi'\rangle &= 0 |g\rangle + 1 |\psi'\rangle \\ |\psi\rangle &= \frac{1}{2^n} |g\rangle + \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\psi'\rangle \end{aligned}$$

So $|g\rangle, |\psi\rangle, |\psi'\rangle \in S$.

We have a picture:



and since the distance is negligible, $\phi \approx \frac{\pi}{2}$

Any unitary operator $U : S \rightarrow S$ will satisfy

$$U(\alpha |g\rangle + \beta |\psi'\rangle) = \alpha U |g\rangle + \beta U |\psi'\rangle$$

so we can define V by

$$V = I - 2 |g\rangle \langle g|$$

$$Vx = \begin{cases} -1 & x = g \\ 1 & x \neq g \end{cases} = (-1)^{f(x)} |x\rangle$$

We can check that $V^\dagger V = VV^\dagger = I$ and add another operator

$$W = 2 |\psi\rangle \langle \psi| - I$$

So WV is unitary. Doing some arithmetic, we find

$$WV |g\rangle = a |g\rangle - b |\psi'\rangle$$

$$WV |\psi'\rangle = b |g\rangle + a |\psi'\rangle$$

and

$$a = (1 - \frac{2}{2^n})$$

$$b = \frac{2\sqrt{2^n - 1}}{2^n}$$

which means that WV acts on S be a rotation clockwise through

$$\theta = \sin^{-1}(b) = \sin^{-1}(\frac{2\sqrt{2^n - 1}}{2^n}) \approx \frac{1}{\sqrt{2^n}}$$

Thus, by repeatedly applying VW we can get arbitrarily close to $\theta = 0$ and thus find g .

Lecture 34: Dec 06

Quantum Gates

In the implementation of Grover's Algorithm, we used two gates, V and W , that seemed to be arbitrary. Here we will explore V a bit more.

We'll use the usual basis $B = \{|x_1, \dots, x_n\rangle : x_k \in \{0, 1\}\}$ and a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$

Recall from above that

$$V|x\rangle = (-1)^{f(x)}|x\rangle \quad |x\rangle \in B$$

so the effect of $V|\psi\rangle$ is to act on the superposition of all possible states to “mark” the solution g by changing the sign of the amplitude of $|g\rangle$:

$$V|\psi\rangle = V \sum_x \gamma_x |x\rangle = \sum_x \gamma_x V|x\rangle = \sum_x \gamma_x (-1)^{f(x)} |x\rangle$$

Now we define a new operator \oplus which takes $|x, y\rangle \rightarrow |x, x \oplus y\rangle$ where $x, y \in \{0, 1\}$ and $x \oplus y = x + y \pmod{2}$:

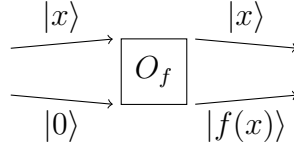
$$\begin{aligned} (0, 0) &\rightarrow (0, 0) \\ (0, 1) &\rightarrow (0, 1) \\ (1, 0) &\rightarrow (1, 1) \\ (1, 1) &\rightarrow (1, 0) \end{aligned}$$

which can be express as a matrix

$$\oplus = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and this happens to be precisely CNOT.

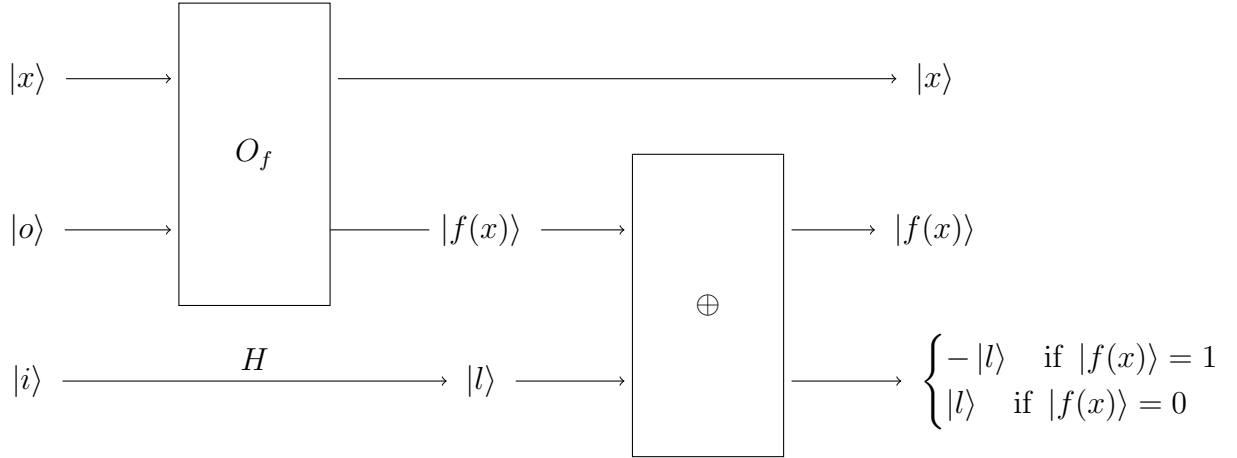
The problem is that if we applied this directly to $|\psi\rangle$, we would no longer have a unitary operator because some info was destroyed. To solve this, we add an *ancillary bit* so $x \rightarrow |x, y\rangle$ so our oracle now looks like:



Now we have

$$H|x\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} |x\rangle \rightarrow \begin{cases} |r\rangle = \frac{1}{\sqrt{2}}(|o\rangle + |i\rangle) & x = 0 \\ |l\rangle = \frac{1}{\sqrt{2}}(|o\rangle - |i\rangle) & x = 1 \end{cases}$$

Which gives us a full circuit,



So a single bit is flipped for the correct input and we can see that by measuring the outputted $|x\rangle$