NYU

Introduction to Data Science

Center for Data Science
Iddo Drori, Spring 2019

NYU

Quantum Information Science

Quantum Information Science

- Disruptive

- IBM research made available access to IBM QX via the cloud.

Quantum Information Science

- Speculative
- Quantum supremacy in 2 years, advantage in 5 years, computers in 20 years.

Math and CS

- Linear Algebra: linear combination of orthonormal basis, tensor product
- Probability
- Logic: gates and circuits
- Algorithms
- Geometry

Applications

- Cryptography
- Radar
- Computation

Spin

- Bit: 0/1
- Qubit: spin of electron, polarization of photon

Atom

- Positive nucleus
- Negative electrons orbiting

Atom

Atom as whole is magnet with S/N poles

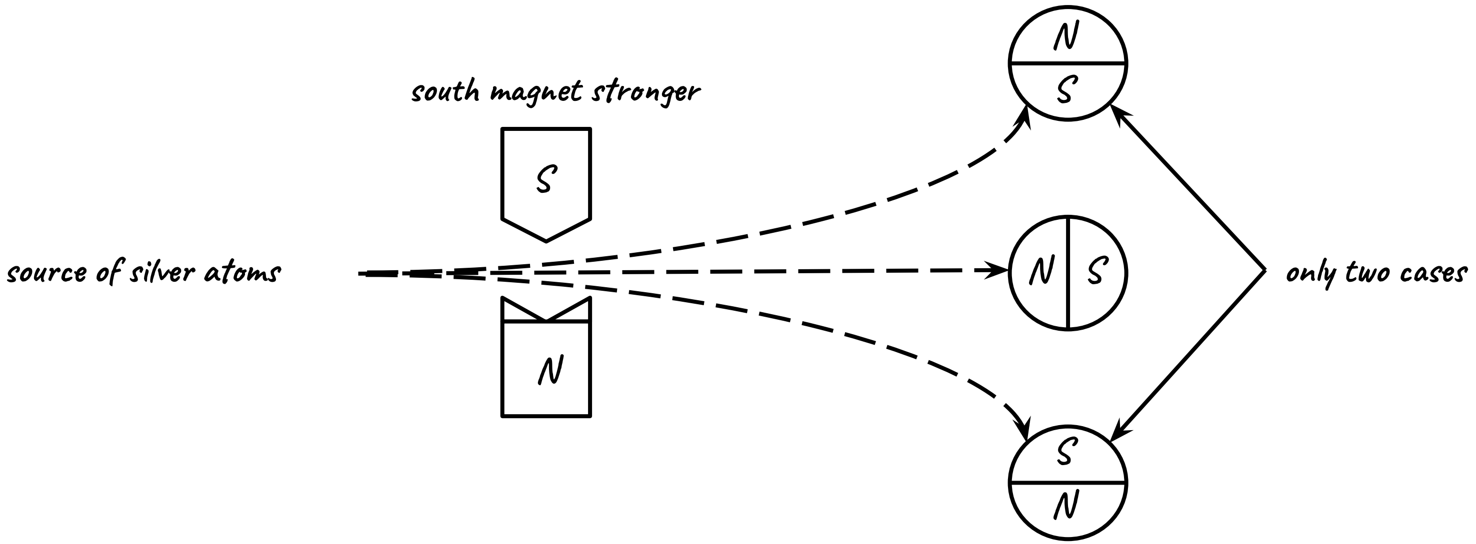
Magnetic fields cancel each other

- Inner orbit: 2 electrons opposite directions
- 2nd orbit: 8 electrons
- 3rd orbit: 18 electrons
- 4th orbit: 18 electrons

Not cancelled

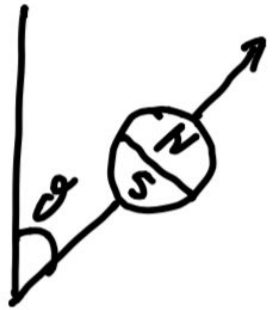
- 5th orbit: 1 electron for silver

Experiment: Stern and Gerlach



Electron Spin

- Ask/measure direction: either yes in direction or in opposite direction
- Qubit -> measurement -> bit
- Repeat same measurement get same answer
- Measurements in different directions: measure vertical then horizontal 50/50



Electron Spin

- Repeat same measurements -> same answer
- Randomness occurs: sequence of measurements
- Measurements effect outcomes
    - Classical mechanics: throw ball, measure velocity, no effect of random photons on ball
    - Quantum mechanics: measuring electron spin effects spin, tiny particles.

Randomness

- Measure spin in vertical direction
- Then, measure spin in horizontal direction
- Random sequence of N,S,...
- Real randomness, no hidden variables
- Vs. coin flip: classical mechanics, sensitive dependence on initial conditions.

Polarization

- Polarized light experiment: more light through 3 than 2 sheets.
- Photons are polarized in two directions, orthogonal to direction of light travel

Notation

- $|a\rangle$ column vector
- $\langle a|$ row vector

Linear algebra

- Are $|a_1\rangle,\ldots,|a_n\rangle$ an orthonormal basis? Iff $A^TA = I$
- Express $|y\rangle$ using orthonormal basis |a1>,...,|an>

$|y\rangle = x_1|a_1\rangle+\ldots+x_n|a_n\rangle$ iff $\langle y| = x_1\langle a_1|+\ldots+x_n\langle a_n|$

$y = Ax$

$A^Ty = A^TAx$

$A^Ty = x$

$\langle a_i|y\rangle = x_i$

Notation

- What is the length of $|y\rangle$?

$$\||y\rangle\|^2 = \langle y|y\rangle = (x_1|a_1\rangle+\dots+x_n|a_n\rangle)(x_1|a_1\rangle+\dots+x_n|a_n\rangle) = x_1^2+\dots+x_n^2$$

Notation

Orthonormal basis:

- |up> = [1]
[0] |down> = [0]
[1]
- <up|up> = 1 <down|down> = 1 <up|down> = 0 <down|up> = 0

- |right> = [1/sqrt(2)]
[-1/sqrt(2)] |left> = [1/sqrt(2)]
[1/sqrt(2)]
- <right|right> = 1 <left|left> = 1 <right|left> = 0 <left|right> = 0

- |upright> = [½]
[-sqrt(3)/2] |downleft> = [sqrt(3)/2]
[½]
- <upright|upright> = 1 <downleft|downleft> = 1 <upright|downleft> = 0 <downleft|upright> = 0

Spin State: Linear Combination

- $|y\rangle = x_0|a_0\rangle + x_1|a_1\rangle$ represented by orthonormal basis

Once measured:

- $|y\rangle$ jumps to $|a_0\rangle$ with probability x_0^2, $x_0 = \langle a_0|y\rangle$
- $|y\rangle$ jump to $|a_1\rangle$ with probability x_1^2, $x_1 = \langle a_1|y\rangle$

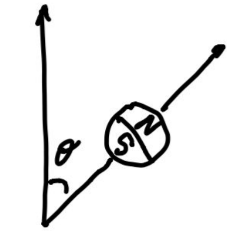
Electron Spin State

- |y>
- Measure using orthonormal basis |up>, |down>
- Measurement results in |up>
- Measure again using orthonormal basis |up>, |down>
- |up> = 1 |up> + 0 |down>
- Measurement results in |up>
- Measure using orthonormal basis |right>,|left>
- |up> = [1] = x0|right> + x1|left> = x0[1/sqrt(2)] + x1[1/sqrt(2)]
  [0]   [-1/sqrt(2)]   [1/sqrt(2)]
- |xi> = <ai|y>
- x0 = <up|right> = [1/sqrt(2), -1/sqrt(2)][1] = 1/sqrt(2)   x0^2 = ½
  [0]
- x1 = <up|left> = [1/sqrt(2)], 1/sqrt(2)][1] = 1/sqrt(2)   x1^2 = ½
  [0]

Linear Combination

- No measurement can distinguish between
- $|up\rangle = x_0|a_0\rangle + x_1|a_1\rangle$ and $-|up\rangle = -x_0|a_0\rangle - x_1|a_1\rangle$
- Or between $|y\rangle$ and $-|y\rangle$ since $x_0^2 = (-x_0)^2$ and $x_1^2 = (-x_1)^2$
- so they are equivalent

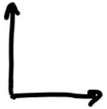
Basis of Measurement



$$\begin{bmatrix}\cos\frac{\theta}{2}\\ -\sin\frac{\theta}{2}\end{bmatrix}, \begin{bmatrix}\sin\frac{\theta}{2}\\ \cos\frac{\theta}{2}\end{bmatrix}$$ basis of measurement

θ angle rotating measurement

α angle rotating basis vectors

 equivalent to  in different orders

so $\theta = 2\alpha$

Polarization Experiment

- Rotate polarized filter by angle beta
- Lets through photons polarized in direction beta
- Blocks photons polarized in direction orthogonal to beta
- Orthonormal basis [cos(beta)] [sin(beta)]

  [-sin(beta)] [cos(beta)]

NYU

Polarization Experiment

- 1st measurement: $\begin{bmatrix}1\\0\end{bmatrix}$, $\begin{bmatrix}0\\1\end{bmatrix}$ photons will be in state $\begin{bmatrix}1\\0\end{bmatrix}$
- 2nd measurement: rotated 45 degrees $\begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix}$, $\begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}$
- $\begin{bmatrix}0\\1\end{bmatrix} = 1/\sqrt{2} \begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix} + 1/\sqrt{2} \begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}$
- Probability of passing is ½, photons passing in state $\begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix}$
- 3rd measurement: $\begin{bmatrix}0\\1\end{bmatrix}$, $\begin{bmatrix}1\\0\end{bmatrix}$

  $[1/\sqrt{2},-1/\sqrt{2}] = -1/\sqrt{2}\begin{bmatrix}0\\1\end{bmatrix} + 1/\sqrt{2}\begin{bmatrix}1\\0\end{bmatrix}$
- Probability of passing ½, lets through photons in state $\begin{bmatrix}1\\0\end{bmatrix}$

Qubit

- $|y\rangle$ in R^2
- Measurement introduces orthonormal basis $|a_0\rangle, |a_1\rangle$
- Qubit written as superposition of basis vectors same as
- Vector written as linear combination of basis vectors

$$|y\rangle = x_0|a_0\rangle + x_1|a_1\rangle$$

- After measurement qubit state jumps

  to $|a0\rangle$ with probability x_0^2

  to $|a1\rangle$ with probability x_1^2

- Associate $|a0\rangle$ with 0 and $|a1\rangle$ with 1
- Qubit has infinite possible values, once measured we get $0/1$

Two Qubits

- Alice: orthonormal basis $|a_0\rangle, |a_1\rangle$
- Bob: orthonormal basis $|b_0\rangle, |b_1\rangle$
- Alice wants to send Bob a 0
- Alice sends qubit in state $|a_0\rangle$
- Bob measures with respect to his basis

  $|a_0\rangle = x_0|b_0\rangle + x_1|b_1\rangle$
- State jumps to $|b_0\rangle$ with probability x_0^2
- Jumps to $|b_1\rangle$ with probability x_1^2

Secure Communication: Bennet & Brassard (BB84)

- Alice and Bob want to communicate securely, Eve wants to eavesdrop.
- Alice sends Bob a stream of qubits
- Alice measures qubits using her orthonormal basis |a0>,|a1>
- Bob measures qubits that Alice sends him using his orthonormal basis |b0>,|b1>
- If Alice wants to send 0 she can send qubit in state |a0>
- Bob measures with respect to his basis so |a0> = d0|b0>+d1|b1>
- Qubit jumps

  To |b0> with probability d0^2 and Bob writes 0

  To |b1> with probability d1^2 and Bob writes 1
- If Alice and Bob use the same basis they will always receive same bit, however if Eve chooses same basis she will receive the message
- Therefore, Alice and Bob choose different basis

Secure Communication: Bennet & Brassard (BB84)

- If Alice and Bob choose same bases then Bob will get same bit that Alice sent
- If Alice and Bob choose different bases then half the time Bob gets correct bit and half the time Bob gets wrong bit.

Secure Communication: Bennet & Brassard (BB84)

- Alice chooses a key she wants to send to Bob
- 2 basis:
- *V* = [1],[0]   *H* = [1/sqrt(2)], [1/sqrt(2)]
  [0] [1]   [-1/sqrt(2)], [1/sqrt(2)]
- Key is string of bits used for encryption
- Alice chooses a basis *V* or *H* at random with equal probability
- Alice sends Bob qubit consisting of appropriate basis vector

  If Alice wants to send Bob *0* and chooses *V* she sends [1]
  [0]

  If Alice wants to send Bob *0* and chooses *H* she sends [1/sqrt(2)]
  [-1/sqrt(2)]

- If key string is length *4n* binary bits then Alice stores string of *4n* *V*s or *H*s

BB84

- Bob randomly chooses between basis V and H with equal probability
- Bob measures qubit in chosen basis
- Bob stores string of length $4n$ of bits: measurements
- Bob stores string of length $4n$ of Vs, Hs: basis chosen

BB84

- Alice and Bob choose basis at random
- Half the time they choose the same basis then Bob gets bit that Alice sent
- Half the time they choose different basis then

    Half the time Bob gets right bit

    Half the time Bob gets wrong bit
- Alice and Bob compare basis strings of Vs, Hs over unencrypted line and keep bits where basis are same

  Erase bits where basis are different
- If Eve is not intercepting they get same string of bit of length $2n$

BB84: Eve

- If Eve intercepts
- Consider only $2n$ cases where Alice and Bob's basis are the same
- Eve choose basis at random
- Half the time (n) Eve choose right basis which is same for all three
- Half the time (n) Eve chooses wrong basis

  Eve sends Bob qubit

  Bob measures qubit and gets $0/1$ with equal probability

  Bob gets correct bit half the time $\frac{1}{2}n$

BB84: Eve

- Alice and Bob have strings of bits of length $2n$
- If Eve is not intercepting the strings are identical
  and they use n of the bits as key

- If Eve is intercepting she will choose wrong basis half the time, so a quarter of Bob’s bits will disagree with Alice
  and they know the line is insecure

2 Qubits

- Alice has 1 qubit

$$/v> = x0/a0> + x1/a1>$$

- Bob has another qubit

$$/w> = y0/b0> + y1/b1>$$

- Tensor product

$$/v> x /w> = x0y0/a0>x/b0>+x0y1/a0>x/b1>+x1y0/a1>x/b0>+x1y1/a1>x/b1>$$

$$/v>/w> = x0y0/a0>/b0>+x0y1/a0>/b1>+x1y0/a1>/b0>+x1y1/a1>/b1>$$

$$/vw> = r/00>+s/01>+t/10>+u/11>$$

$r^2 + s^2 + t^2 + u^2 = 1$ probabilities

$$ru = st = x_0y_0x_1y_1$$

2 Qubits

- Represent $|v\rangle$ and $|w\rangle$ using the form
- $r|a_0\rangle|b_0\rangle + s|a_0\rangle|b_1\rangle + t|a_1\rangle|b_0\rangle + u|a_1\rangle|b_1\rangle$
- Allow any values of r,s,t,u such that $r^2 + s^2 + t^2 + u^2 = 1$
- If $ru = st$ Alice and Bob's qubits are not entangled
- If $ru \mathrel{!}= st$ Alice and Bob's qubits are entangled

Unentangled Qubits

- $|v\rangle|w\rangle = 1/2\mathrm{sqrt}(2)|a_0\rangle|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_0\rangle|b_1\rangle + 1/2\mathrm{sqrt}(2)|a_1\rangle|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_1\rangle|b_1\rangle$
- $ru = \mathrm{sqrt}(3)/8 = st$ -> qubits are not entangled
- If Alice and Bob both make measurements:
- 00 with probability ⅛
- 01 with probability ⅜
- 10 with probability ⅛
- 11 with probability ⅜

Unentangled Qubits

- $|v\rangle|w\rangle = 1/2\mathrm{sqrt}(2)|a_0\rangle|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_0\rangle|b_1\rangle + 1/2\mathrm{sqrt}(2)|a_1\rangle|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_1\rangle|b_1\rangle =$
  $|a_0\rangle(|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_0\rangle|b_1\rangle + 1/2\mathrm{sqrt}(2)|a_1\rangle|b_0\rangle + \mathrm{sqrt}(3)/2\mathrm{sqrt}(2)|a_1\rangle|b_1\rangle =$
  $(1/\mathrm{sqrt}(2)|a_0\rangle+1/\mathrm{sqrt}(2)|a_1\rangle)(\tfrac{1}{2}|b_0\rangle+\mathrm{sqrt}(3)/2|b_1\rangle)$
- If Alice measures first obtains $0/1$ with probability $\tfrac{1}{2}$
- If bob measures first obtains $0/1$ with probability $\tfrac{1}{4}, \tfrac{3}{4}$
- Alice’s measurements have no effect on Bob’s measurements
- Bob’s measurements have no effect on Alice’s measurements

Entangled Qubits

- $v\rangle|w\rangle = 1/2|a_0\rangle|b_0\rangle + 1/2|a_0\rangle|b_1\rangle + 1/sqrt(2)|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle$
- $ru = 0 \mathrel{!=} st = 1/2sqrt(2)$ -> qubits are entangled
- If Alice and Bob both make measurements
- 00 with probability ¼
- 01 with probability ¼
- 10 with probability ½
- 11 with probability 0

Entangled Qubits

- $|v\rangle|w\rangle = \frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + 1/\text{sqrt}(2)|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle =$ $|a_0\rangle(\frac{1}{2}|b_0\rangle + \frac{1}{2}|b_1\rangle) + |a_1\rangle(1/\text{sqrt}(2)|b_0\rangle + 0|b_1\rangle) =$ $1/\text{sqrt}(2)|a_0\rangle(1/\text{sqrt}(2)|b_0\rangle + 1/\text{sqrt}(2)|b_1\rangle) + 1/\text{sqrt}(2)|a_1\rangle(1|b_0\rangle + 0|b_1\rangle)$
- Terms in parentheses are different, qubits are entangled
- If Alice makes a measurement, will get $0/1$ with probability $\frac{1}{2}$
- When Alice gets 0 her qubit jumps to $|a_0\rangle$ and system jumps to $|a_0\rangle(1/\text{sqrt}(2)|b_0\rangle + 1/\text{sqrt}(2)|b_1\rangle)$ and Bob's qubit becomes $(1/\text{sqrt}(2)|b_0\rangle + 1/\text{sqrt}(2)|b_1\rangle)$ and is no longer entangled with Alice's
- Alice gets 1 her qubit jumps to $|a_1\rangle$ system jumps to $|a_1\rangle(1|b_0\rangle + 0|b_1\rangle)$ and Bob's qubit becomes $|b_0\rangle$ and is no longer entangled with Alice's

Entangled Qubits

- $v\rangle|w\rangle = 1/\text{sqrt}(2)|a_0\rangle(1/\text{sqrt}(2)|b_0\rangle + 1/\text{sqrt}(2)|b_1\rangle) + 1/\text{sqrt}(2)|a_1\rangle(1|b_0\rangle + 0|b_1\rangle)$
- Terms in parentheses are different, qubits are entangled
- Result of Alice's measurement effects Bob's qubit
- When Alice gets 0 -> Bob's qubit becomes $(1/\text{sqrt}(2)|b_0\rangle + 1/\text{sqrt}(2)|b_1\rangle)$
- When Alice gets 1 -> Bob's qubit becomes $|b_0\rangle$
- Alice and Bob's qubits can be far apart!

Entangled Qubits

- From Bob's perspective
- $v\rangle|w\rangle = \frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + 1/\mathrm{sqrt}(2)|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle =$
  $\mathrm{sqrt}(3)/2|b_0\rangle(1/\mathrm{sqrt}(3)|a_0\rangle+\mathrm{sqrt}(2)/\mathrm{sqrt}(3)|a_1\rangle)+\frac{1}{2}|b_1\rangle(1|a_0\rangle+0|a_1\rangle)$
- When Bob measures his qubit he gets
- 0 with probability $\frac{3}{4}$ and Alice jumps to $(1/\mathrm{sqrt}(3)|a_0\rangle+\mathrm{sqrt}(2)/\mathrm{sqrt}(3)|a_1\rangle)$
- 1 with probability $\frac{1}{4}$ and Alice jumps to $(1|a_0\rangle+0|a_1\rangle)$
- 00 with probability $\frac{3}{4}\ \frac{1}{3} = \frac{1}{4}$ Alice get $0/1$ with probability $\frac{1}{2}$
- 10 with probability $\frac{3}{4}\ \frac{2}{3} = \frac{1}{2}$ Alice cannot tell from her measurements
- 01 with probability $\frac{1}{4}\ 1 = \frac{1}{4}$ whether they were before or after Bob's
- 11 with probability $\frac{1}{4}\ 0 = 0$ no conflict with Einstein's theory of relativity