☐ Quantum Computing - Less Formulae - More Understanding

☐ The Introduction to Quantum Computing

(1.) Introduction
- Why Quantum Computers are so powerful?
- Why is it hard to implement them?

(2) The Origins of Mathematical Model. (P1)

(3) The Origins of Mathematical Model. (P2)

(4) The Language of Quantum mechanics.

(5) Quantum Cryptography & Teleportation

DR. SERGEY SYSOEV

"THERE IS NO USEFUL QUANTUM COMPUTER IMPLEMENTED UPTO THIS TIME." 04/08/2021

School Level Math (Week 1)

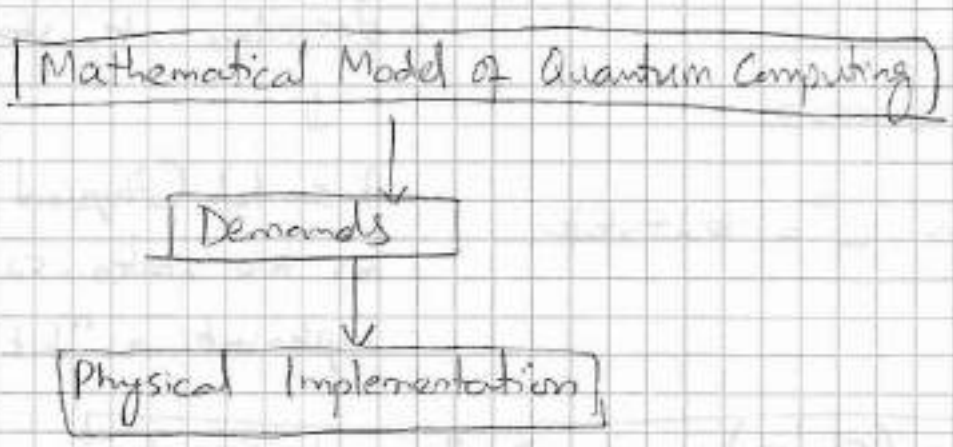
QUANTUM COMPUTING
LESS FORMULAS —
MORE UNDERSTANDING

THE CONSEQUENCES OF THE MATHEMATICAL MODEL

Simple but wrong Explanation

VERSUS

Correct but too Complicated Explanation



- We will assume that we already have the mathematical Model.

Description (As an input)

↳ (Deduce) → Which kind of physical process meets the requirements of this Mathematical Model.

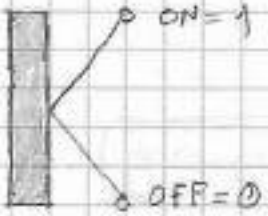
THREE DEMANDS TO COMPUTE THE PHYSICAL PROCESS, THAT WE DEDUCE FROM MATHEMATICAL MODEL, ARE:

1. Continuum of States
2. True Randomness
3. Interference

THE STATE SPACE

(Infinity of States)

A QUBIT



10-Switches = 2^{10} = 1024 states

Classical Computing

- 1 bit of information encoding.
- describes its state (on, off)

↓

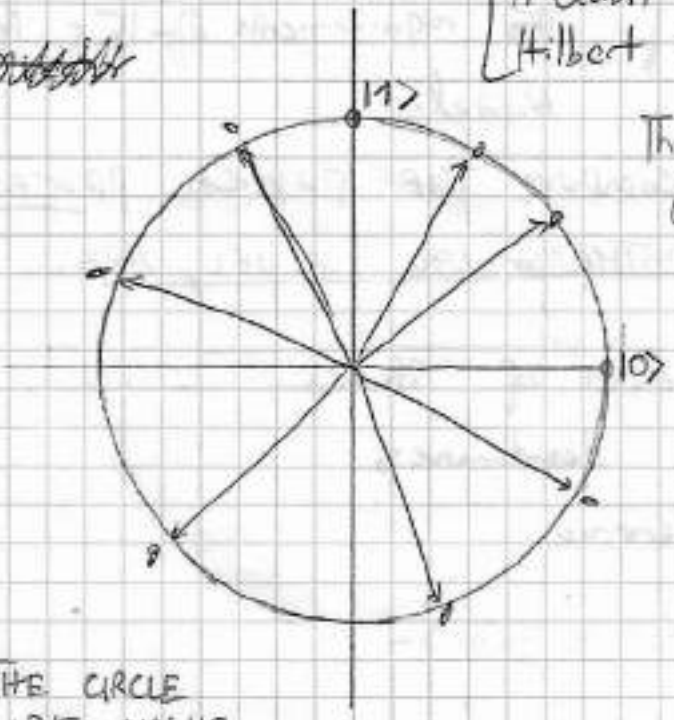
A switch (Physical System) has two states, so it can implement a "bit" for us.

$$\log_2(\text{States}) = \#\text{ of Required Switches}$$

[Mathematical model of Quantum Computing Systems, The simplest quantum system is represented by 1 Qubit instead of one classical bit]

[A Qubit is a unit vector in 2D Hilbert Space]

~~a qubit is in 2D~~



Think of it as a 2D Circle

- So a qubit can represent for us a classical bit two

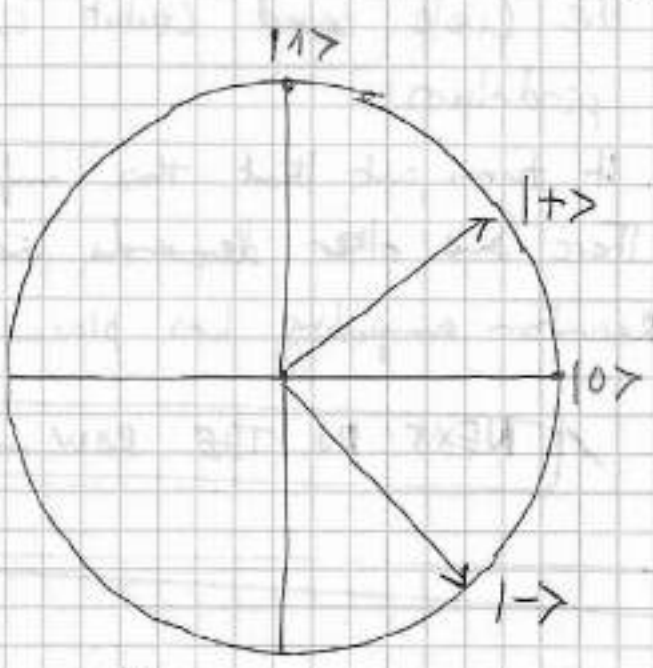
- ANY POINT ON THE CIRCLE COULD BE A QUBIT VALUE

In Quantum Algorithms we are interested in these two states

$|+\rangle$, and $|-\rangle$ (plus & minus)

which we denote as

(The state $|+\rangle$, for example, represents the superposition of 1 & 0 states)



$$|\phi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

Thus we need only one real parameter θ, (the angle to define the state here on this circle)

A REAL QUBIT IS DEFINED BY TWO REAL PARAMETERS, OR EVEN BY TWO COMPLEX NUMBERS

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}i(|1\rangle)$$

A perfectly valid qubit which doesn't correspond to any point on this circle

↳ Counter clockwise Rotation that passes all points on this circle.

→ If we are able to define this kind of qubit without complex numbers, we will be able to run those algorithms which show a exponential speed up over classical computers

BENIFIT? A Classical bit can store one of two values.
A Quantumbit (Qubit) can store one of infinite many values.

- The circle based Qubit could be implemented using a pendulum.
- It turns out that this infinity of states is just not enough.
- There are other demands that the mathematical model of Quantum computing has placed for us.

NEXT IN THE ROW → TRUE RANDOMNESS

TRUE RANDOMNESS

Everyone can think of himself as a perfect randomness generator we just need a fair coin [H=0, T=1]

This is not truly Random.

because:

in classical mechanics, all you need to do is to measure the initial parameters of them with sufficient accuracy to predict the outcome.

- Even if we donot know the initial parameters, the system knows them. (By system we mean everything which can alter the throw, like the coin itself, your hand, air, temperature, pressure, etc).

→ Even if the result for you looks random, it is not really random for the universe.

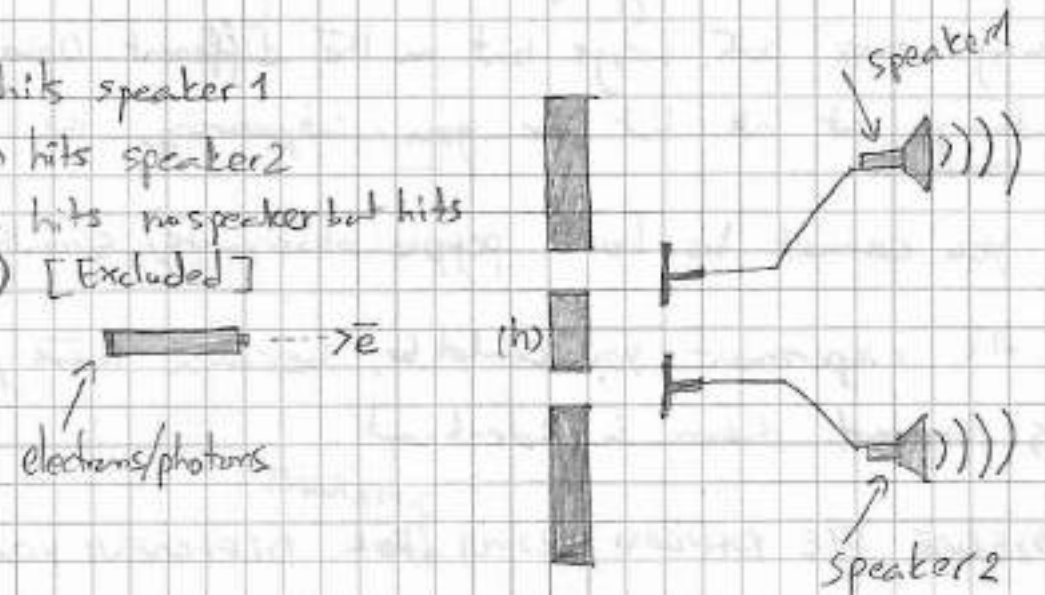
→ For quantum computers we need such randomness that principally cannot be predicted.

Theoretical physicists Agree that There is a such a thing as TRUE RANDOMNESS (Thomas Young, British)

TO DEMONSTRATE, WE WILL SEE YOUNG'S DOUBLE SLIT EXPERIMENT

OUTCOMES

1. electron hits speaker 1
2. electron hits speaker 2
3. electron hits no speaker but hits barrier (b) [Excluded]



Physicist tell us that this set is a source of true randomness because: to measure the outcome, we need to determine the initial conditions, which are.

① Position of the electron
② Momentum of the electron
→ At the start of electron's journey

According to Heisenberg's uncertainty principle

- If we know the position. (there is uncertainty about momentum)
- if we know the momentum (there is uncertainty about pos)

⇒ it is not because of method is not perfect. it is because the momentum of electron is not well defined

- ~~Instead~~ Consider identical parallel universes in which we perform the same experiment. ~~In one~~ There are identical you's in both universes standing at the side of detectors. In one universe electron takes the top way, and bottom ~~at~~ by the other universe. You will not be the same after end of the experiment since you'll disagree about the out come.

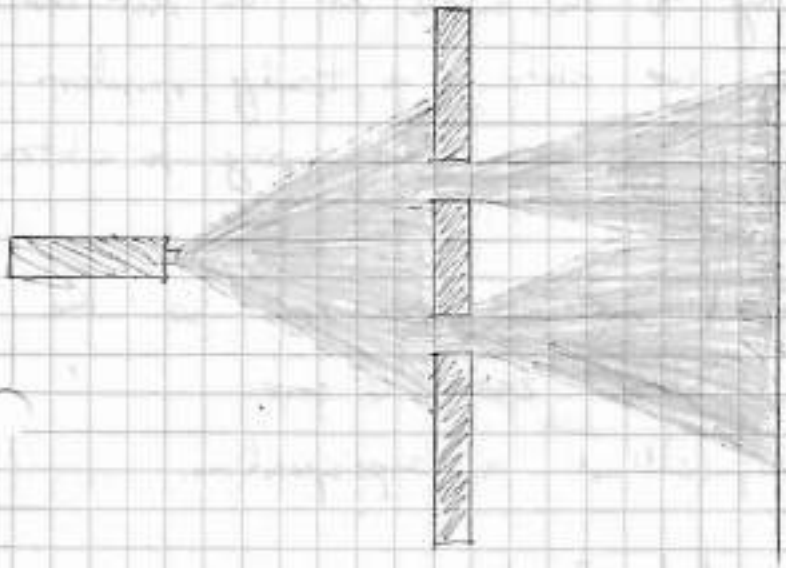
Instead the notion of Randomness, we use these
The electron does not Randomly choose its way.
" It always take both ways but in the different Universes"
There's no randomness at all but for you, subjectively, the result appears to be random.

↳ Because you cannot be both pepple (observants) simultaneously

↳ Before the experiment you could be, because these person and everything around them is identical

YOU OBSERVE THE RANDOM RESULT FOR DIFFERENT (DIFFERENT) YOU!

- In Quantum Mechanics, there is no such thing as a trajectory of an electron.
- We can however fix the departure & arrival points and as almost as if nothing happens in between.



- it appears as if almost at any point, it could principally be detected, though with different probabilities
- Closer to the straight line, we have bigger probabilities of detection, while far from it, we have very small but not zero probabilities of detection.

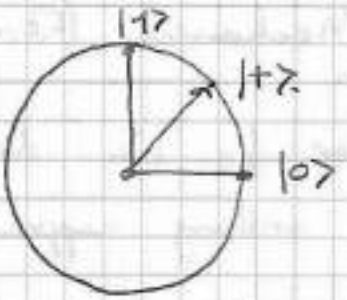
- These probabilities are true probabilities. it is not some lack of information.
- The results of electon detection cannot principally be predicted.
- You can only expect to detect it at some areas with ~~slightly~~ higher probabilities but you can never be completely sure.

~~The electron~~

- Its really like that electon takes all these paths & the physicists say that the measurements somehow destroy all other paths to you. (subjectively)
- Every-thing in this universe is represented with many identical copies. (While these copies are identical, there is no interest in them) When they stop being identical, we can subjectively perceive only one type of them (the copies of ourselves (observers) stop being identical either. and we perceive this change as a random event (THE TRULY RANDOM EVENT)

MAIN POINT If there is a process which is truly Random, then you can probably extract some use of it to create a more effective computation.

TRUE RANDOMNESS



Now how this true randomness is used in Mathematical models.

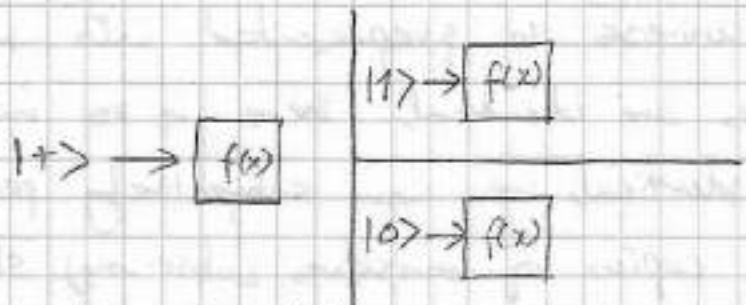
- If we have this Qubit thing in the state $|+\rangle$, and we try to measure it in our ordinary bases like $|0\rangle$ and $|1\rangle$, then we obtain a truly random result. With the probability (0.5) we are going to obtain 1, and with (0.5) 0.

→ Now we know that the qubit in a state $|+\rangle$ is the qubit being simultaneously in state zero & one.

→ This is why this state is called a superposition.

[Does not work with pendulum]

Imagine Some Function that takes one bit as an input and if we pass the qubit, in a state $|+\rangle$, to this function. We will make the function to compute its values on both inputs (0 and 1 simultaneously) thus doubling our computing power.



Source of Quantum Parallelism

Qubit not just can store many different possible values
It can have two values simultaneously

$2^{\text{Num of qubits}} = X$. values could be stored simultaneously

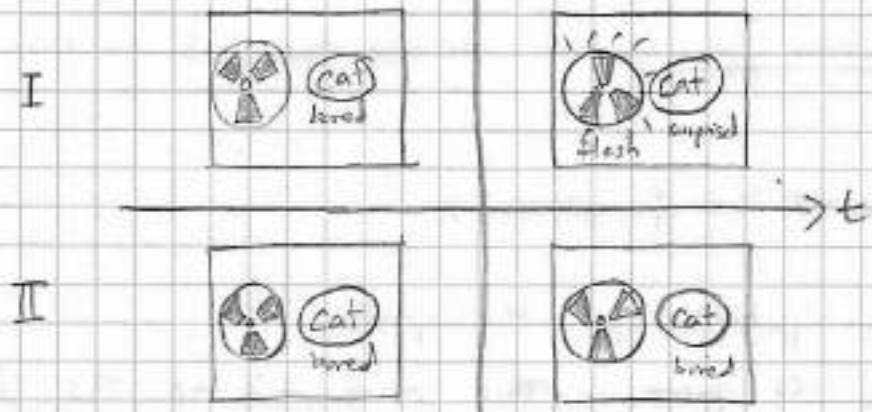
How Do we implement it:

All we need is a source of true source of randomness.

- In 21st century we have those sources of true randomness.
- We can arrange experiments with small particles and obtain those results. The systems measuring those results will split their behavior.

An alternate version of "Schrödinger's cat" [thought experiment]

Bored vs Surprised Cat

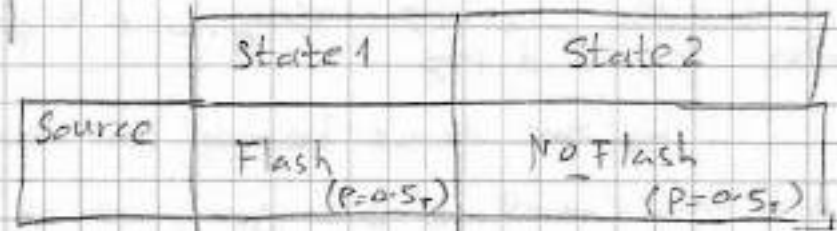


[Imagine the radio active material produces a flash with true probability $\frac{1}{2}$]

The problem now is to collect the results of this computation

because if you open the box, our state will split and instead of superposition we will observe randomly one of these two ~~states~~ cats

Obtaining the result is probably one of the most difficult part



State of superposition

↓

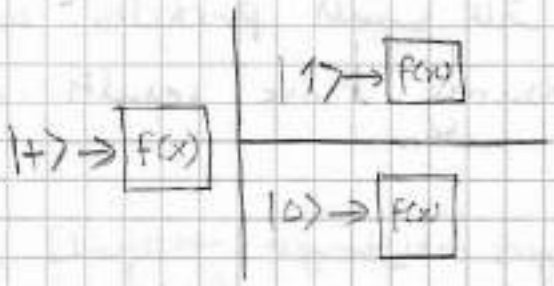
Cat splits to become a superposition of "itself"

Now we have two cats with different states of mind, able to compute twice as before

INTERFERENCE

If some event is truly random, then mathematically we can control & distribute the computation using this event.

1.



- If we have some <u>function f</u>, which takes one bit as an input,
- <u>A device</u> which implements this function f
- This device can take qubits as its input
- Then we can feed the qubit in this state |+⟩ to this device
  Since this plus |+⟩ really is a superposition of these two states |0⟩ and |1⟩
  ↳ our device becomes an observer of the state.
  - Which means → there are going to be two types of these devices
  - One of them observes |0⟩ and acts on |0⟩ qubit
  - Second one observes |1⟩ and acts on |1⟩ qubit

Hence for each of these devices, the value of the qubit |+⟩ that we fed to them seems random.

We had simultaneous computation of both available inputs to function f on just one run.

You can try to observe these two cats, or, two whatever else, but as soon as you do, you observe only one of them as a random event since your identical copies became different. They split on this event

- The other question would be,

I can't observe the second cat since another me observes it, but can I observe that second me observing that cat?
a very hard question

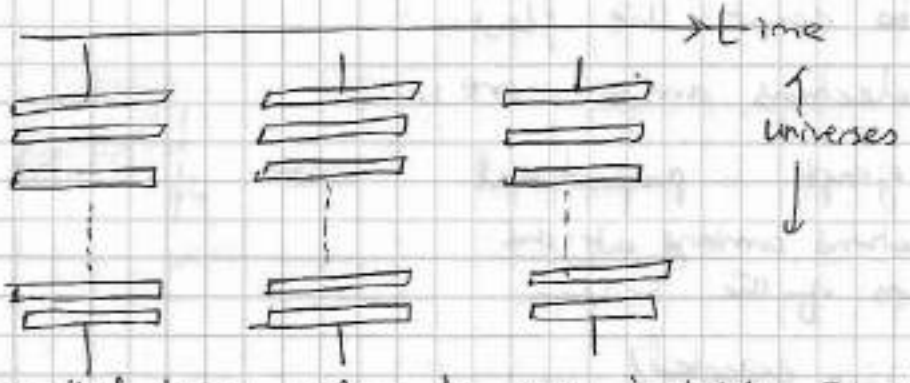
"The concept of the space is immanent to our brain"

-Immanuel Kant

HUGH EVERETT - III

Multiverse - 1957

Some large, large enough stack of infinite universes which are in some sense parallel



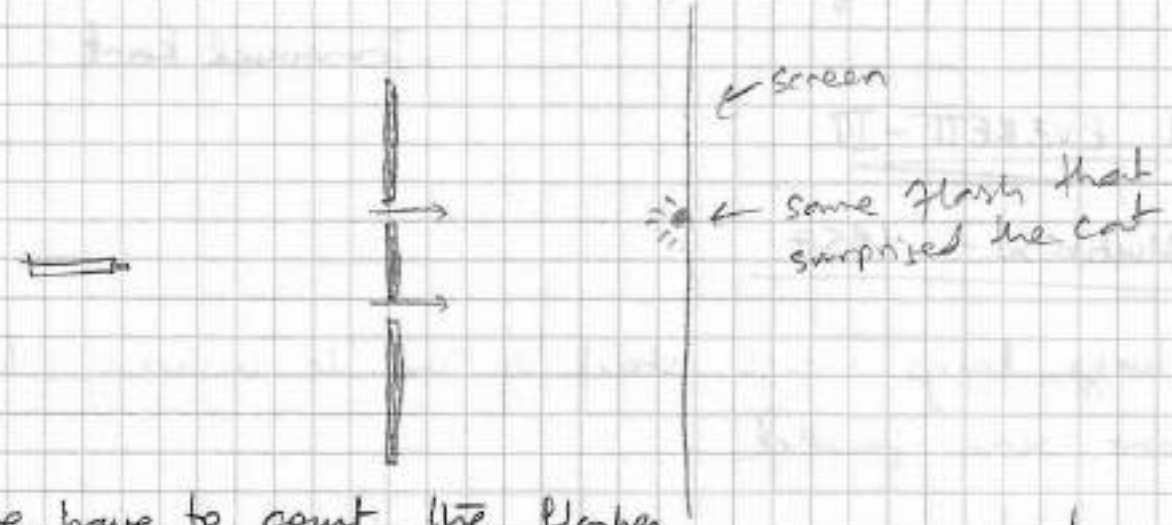
The term parallel here refers to the inability of objects in different universes to interact with each other.

- In the beginning of time all these universes existed as identical
- In time random events occur which divide these universes into different types, depending on the results of these random events.
- When we observe some random event, all our previously identical copies in different universes start to differ and these different copies from now on can act and compute differently.
- We cannot interact with each other since we are in different universes.

As there is a lot of computational power available in this multiverse we are not supposed to be able to use it, since there is no way we could collect the results of this distributed computation, right?

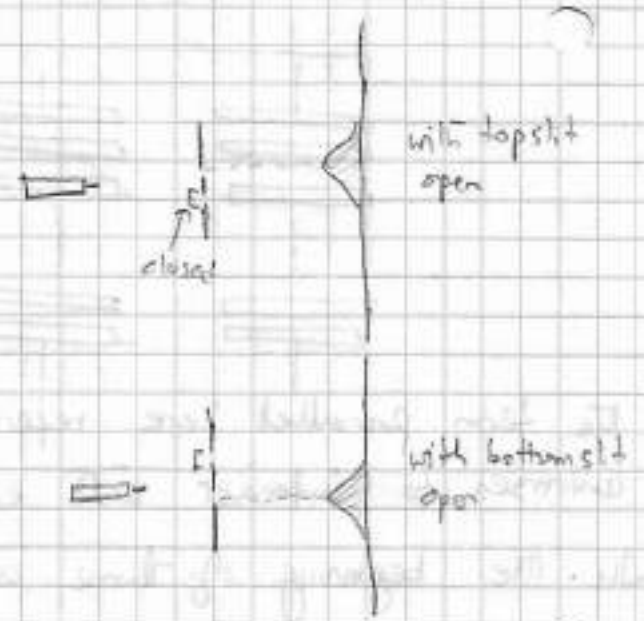
and this is possible through a process, that physicists call interference.

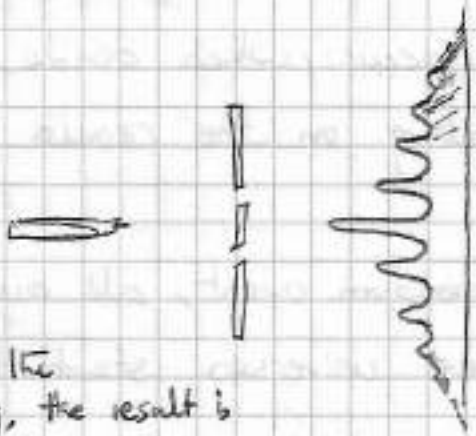
Young's Interferometer



- Now we have to count the flashes to see where electrons arrive more.
- the height of graph is proportional to the # of electrons arriving at the corresponding areas of the screen.

[the result is very expected]
we get more electrons closer to the straight line of opening.]





When we open two slits, the results change dramatically, the result is contrary to the obvious.

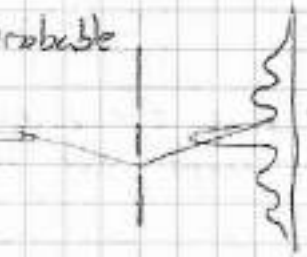
→ previously lightly lit regions are darkened. When we open another slit, suddenly an electron can't go there any more.

CAN WE EXPLAIN WHY?

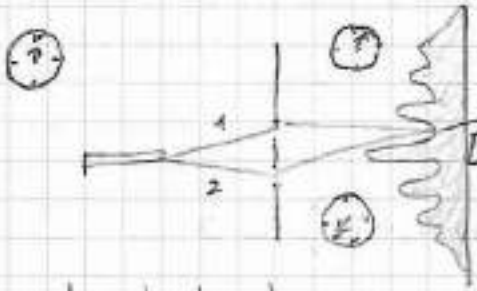
(Next Page)

Well, why? (we can try explaining that)

- When both slits are open, there are two equiprobable opportunities for an electron to reach this detection screen and go to the prohibited point. (it can go through the upper slit or the lower slit)
- Since it is true randomness, we now know that it chooses both these opportunities. But in different universes.



Since everything else in these two universes, except for the electron path, is identical; we can combine these two pictures in one.



- Apparently the state of an electron is not a very straight forward thing [forbidden pt]
- It is defined by many parameters but for now we need only one of them.

- In one of his popular books, he proposed to use this image of a clock

[Feynmann, QED, the strange theory of Light & Matter]

- Imagine, electrons have some clock attached to them and the arrow of the clock rotates very quickly but with the same velocity for all electrons.
- Suppose when electron goes out of the electon gun, the clock in (blue) shows 12'o, clock — now electron(1) travels and when it reaches the [forbidden pt], it shows [1, o, clock] [black clock] — While for lower electron(2) its clock shows [7'o'clock] the (clock in pencil) — the time on their clocks are different because the length of their paths are different

- For some points on the screen, the difference in paths will be so that the clock arrows will point in opposite directions.

[Physicists tell us that these two electrons are in exactly same state]*

$$|A_1\rangle|a_1\rangle + |A_2\rangle|a_2\rangle$$

[* but with different signs]. Since everything in these two universes, except the electrons here is completely identical, we can say that these two universes are exactly in the same state, but they have different signs.

$|a_1\rangle$ ← Small a will denote the state of electon for us
subscript denotes the number of the universe

$|A_1\rangle$ ← Big letter A denotes the state of the entire universe except that electron.

with a little simplification:

$$|A_1\rangle|a_1\rangle + |A_2\rangle|a_2\rangle$$

∵ Since the electron in different universes is exactly the same, except for the sign.

(the whole state could be re-written as)

$$\Leftrightarrow |A\rangle(|a_1\rangle - |a_1\rangle) \quad \because |A_1\rangle = |A_2\rangle = |A\rangle$$

$$\because |a_2\rangle = -|a_1\rangle$$

this is how superposition works

- we can add up the states from different universes.

and mathematically, $|A\rangle(|a_1\rangle - |a_1\rangle) = 0$

~~they assume~~ this sum equals to zero.

WHAT DOES THIS ZERO MEAN TO US?

This means that there is no universe that corresponds to this superposition.

And on the physical level:

There is no universe where an electron arrive to this "prohibited area", and for the points of the screen where electron from different slits arrived with arrows close to each other, the result of this addition is not zero (the superposition becomes meaningful): it can be observed.

The closer the arrows are, the higher the probability to observe the electron in that area.

Why are we interested in this addition? That's how are write the superposition of the states (different)

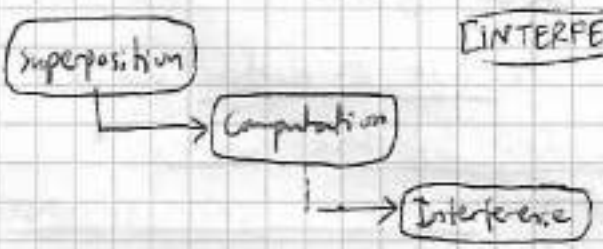
Well, because this addition is really the kind of interaction b/w these different universes. and it's called **interference**

Apparently, this is the only interaction b/w these universes: and through this interaction we can extract something from our distributed computation.

INTERFERENCE

If you manage to run different paths of computation, in different universes and make them to interfere, then we will be able to collect some information, about the result from all these branches.

This is why



THIS IS WHAT QUANTUM COMPUTING IS ABOUT

First, we split the paths,
then we do something interesting in between,
and then, we make the paths to interfere,
to read the result.

SIMPLE ! Can we implement it???

- theoretically, yes we can.
- but in practice, there is a problem.

$$|A_1\rangle = |A_2\rangle = |A\rangle \quad \text{(i)}$$

$$|a_2\rangle = -|a_1\rangle \quad \text{(ii)}$$

- Imagine we are going to have a type of self-destructing interference.
- to obtain a zero, we really need both these conditions to be fulfilled (i) & (ii)

'a': state of the electron
'A': state of everything but the electron
in the two almost identical universes 1 and 2

- Now imagine, some other random event occurs in the universe before the interference takes place.
- In this case $|A_1\rangle$ wouldn't be equal to $|A_2\rangle$ anymore

$$|A_1\rangle \neq |A_2\rangle \quad \text{(anymore)}$$

- & If the electron somehow interacts with the environment, it will also change $|A_1\rangle$ and $|A_2\rangle$ in different ways.

"WE WILL NOT HAVE OUR ZERO, AND THE INTERFERENCE WILL BE DESTROYED"

TO HAVE THE DESIRED INTERFERENCE

A COMPUTING PROCESS MUST BE

1. Fast (Make it very fast to eliminate the probability of other random event in the environment)
2. Cold (lower the surrounding temperature to lower these probabilities. Cold systems evolve slow, they will have more time before something bad for our interference happens.)
3. Isolated (Isolate our computing system from the environment as well as we can to avoid, again, these interactions and the change in the bigger A's)

Nothing in this list is easy. But the isolation part is the hardest. Even if you manage to isolate the quantum data itself, the qubits themselves are not the computation yet. You need to control & change their states, make them interact with each other, even

This is how the CONTROL GATE NOT works, for example.

- All this control stuff achieved by the equivalents much larger than the control system and ideally, you need to isolate this equipment from the environment as much as possible. because it is the part of the computational process as well.

[Thats why quantum computers are so short lived, so cold & so isolated. , as of now, still not implemented on the industrial scale.

WEEK-2

- Quantum Computing:

Less Formulas - More Understanding

-

This weeks Contents (WEEK-2)

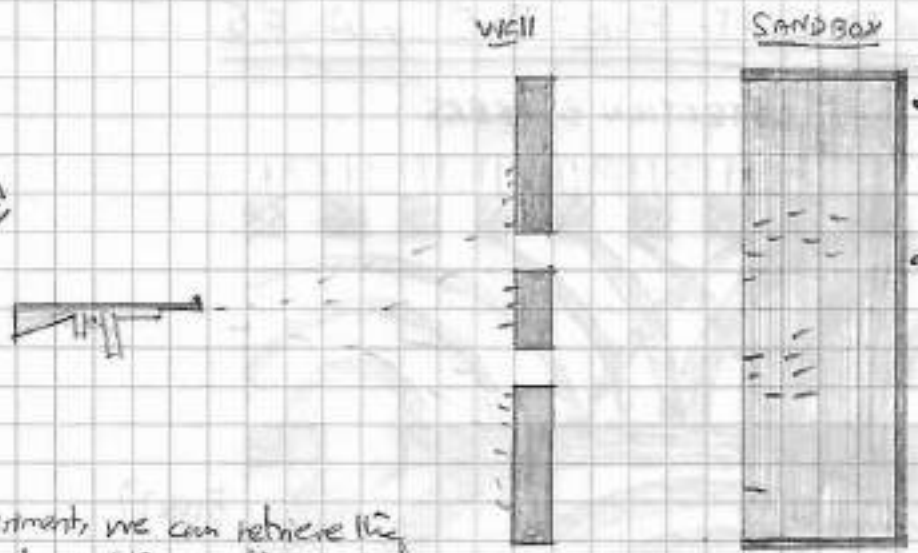
(i) Qubit
(ii) Superposition states
(iii) Complex Numbers
(iv) Measurements & observables
(v) Multiple Qubits
(vi) Entanglement.

DOUBLE-SLIT EXPERIMENT.

BULLETS & WAVES

* The most famous experiment in quantum Mechanics. "The Double Slit experiment"

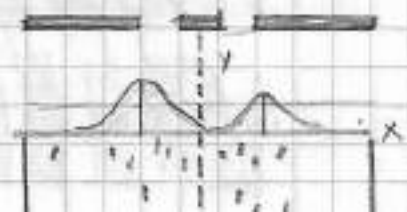
The description follows the description provided by Richard Feynman - LECTURES ON PHYSICS - VOL-III

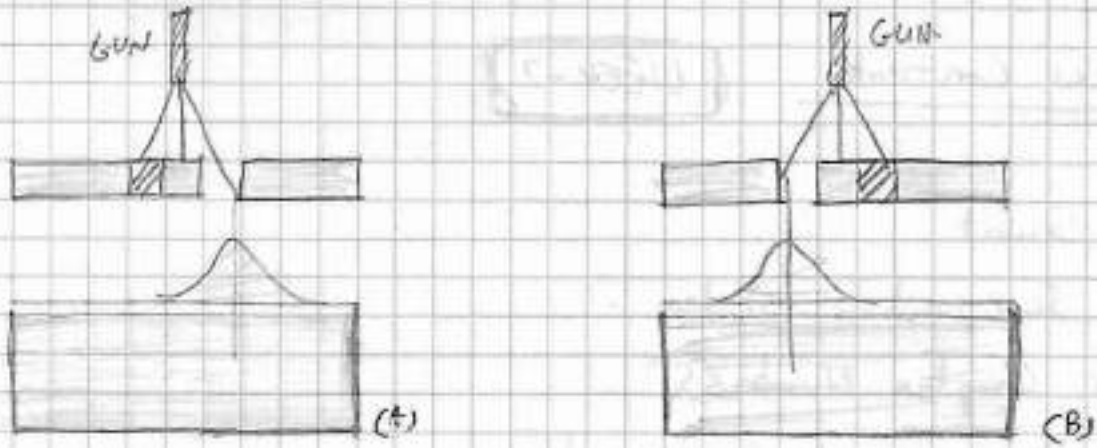


"Imagine a wall with two narrow slits & a sandbox after it."

- The gun is far enough from the wall, the slits are very close to each other. So the bullets that pass through the slits have the equal chance to pass through the top & bottom slits.

Post-experiment, we can retrieve the bullets from the sandbox and can count them and draw a graph.
X-axis, corresponds to the position of the bullets in the box (how far it went from the line of symmetry of the whole set-up). Y-axis will correspond to the # of bullets found in this position (Frequency)





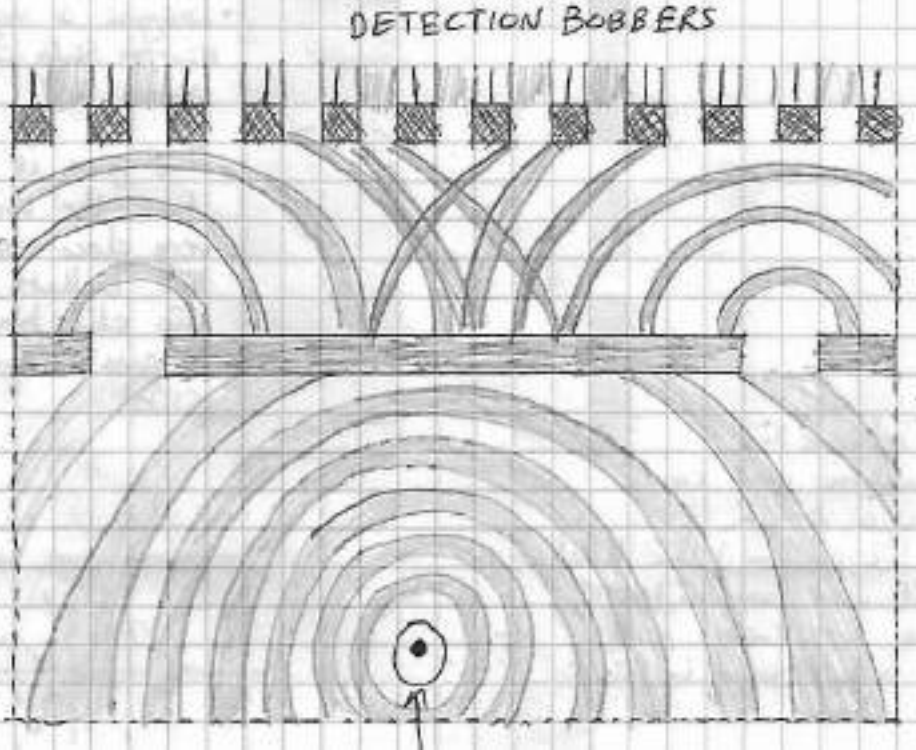
If we do this experiment with one slit open, we obtain a very straight forward result. Most of the bullets go in direction of the open slit. Fewer of them go away from straight line as they bounce off of the edge of the slit.

Question: Can we predict the resulting graph for the experiment with both slits opened, using graphs (A) & (B):

yes, we can. The graph for both slits opened is the sum of the graphs with individual slits opened.

Our reasoning worked well for this case and we were able to give the correct prediction.

DOUBLE-SLIT-EXPERIMENT-FOR-THE WAVES



Fig(2)

Consider Fig(2), on the previous page.

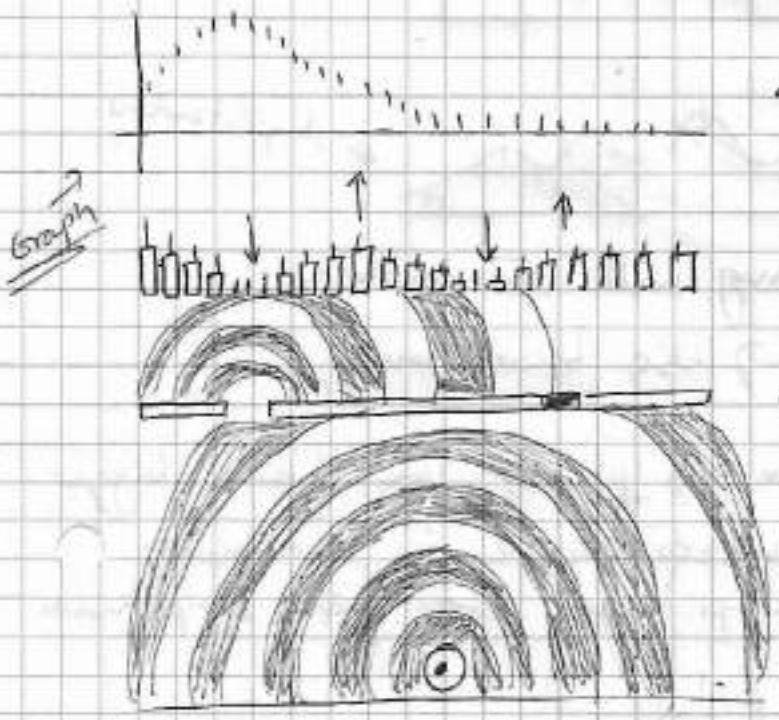
Instead of a machine gun, we have some source of water waves, an oscillating Bobber.

We are going to make this bobber oscillate with some frequency and it will produce waves of same frequency and the are going to reach the screen through the slits, the screen doesn't reflect the waves, any wave that hits the screen is absorbed by it.

The slits in the screen donot absorb the waves and in turn become the secondary source of the waves themselves.

To detect the secondary waves, we are going to place small bobbers at some distance, parallel to the screen.

These bobbers will swing and do some work we will measure that work.
Waves donot transmit matter, but energy.



- the bobbers which are closer to the small wave front meet the small wave circles and the bobbers far away meet the waves with the bigger circles (as the same amount of energy is distributed over the larger wave circle, the swing less.
- Every bobber in this line oscillates and produces work for us.

(1) We measure the energy of each bobber movement per unit of time.
→ Energy/time = power.

(2) Each bobber represents for us, a small share of the wave front. which means that we just not measure the power, but power per unit surface of the wave. (intensity of the wave)

(3) We know from physics that intensity of a wave is proportional to its squared amplitude

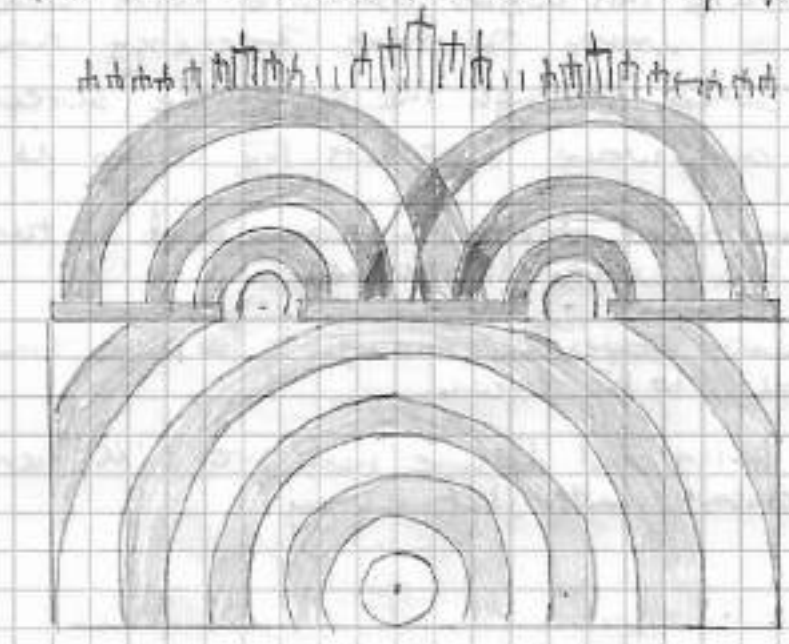
(4) The graph above shows the intensity of the wave measured by each bobber while the bobbers themselves are captured at different positions at ~~different~~ some points in time.

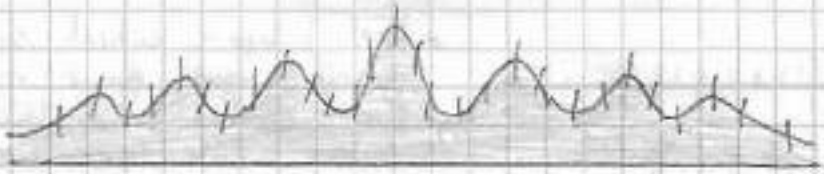
The arrows show that these bobbers oscillate in anti-phase.
Because the bobber 1 is on the wave peak, the bobber 2 finds it self exactly between the wave peaks (at its lowest position)
But the power produced by both bobbers is positive.

Can we again predict the graph with both slits open by using the graphs for individual slits open?
OF COURSE WE CAN ... BUT (!) INTERFERE

Since we understand that now we can build energy out of waves per unit area, and not the number of bullets, we understand that this prediction is going to be a little bit tricky than the previous one.

When we open two slits, the thing we are going to deal with, will be the sum of two waves, with the waves superpositioned.

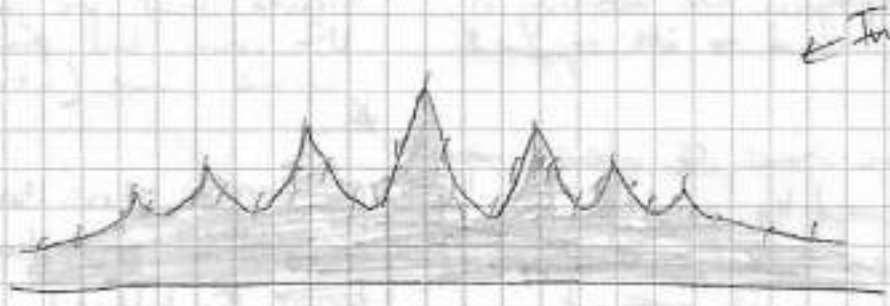




Now we have two waves interacting with the bobbes ...

The resulting wave will be sum of these two waves.

At some point where waves are in phase, we have bigger amplitudes. At points where waves arrive in antiphase we can have much smaller amplitudes. Even zero amplitudes at some points.



The resultant of graphs with both slits opened for the intensity is not the sum of two individual graphs with either slit opened separately.

Double-Slit-Experiment - [PHOTONS & ELECTRONS]

When we do double slit experiment with the waves, there are no particles to be count. so we measure a characteristic of the waves called intensity.

The resultant graph is not at all the sum of graphs that we obtain from either slit opened separately. Therefore. this experiment serves as a good metric when we want to distinguish particles from waves.

PHOTONS

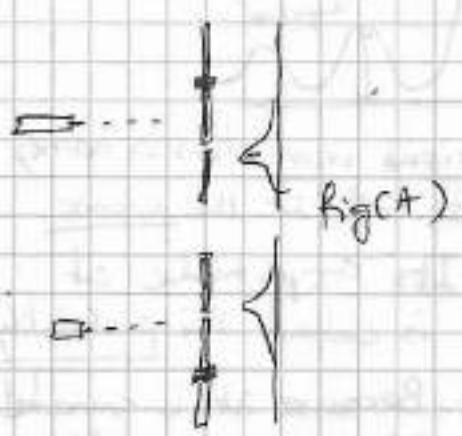
Newton, 1675: Light is particles, but they are weird.

Thomas Young, 1802: Light is waves, Everything is good.

Maxwell, 1865 Light is an EM wave, btw...

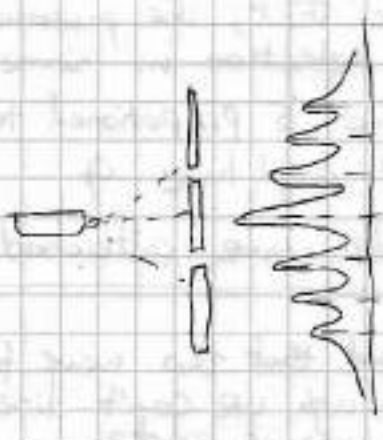
Einstein, 1905: Light is particles, but they are weird.

* Einstein said that its a particle and that particle is an indivisible packet of energy called PHOTON. But the interference pattern it caused in double slit experiment did not disappear. so a new experimental setup was made in which a photo was fired one photon in a minute to the slits Just to make sure that they dinot interact with each other Behind the slits, there was a screen to detect the energy transferred in form of work done per unit area (intensity) and for single slits the results looked like in fig(A) and with both slits opened, they looked like fig(B)



Fig(A)

WITH ONE OPEN SLIT



Fig(B)

WITH BOTH SLITS OPENED

it would be very natural to assume that the resulting graph is same as bullets with both slits opened * BUT NOT

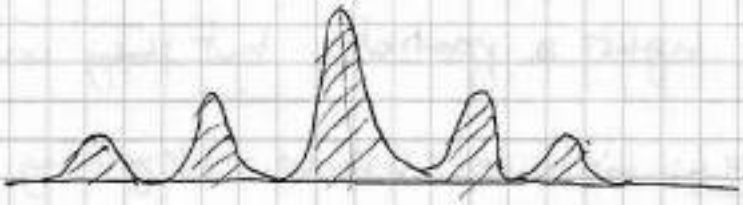
However, the seperate photons act like particles, the overall picture has the wave description even when the photons are fired one/minute so we make sure that they don't interact with each other.

* The interference picture shows us that they are waves. We don't observe them when we watch photons but we must conclude that they somehow exist.

They have parameters like.

(i) amplitude
(ii) Relative phase
(iii) direction of propagation
(iv) frequency etc.

We remember that the intensity of the wave that we observed, has a number of photons at some particular unit area.
If send only one photon in this exp. this [IntensityGraph(A)] has a physical

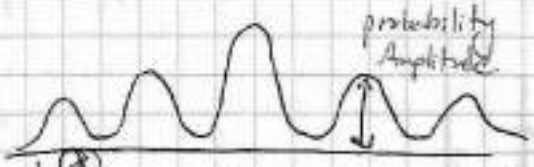


IntensityGraph(A)

* meaning of the probability of getting/catching the photon at some particular area on the screen.
* We just have to divide it by the total # of photons (in the previous experiment) and we obtain the share of photons which arrive at each position. (Intensity)/(total # of photons) = X.
* This share can be considered as the probability for one particular photon to arrive and be detected in this area.

$$(X) \propto (\text{Intensity})_{\text{wave}} \propto (\text{amplitude})^2$$

We can conclude that, the probability of the photon detection in some area of the space is proportional to the squared amplitude of some undetectable wave attached to it.



This mysterious wave has a name, the physicists call it the wave function. Its amplitude at each point is called the probability amplitude. Because it is connected to the probability of a particle detection there. *

Now, we are convinced that this wave function exists somehow, though we can't directly observe it. Where does it exist?
One possible way to look at it is to employ the notion of the "Multiverse". The photon itself exists as a particle but in a bigger picture (multiverse) - which

* Thus the structure of a wave

"Nobody Really understands Quantum Mechanics" - R. Feynman.

LOUIS DE BROGLIE What if we repeat same experiment with electrons. (light always had controversies). But for electrons we always imagined them as small balls. (it even has a radius) But electrons also have interference in the same experimental setting. Turns out that they also have wave functions (waves in the multiverse picture). But these waves have much larger Frequencies and much sharper distributions over the space than that of photons.

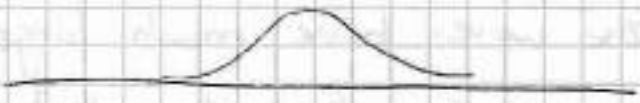
Everything in this universe has a wave function and shows a wave like behaviour.

However, massive particles have sharper peaks in their probability distributions. Which allows us to detect them in certain positions with higher probabilities.

This wave like nature of everything was proposed in 1924 by Louis de Broglie, (French): and is now known as de Broglie Relations, Turns out that describing every particle in terms of its wave function is much more rigorous & informative way of description, than, to just specify its classical parameters, like position & momentum.

WAVE FUNCTIONS

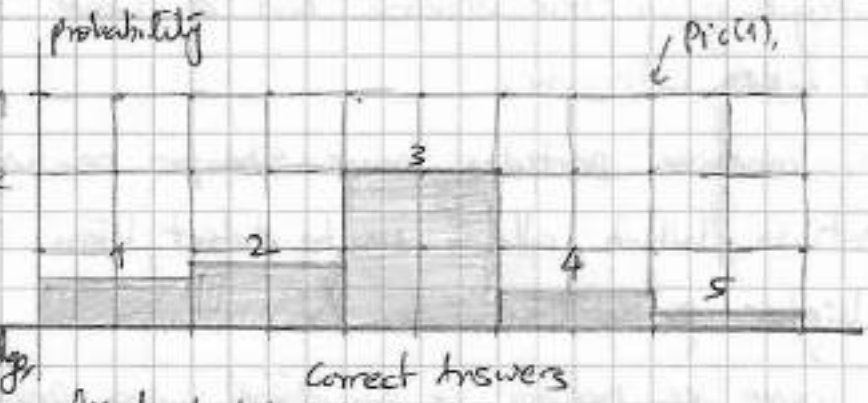
{the vertical axis is the probability distribution of some random value}



Probability distribution

If you have some random value x, it means that we can't predict the exact value of x.

Instead we get some knowledge that which values, x is more likely to take.



- Let's imagine that you have taken some test consisting of 5 questions. You are yet uncertain about your mark for this test.
- This mark will be our random value X in this example.
- Imagine that you try to estimate this value.
- On x-axis, we have all possible results for x_i from (zero) to (five) (Since the test has 5 equal weighted questions)
- You are perfectly sure that at least 1 question, that you've answered, is correct

SD $\boxed{P(X=0) = 0 \quad P(X=1) = 0.1}$ $\boxed{P(X=2) = 0.2 \quad P(X=3) = 0.5}$ $\boxed{P(X=4) = 0.15 \quad P(X=5) = 0.05}$ {distribution of probability for Discrete random value X: $p_i(4)$}

Imp! → $\boxed{\sum_{i=0}^{5} P(X=i) = 1}$

PROBABILITY DENSITY FUNCTION.

Now, what if it has a continuous distribution.
What if it can take any value from some interval. There is an infinity of possible values of [x] in this interval; since there are infinite many real numbers in that interval.

Fig(1)

In this case, we cannot assign a definite probability to these numbers.
[Because, the sum of these probabilities will be infinity, too]
[and we need the total sum of all the probabilities to be 1]

In case of continuous distribution, there is no such thing as the probability of each exact value.

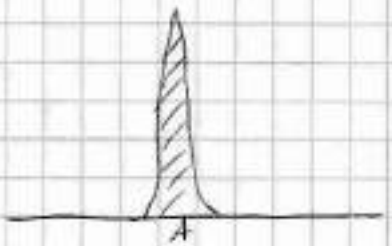
Instead, we can have the probability of x to belong to some subinterval of the whole set of possible values.

& THIS PROBABILITY WILL BE THE AREA UNDER THE GRAPH OF ITS P.D. BOUNDED BY THIS SUB INTERVAL . FIG(1) - P

This Area = Integral of the P.D. on the considered sub-interval
the integral of P.D. over the whole interval must be one

$$1 = \int_{-\infty}^{\infty} f(x)$$

WAVE FUNCTIONS AGAIN

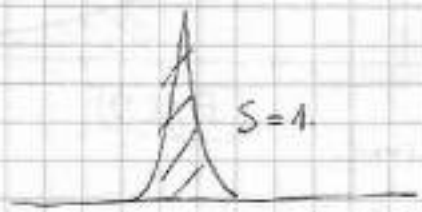


- Both graphs show some probability distributions for a particle to be detected somewhere in space.
- The Graph(i) is zero everywhere except for a very small area around some point A where it has a very sharp peak
- This Graph(i) refers to the situation when we have a good certainty about a particles position. This is what we have, when we study the particles in terms of the Classical Physics.
- In quantum Mechanics, we have this type of description for massive particles. Because massive particles have this type of P.D.
- In classical Physics, we can talk about position of a point-sized particle at any moment.

- For small enough particles like ones we study in Quantum Mechanics the probability dist. looks like Fig(i)

Fig(ii)

- And the particle's position cannot be considered as some point in space anymore.



- The area under the graph, the probability distribution of the particle position, of the whole space must always be equal to 1.
- Physically this means that the particle that we're studying exists and can principally be detected anywhere in space.
- Another thing to recall that the probability of particle detection somewhere is proportional to the wave function ~~and density~~ which is proportional to the squared wave function amplitude intensity
- This all means that the wave function of a particle can't just be any function, the integral of the squared wave function over the whole space must be finite.

  This is why we are going to narrow of domain of consideration to squared integrable functions

SQUARE INTEGRABLE FUNCTIONS

(i) The position of any point in space is defined by the probability distribution, which itself is proportional to the square of the wave function of this particle

(ii) The probability for a particle to be detected in some area is proportional to the integral of its wave function square of this, over this area.

(iii) For a particle to exist somewhere in space, the integral of its wave function square over the whole space must be non zero & finite.

NORMALIZATION

- The integral of this function over the whole space equals to some value A.
- Does this graph represent some probability distribution ??? No. Because integral of the function over this interval must result into A=1.

- If A≠1, there is still a way to make this into correct probability distribution. We can just divide it by A. (the whole)! The resulting function, we'll have integral = 1 which is a correct probability distribution.
- This procedure is called as NORMALIZATION

WHY DO WE NEED NORMALIZATION

Because we want the wave functions to form an infinite dimensional vector space

- Vectorspace (IF) is a set (means it has elements), the elements of this set we're going to call vectors
- The set is called a vector space if

(i) You can multiply any of its elements by a number the resulting element must still belong to this set

LINEAR VECTOR SPACE

IF - linear vector space
A, B ∈ IF, α, β - scalars.

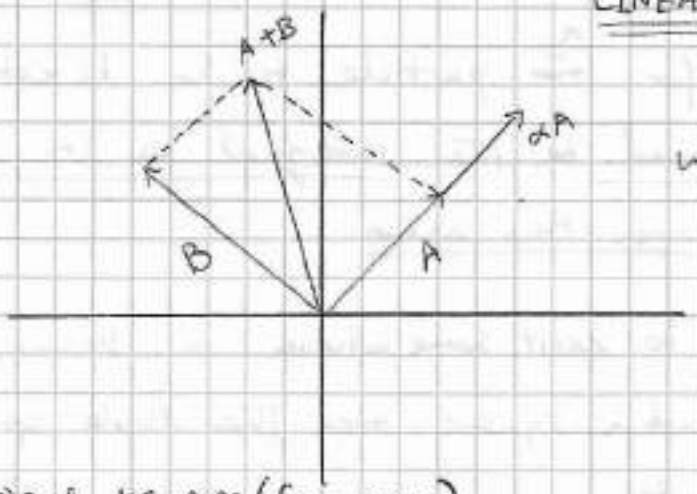
(1.) αA ∈ IF

(2.) A+B ∈ IF

~~These #'s (scalars) / vectors~~ α, β.

- These numbers, of $\mathbb{R}$, we will call the vectorspace to be defined over Real Numbers.
- These numbers if Complex, we will say that this vector space is defined over complex Numbers sets.

LINEAR VECTOR SPACE



The arrows A & B which begin a same initial point, form a vector space over Real #'s

For some non-obvious reason (for now)

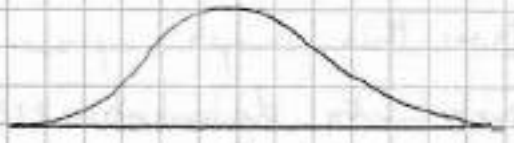
We want to define a vector space $\mathbb{F}$ on the set of wave functions.

to do this we have to define these procedures,

- For example we have some wave function f, Lets assume that its integral over the whole of its square over the wole space is equal to 1. Thus its square integrable.
- and it defines the correct probability distribution.
- Then we can say that this function f can have a physical meaning:
  - it can define position of some particle in quantum mechanical sense.

SQUARE-INTEGRABLE-FUNCTIONS

$$f(x) : \int f^2(x)\,dx < \infty \quad \text{(a)}$$



$$g(x) = a f(x) \quad \text{(b)}$$

$$g^2(x) = a^2 \int f^2(x)\,dx < \infty \quad \text{(ii)}$$

- What happens if we multiply this function with a number (scalar) lets say $a ? \in \mathbb{R}$.
  - ↳ the resulting # still stays square integrable i.e., the integral of its square is still finite —(ii) and this integral will also be multiplied by some number b which is square of the number a. $(b = a^2) \in \mathbb{R}$.
- Now for the resulting distribution to be correct, we have to normalize it. which means, to divide it by $b = a^2$ and after it we obtain exactly the same probability distribution as before, having the same physical meaning.

- After introducing data renormalization procedure for our probability distributions, we obtain the possibility to multiply square integrable functions by scalars.
- All such functions still have a physical meaning for us, since we now know how to obtain the correct probability distribution for any of them.

"FOR ANY ~~state~~ WELL-DEFINED WAVE FUNCTION f. MULTIPLICATION OF IT BY ANY SCALAR, (Except for zero) DOES NOT CHANGE IT'S PHYSICAL MEANING"

for any scalar 'a', f multiplied by 'a' physically represents the same state of the particle.

Vector space of Square-Integrable functions,

$\mathbb{F}$ square-integrable-functions $f, g \in \mathbb{F}$, α - scalar.

1. $(\alpha f)(x) = \alpha f(x) \in \mathbb{F}$
2. $(f+g)(x) = f(x) + g(x) \in \mathbb{F}$

Sum of two square integrable functions, it will just be the usual sum, which means that for functions f & g, the resulting function $f+g$ at some point (x) equals to sum of function values at these points $f(x)$ plus $g(x)$ (Since $f(x)$ and $g(x)$ are square integrable; it is easy to show that their sum defined this way is also square-integrable)

$$\int f^2(x)\,dx < \infty \quad \text{and} \quad \int g^2(x)\,dx < \infty.$$

$$\int (f(x)+g(x))^2\,dx < \int f^2(x)\,dx + \int g^2(x)\,dx + 2\int f(x)g(x)\,dx \quad \text{— (i)}$$

if $\int f(x)f(x)\,dx = \int f^2(x)\,dx < \infty$

and $\int g(x)g(x)\,dx = \int g^2(x)\,dx < \infty$

By Schwarz inequality $\Rightarrow \int f(x)g(x)\,dx < \infty$, $\int g(x)f(x)\,dx < \infty$

so RHS of (i) $< \infty$.

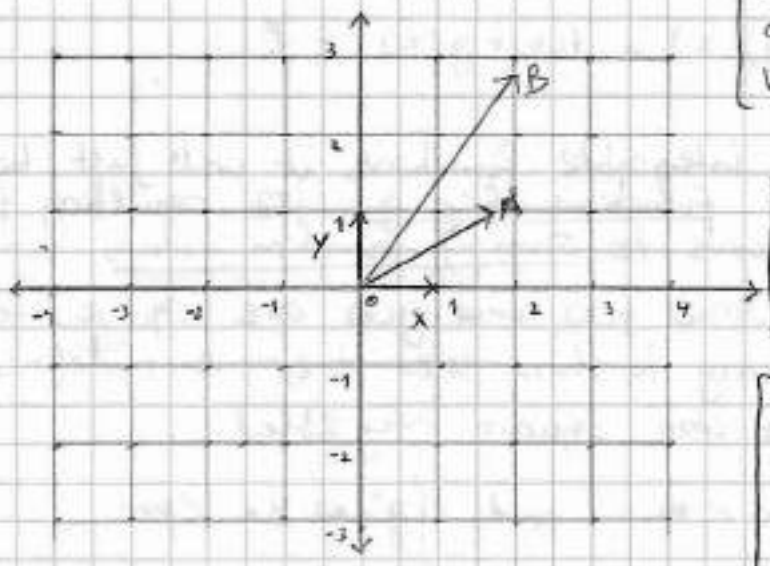
$$\Rightarrow \int (f(x)+g(x))^2\,dx < \infty \quad \text{(square integrable)}$$

- We have now constructed the vector space of the wave functions.
- In any vector space, you can choose a basis, "basis is the set of vectors (usually they are the elements of the considered vectorspace) which generate the whole space i.e., any vector from this vector space can be represented as weighted sum (LinearCombination) of the basis vectors (elements)

There are infinite # of basis that you can choose from a vector space, but they share one very important parameter.

"They will have same number of elements".

the number of elements of the vector space basis (set) is called DIMENSIONALITY of the space.



[Blue Arrows form a basis of this vector space]

[Black arrows form the orthonormal basis of the vector space]

[because the length of each basis vector is = 1. and they are perpendicular to each other]

Blue = {A, B} — Basis

Black = {X, Y} ∧ ||X|| = ||Y|| = 1 ∧ X ⊥ Y (orthonormal Basis)

|Blue| = |Black| = 2 = Dimensionality of the vector space

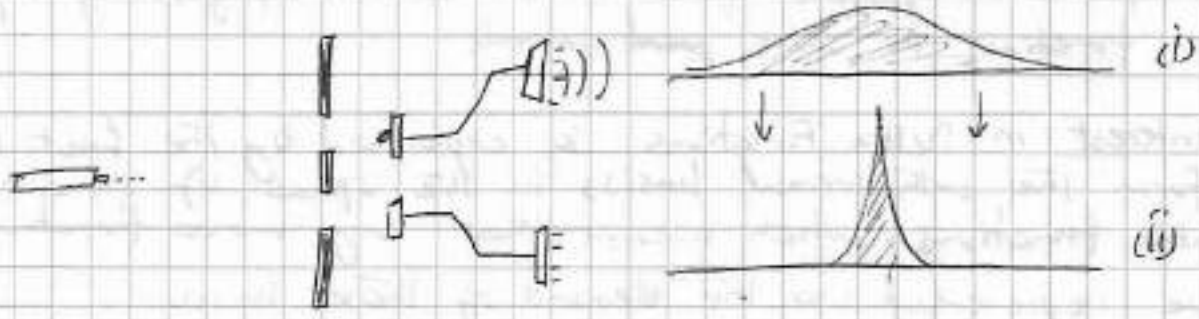
Dimensionality of the plane.

Orthonormal Basis play an important role in quantum mechanics

What is dimensionality of vector space of square-integrable functions?

It is well known from mathematical Analysis that # of dimensions for this space can infinite. Which means that any basis that we'll choose will have infinite # of elements.

MEASUREMENT OF WAVE FUNCTIONS



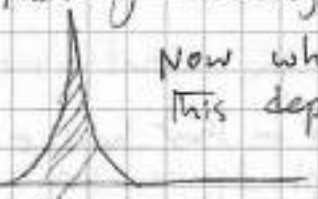
- There is a source of photons to the left. We have photo detectors after each slit.
- When we fire the photon, we don't know which photo detector is going to be hit because the photon position is not an exact point in space. But it is a wave function square of which determines its probability distribution
- After the photon hits the detector, the position of the photon becomes well-known. It is exactly where the position of the detector situates.
- In terms of wave functions. The (i) becomes somewhat like (ii) which has one sharp narrow peak

Physicists call this process "The Wave Function" collapse

Because this beautiful & mysterious thing from above (i) becomes something usual and boring at first sight as (ii)

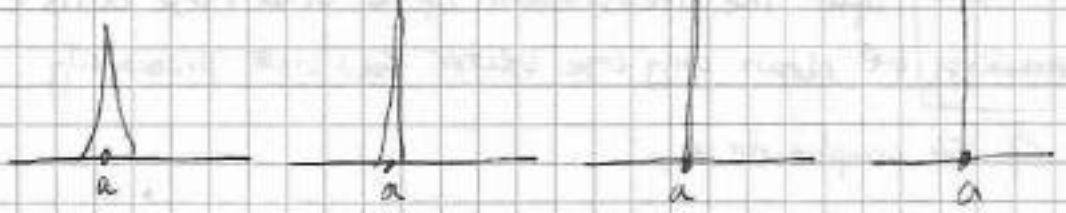
- We know from previous pages that this process doesn't destroy the initial wave function. The "measurement" doesn't alter the wave function; it alters the state of the observer.

→ Making us subjectively observe only this small part of the whole picture.



Now what is this sharp spike anyway? is it a wave function? This depends on how sharp it is.

In practice, no one can measure the exact point in space with zero error. Even if we have a small width of this peak here, we can still call it a wave function, because we can calculate the integral of its square and we can see that its finite

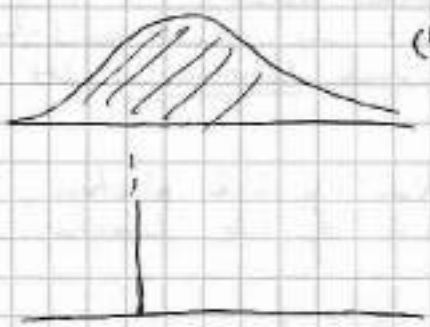


$\delta(x-a)$ — (iii)

But mathematically, we are interested in some limit situation where this peak narrows upto zero, and giving us (hence) the exact point in space. While getting higher & higher, at infinity. This (iii) limit thing is called [Dirac Delta Function]

Dirac's Delta function is not a function in its usual sense, of course it's not a square integrable function & since this thing is not a square integrable function, it does not physically represent a wave function of some ~~point~~ particle.

- Our interest in Delta Functions is explained by the fact that they form the orthonormal basis, in the space of squared integrable functions, which means that any wave function f can be represented via the elements of these basis
- Well these delta functions don't even belong to the vector space of our square integrable functions, (but still they form the basis there)



(upper)

- our upper wave function f is somehow represented in the basis of the Delta functions.
- And after the measurement in an idealized case where we obtain the exact point in space, the wave function becomes for us the delta function.
- So the initial representation with the infinite number of delta functions, collapses to just one basis element

- That's what measurement does from the quantum mechanic point of view.
- it always transforms the wave function decomposition in some basis, into just one vector of these basis & This vector is chosen randomly according to the distribution defined by the initial decomposition

EXAMPLE (SIMPLER) WITH FINITE BASIS

$$E = \{e_i\}_{i=1}^{n}$$

$$\vec{x} = \sum_{i=1}^{n} x_i e_i \xrightarrow{\text{measurement}} e_a$$

x_i: [probability Amplitudes]

- the letter "e" denotes the vectors of some orthonormal basis
- The letter "$\vec{x}$" denotes the initial wave function
- ← Wave function decomposition in that basis e
- ← Small letter "x" with subscript denotes the coefficients of this decomposition. (we can call them the probability amplitudes)

after the measurement of x and these basis e_i we obtain only one vector e_a, with probability

$$P(e_a) = x_a^2$$ ← probability

defined by the square of the amplitude x_a

Now, let's take a look at this expression.

$$x = \sum_{i=1}^{n} x_i e_i \longrightarrow e_a$$

$$f(x) = \int_{-\infty}^{\infty} f(a)\,\delta(x-a)\,da$$

[it represents the decomposition of the initial wave function and the basis of the delta functions]

(Lebesgue Integral)

[Named after the french mathematician Henri Lebesgue who invented a way of integrating such things as this]

- Instead of basis e_i we now have infinite basis (continuous) of delta functions.
- Instead the sum over the set of vectors, we must write an integral since our basis are now continuous.
- Instead of x_a ; you write here $f(a)$ which is a coefficient in this decomposition.

after the measurements in the basis of delta functions, we obtain one delta function

$$X = \sum_{i=1}^{n} x_i e_i \longrightarrow e_a$$

$$f(x) = \int_{-\infty}^{\infty} f(a)\,\delta(x-a)\,da \longrightarrow \delta(x-a)$$

with probability defined by the distribution f of (x) squared

SUMMARY

(i) Wave functions can be measured

(ii) the measurement procedure can randomly give us different results.

(iii) the whole set of results form the orthonormed basis in the space of wave functions. [Most important point]

we can measure different things about a particle we can measure its position in space, its momentum, its polarization, its energy level etc... (orthonormal basis are in some vector space where we

But before any such measurement, the set of all possible outcomes form

(iv) After the measurement, the wave function collapses, subjectively for us into one of these basis states.

The probability for the basis vector to be chosen by the measurement procedure is defined by square of the coefficient for this basis vector in the initial decomposition

- This set of possible outcomes which form the basis in the wave function vector space and defines the characteristics of our measurement procedure. (physicists call an <u>observable</u>)

More precisely, it defines, what physicists call an "observable"

WEEK-3

QUANTUM COMPUTING -

LESS FORMULAE. MORE UNDERSTANDING

WEEK THREE

→ Observables are denoted with R or Q

The letters R & Q come from Lagrangian Mechanics where 'q' denotes generalized coordinates of a system
'p' denotes generalized momentum of a system.

P – Observable for momentum of a particle in Quantum Mechanics

- Entangled States

TWO STATE SYSTEMS

The State Space :–

- Quantum Mechanical description of a particle is referred to as its state (instead of its wave function)
- State (An abstraction to make the picture of world more simple for us)
- Wave Functions form a linear vector space. The functions in that space are square integrable functions.
  – As soon as we know that some objects form a vector space, we can use with them all instruments that Linear Algebra gives us for this.

← Linear Algebra Notation

$$E = \{e_i\}_{i=1}^{N} \leftarrow \text{Basis.}$$

$$\vec{x} = \sum_{i=1}^{N} x_i \vec{e}_i \leftarrow \text{Basis vectors}$$

$\vec{x}$ ↑ wave function; x_i ↑ probability Amplitudes

- Finite dimensional space : dim = N
- Basis consists of N vectors.
- The sum of wave function decomposition in this basis has N elements.
- Each element of this sum is a basis vector X with a coefficient, which we call it's amplitude.

Lets consider a special state which consist of columns of N digits

$$e_1=\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix},\quad e_2=\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix},\quad e_3=\begin{pmatrix}0\\0\\1\\\vdots\\0\end{pmatrix},\quad \dots,\quad e_{N-1}=\begin{pmatrix}0\\0\\0\\\vdots\\1\\0\end{pmatrix},\quad e_N=\begin{pmatrix}0\\0\\0\\\vdots\\0\\1\end{pmatrix}$$

We will call them vector columns.

"each element of the basis: lets say m^{th} is its m^{th} column vector with all places holding a zero except for the m^{th} place which holds a 1"

Since its a vector space, so we are defining two operations with them.

i) Multiplication of a vector with a scalar.

ii) Addition of two vectors.

$$\alpha\begin{pmatrix}x_1\\x_2\\\vdots\\x_N\end{pmatrix}=\begin{pmatrix}\alpha x_1\\\alpha x_2\\\vdots\\\alpha x_N\end{pmatrix}\qquad \text{AND}\qquad \begin{pmatrix}x_1\\x_2\\\vdots\\x_N\end{pmatrix}+\begin{pmatrix}y_1\\y_2\\\vdots\\y_N\end{pmatrix}=\begin{pmatrix}x_1+y_1\\x_1+y_2\\\\x_N+y_N\end{pmatrix}$$

Having all this, we can now determine, which column vector corresponds to our initial wave function, (through its decomposition) to the basis "e")

$$\vec{x}=\sum_{i=1}^{N}x_i\vec{e}_i=\begin{pmatrix}x_1\\0\\0\\\vdots\\0\end{pmatrix}+\begin{pmatrix}0\\x_2\\\vdots\\0\end{pmatrix}+\dots+\begin{pmatrix}0\\0\\\vdots\\x_{N-1}\\0\end{pmatrix}+\begin{pmatrix}0\\0\\\vdots\\0\\x_N\end{pmatrix}$$

- First we multiply each column vector by its amplitude from our decomposition.
- Second, we add all these columns to obtain just one column.

$$\vec{x}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_{N-1}\\x_N\end{pmatrix}$$

- x's are our amplitudes

This thing is known as isomorphism in Mathematics

For vector space of wave functions we have built an isomorphic vector space. (our wave function is represented by a column vector of vector columns)

- This space we just built, we will call the state space of the system. and its columns' (elements), we will call states.

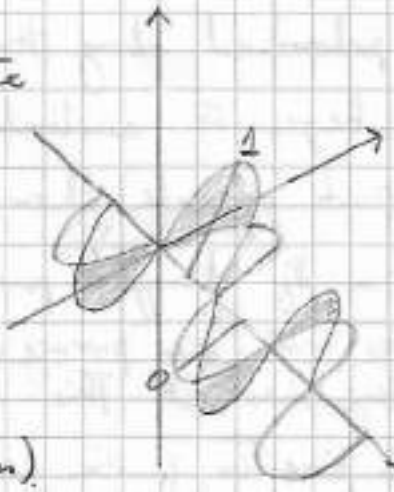
- It is more convenient to work with the state space of the system than the wave function
  - we have a notation for it (Dirac's Notation) (week 4)
  - There are characteristics of a particle that we cannot describe in terms of its wave function (but we can do it in terms of column vectors)

- This could also be done for infinite dimensional state. in that case, the columns will have a beginning but no end.

TWO STATE SYSTEMS — POLARIZATION OF PHOTONS

Light Polarization

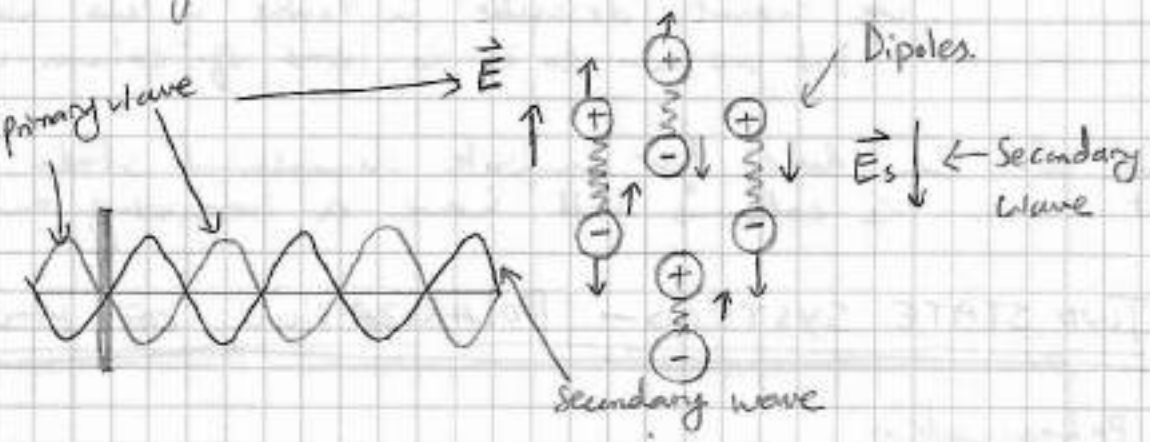
The wave theory of light describes the light waves as transverse waves. (Direction of wave oscillating is perpendicular to the direction of wave propagation. This direction of wave oscillation is called wave polarization)



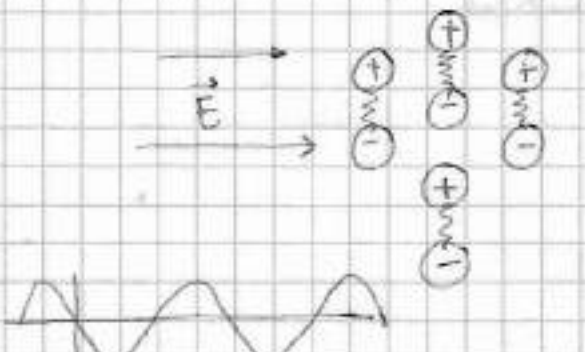
When light is coming from a source, there are many different waves polarized in different directions. The whole flow in this case does not have their preferred direction of oscillations.
"Which means that the light is not polarized."
When we have light which was reflected from some object (eg water) which partly polarizes it, then the majority of waves will have the same direction of polarization the light will become polarized. because it will have the same direction of oscillations

Linear Polarizer

Linear polarizer, it is made of a thin slice of crystal with a peculiar organization of the molecular level. Molecules of this crystal form dipoles, with alignment along same axis or direction.



- When light polarized along this axis falls at the crystal, the dipoles begin to oscillate. Because light is an EM wave. & it can push opposite charges to opposite directions.
- This oscillation of charged particles produces a secondary wave. which interferes with the primary wave on the other side of the crystal & extinguishes it. This secondary wave goes in both directions First to the direction of the crystals where both waves interfere to nothing and second, it the opposite direction. (to the side where the primary wave came from. (This second wave going in opposite direction is perceived by us as the reflected wave. This reflected wave is polarized in the same direction as the primary wave. which is this direction of orientation of the dipoles in the crystal.
- Now if the primary wave is polarized orthogonally to direction of axis of dipoles orientation, and doesn't produce any oscillations of the dipoles, thus there is no secondary wave & no reflection.*



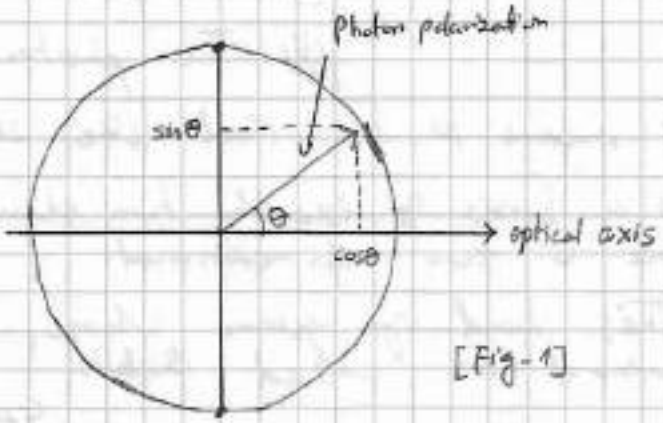
* the wave easily just goes through the crystal
- This direction ~~~~ arises orthogonal to the line along which all dipoles are oriented — is called the optical axis of the crystal. the light polarized along this optical axis, easily passes through the crystal + the light polarized orthogonally to

This is actually how transparency and reflection work.

Materials that have something to oscillate on the frequency of the following electromagnetic waves are more likely to produce secondary waves. Which will extinguish the waves after the material and form the reflected waves.

"Now imagine, the primary wave of incidence is neither in the direction of optical axis nor orthogonal to it" (it's somewhere in between)

Also, let's imagine that this wave is represented by only one photon.



[Fig-1]

If it's just one photon, it cannot partly pass and partly reflect, it must either partly pass or partly reflect because it's just one photon and it cannot be divided in parts.

It comes as no surprise that this photon passes the crystal with probability P and is reflected with probability R.

$P = \cos^2(\theta)$
$R = \sin^2(\theta)$
} This result is truly random.

Reflection:

- The photon will have its polarization orthogonal to the optical axis.

Passing:

- The photon will have the polarization collinear to the optical axis.

Hence, the interaction with the crystal, alters the photon polarization.

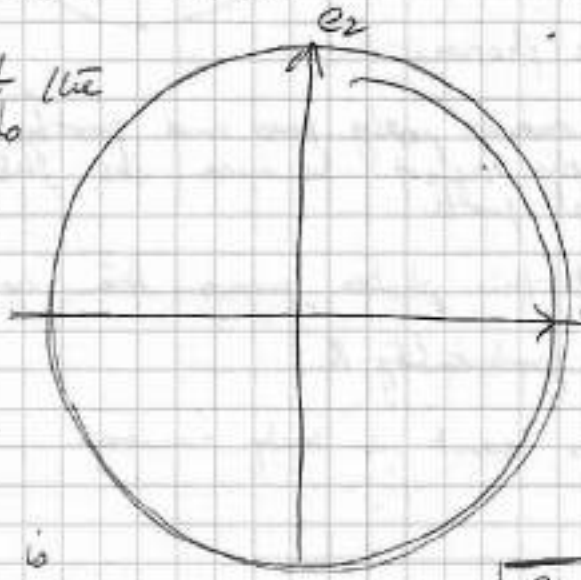
- Attaching two polarizers, such as their axis are collinear, the photon coming from the first polarizer passes through the second one too since their optical axis are collinear, if we rotate them such that their optical axes are orthogonal, the incident photons reflect and as if no light passes through (The important thing to notice here is that we have a measurement process with exactly two possible random outcomes)

- The whole set of possible measure outcomes forms, the basis in the state space.

- For the photon polarizer, we only have two possible measured out comes.
  (i) The photon passes through the polarizer (P)
  (ii) The photon reflects through the polarizer (R)

- it means to us that the state space for the photon polarizer has a basis of exactly two elements. (Which means that this state space is two dimensional.

This kind of systems whose state space is exactly two dimensional are called Qubits.



$basis = \{e_1, e_2\}$

- This optical instrument the polarizer, allows us to demonstrate one more important thing.
- Our freedom in choosing the basis, the observable.
- The choice of basis is achieved simply by rotating the polarizer

e_2: basis vector which corresponds to the state of photon with vertical polarization. These photons are ejected from the polarizer with the probability 1.

e_1: basis vector which corresponds to the state of photon with horizontal polarization. These photons pass through the polarizer with prob. 1

All other photons as all other states are represented as a weighted sum of these two basis vectors.

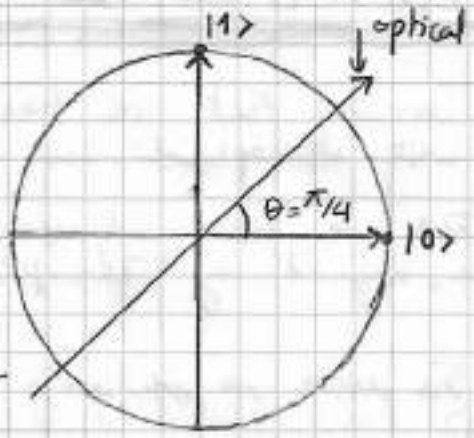
- Let's denote e_1 as $|0\rangle$
- Let's denote e_2 as $|1\rangle$

$|\ \rangle$, these strange brackets are called Dirac's Brackets

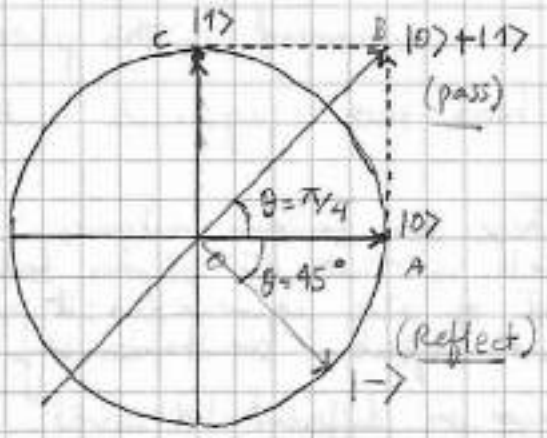
- Dirac's brackets are used to denote vectors in the state-space.

Qubit (HADAMARD BASIS)

- What if we rotate our polarizer by an angle $\pi/4$ radians.
- Now the basis of our measurements are going to be completely different.



- The photons that pass through the polarizer with probability 1 are now neither horizontal nor vertical.
- In terms of previously introduced basis, they will now have state zero plus one.



- Since we remember that zero & one are unit vectors, we want our new basis vector also to be unit.

$$|OB| = |OA| \cos\theta + |OC| \sin\theta.$$

$$|0\rangle + |1\rangle = |0\rangle \frac{1}{\sqrt{2}} + |1\rangle \frac{1}{\sqrt{2}}$$

$$\boxed{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)} \quad \text{(i)} \qquad \| |0\rangle + |1\rangle \| = \sqrt{2}$$

↑ division by square root $\sqrt{2}$ is to Normalize it.

- This new basis that we obtained by rotation of previous basis by 45 degrees is very important in Quantum Computing.

So naturally its vectors also have special names.

(i) — is called {VECTOR PLUS} it corresponds to the photons which pass with probability 1 through this rotated polarizer.

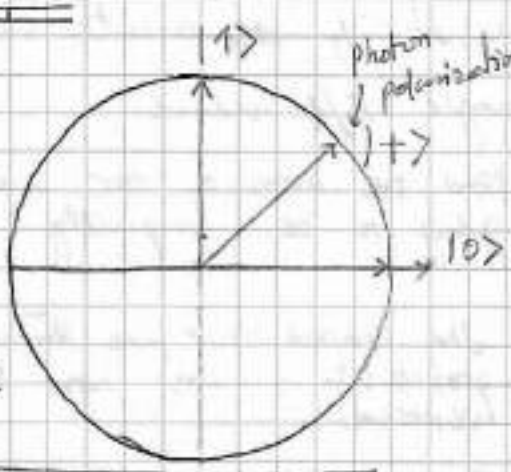
(ii) Those photons which reflect from this rotated polarizer with probability 1 will correspond to the "state minus" defined as follows

$$\boxed{|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)} \quad \text{(ii)}$$

→ These two vectors $|+\rangle$ & $|-\rangle$ also form the basis in the state space and they also define the measurement procedure. But it is a different measurement procedure, since the basis is different.

As we can see in the case of light polarization we can either our measurement process or choose the measurement basis simply by rotation of this linear polarizer. These basis are called "the Hadamard Basis"

WAVES AND COMPLEX NUMBERS. PART I



- Lets assume that we have placed our polarizer with its optical axis parallel to the ground.
  (Thus we have adjusted the measurement procedure, defined by the |0>, |1> basis.

Imagine the photon we are going to measure is in the state |+>

Which is a state right b/w our basis state

For the measurement of this photon in these basis we have two equiprobable outcomes. (First photon passes through the polarizer and obtains horizontal polarization) (P)
(Seemdly, photon reflects through the polarizer and attains vertical polarization) (R)

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

(P): jumps to the state 0.
(R): Reflects, jumps to the state |1>

- These two Random outcomes tell us that the photon takes both of these opportunities; it passes and reflects simultaneously. though in different UNIVERSES.

WE SUBJECTIVELY PERCEIVE ONLY ONE OF THESE OUTCOMES.

- If a photon does both things, we can naturally assume that before the measurement, this photon actually was in these two states simultaneously.

state: |0>: with horizontal polarization.
state: |1>: with vertical polarization

- Now each of these photons from a point of view of the wave theory, of light, is represented as a wave.
- **WAVE = Harmonic Oscillations**

Waves propagate oscillations.

$$\frac{d^2 f}{dt^2} = -\omega^2 f$$

f: parameter which oscillates (could be position of the pendulum or its velocity / intensity of EM field)

ω: Angular Frequency

Solutions: Harmonic Oscillations

$$\frac{d^2 f}{dt^2} = -\omega^2 f$$ linear differential equation ✱

$$(\sin \omega t)'' = (\omega \cos \omega t)' = -\omega^2 \sin \omega t$$

$$(\cos \omega t)'' = (-\omega \sin \omega t)' = -\omega^2 \cos \omega t$$

①

✱ LDE: means that if any two functions satisfy this equation then any weighted sum of f and g also satisfies this equation.

② We differentiate the function two times and we obtain just the same function with minus sign.

From mathematical analysis, if we consider only real valued functions of real variables. we can remember only two functions which satisfy this condition.

- Sine & cosine function
- if we differentiate sine twice, we obtain minus sign.
- if we differentiate cosine twice, we obtain minus cosine.

Sine and cosine are actually the same thing which differ only by the phase. So we can write a basic function which solves the equation: $\boxed{\frac{d^2f}{dt^2} = -\omega^2 f}$

$$f(t) = A\cos(\omega t + \phi)$$

where:

ω = angular ~~velocity~~ frequency $= \frac{2\pi}{T} = 2\pi\nu$

A: amplitude of the oscillations

ϕ: phase of osallations.

t	$f(t) = A\cos\left(\frac{2\pi}{T} + \phi\right)$
0	$f(0) = A\cos(\phi)$
	at $\phi = 0$, ; $f = A$ (the largest value)
	; $\phi = \frac{\pi}{2}$; $f = 0$ (central pos. of oscill.)
	; $\phi = \pi$; $f = -A$ (other extreme)
	; $\phi = \frac{3\pi}{2}$, $f = 0$
	; $\phi = 2\pi$, $f = A$ (re-cycle begins)

period of cosine $= 2\pi$ after $\frac{2\pi}{\omega}$, oscillator will be in the same state

$T = \frac{2\pi}{\omega}$ or $\omega = \frac{2\pi}{T}$

$\frac{1}{\nu}$

So angular freq. is wave frequency ν (Nu) multiplied by 2π

ϕ has the physical meaning of the phase shift which tells us at which part of the cycle, the osallations are at time (0)

- Sine & cosines work for because they are real valued functions. What if we look at the functions whose values can be

complex numbers

Harmonic Oscillations:

Lets take a look at this equation again:

$$\frac{d^2 f}{dt^2} = -\omega^2 f$$

we differentiate f & we get f times some constant. The other function with this property is exponents.

$$(e^{\omega t})'' = ((\omega e^{\omega t})' = \omega^2 e^{\omega t}.$$ } Not good enough since we want to have this minus sign.

How can we obtain a negative number after squaring some thing.

$\Rightarrow$ much easier with complex numbers:

$$(e^{i\omega t})'' = i\omega e^{i\omega t} = i^2 \omega^2 e^{i\omega t} = -\omega^2 e^{i\omega t}.$$

$$\Rightarrow f(t) = A e^{i(\omega t + \phi)}$$

- A: Amplitude
- ϕ: phase
- ω: Angular frequency

Question: This function is a complex valued function, how can we interpret or use it in our real world describing real oscillating.

$$f(t) = A e^{i(\omega t + \phi)} = A\cos(\omega t + \phi) + i A \sin(\omega t + \phi)$$ ← Eulers Formula.

we want to obtain physical meaning of this function.

Now when we consider the physical meaning of it, we keep this real valued cosine and forget about the imaginary part. we get the same expression as before.

$$f(t) = A e^{i(\omega t + \phi)} = A\cos(\omega t + \phi)$$

Why do we have to do it with complex # if we can do it with real valued #'s and the result remains just the same?? #.

Reason: Multiplication of a state by a # doesn't change the state.

$f(t) = A\cos\omega t$	$f(t) = Ae^{i\omega t}$
Real valued	Complex valued
Now let's add phase	
$f(t) = A\cos(\omega t + \phi)$	$f(t) = Ae^{i\omega t}e^{i\phi} = Ae^{i(\omega t + \phi)}$

For real valued function, the phase part goes into cosine.

For the complex valued function, adding phase is just multiplication by a constant, $e^{i\phi}$

And this multiplication does not even change the length of the vector.

So if we consider the state space over the complex numbers instead of the real #'s phase

Waves were not considered so far (only oscillations were discussed)

$A\cos(\omega t + \phi - kz)$ | OR | $Ae^{i(\omega t+\phi-kz)} = Ae^{i\omega t}e^{i\phi}e^{-ikz}$

When we have a function that describes harmonic oscillation we can easily ~~differ~~ find the function which describes a simple plain harmonic wave, wave propagate oscillations in space.

Exploiting harmonic wave propagating in one direction. We can simply write this for Real valued and Complex Valued respectively.

$A\cos(\omega t + \phi - kz)$ and | $Ae^{i(\omega t+\phi-kz)}$

↑ Real valued cosine

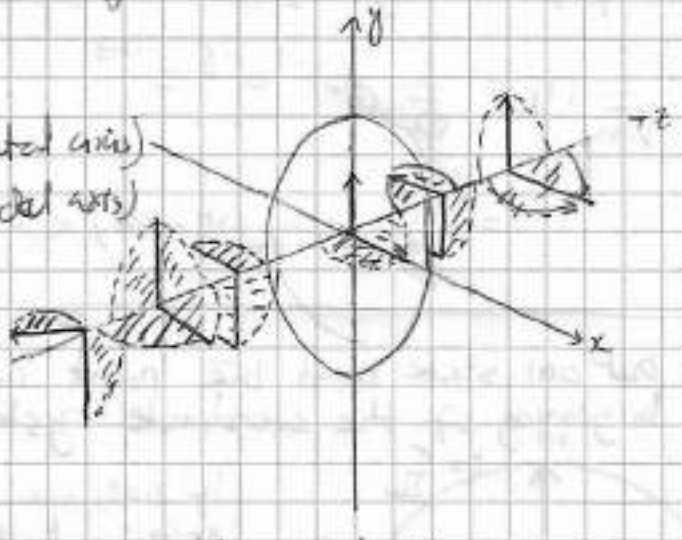
$= Ae^{i\omega t} * e^{i\phi} * e^{-ikz}$

↑ Complex exponent representation

- z: single coordinate
- k: wave number (defined by speed of wave propagation & its angular frequency)

$|0\rangle = xe^{i\omega t}e^{-ikz}$ (oscillates in horizontal axis)

$|1\rangle = ye^{i\omega t}e^{ikz}$ (oscillates along vertical axis)



$|1\rangle$ ~~red~~ blue

$|0\rangle$ – black

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$= \frac{1}{\sqrt{2}}\left(xe^{i\omega t}e^{-ikz} + ye^{i\omega t}e^{-ikz}\right)$$

$$= \frac{1}{\sqrt{2}}(x+y)\left(e^{i\omega t}e^{-ikz}\right)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(x+y)\left(e^{i(\omega t-kz)}\right)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(x+y)\left(\cos(\omega t-kz) + i\sin(\omega t-kz)\right)$$

$$\boxed{|+\rangle = \frac{1}{\sqrt{2}}(x+y)\cos(\omega t-kz)}$$

What if we consider the following state

$$|+'\rangle \neq \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

it looks pretty much the same, ~~except~~ as the state $|+\rangle$ except for the vector of 1, we have a slighty different coefficient (imaginary unit instead of a (real unit)

Does this substitution change our state?

- Though photons themselves are not harmonic waves but they can be represented as sums of harmonic waves.
- For the sake of clarity, we use only one harmonic wave of some angular frequency ω for each photon.
- Photon $|0\rangle$ is described by the following function & its real part is just cosine omegaT minus kz.

$$|0\rangle = xe^{i\omega t}e^{-ikz}$$
$$= x\cos(\omega t - kz) + i\sin(\omega t - kz)$$

↑ this oscillates along the x axis

photon $|1\rangle$ in our state is represented by this following function:

$$\frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}} y e^{i\omega t} e^{i\frac{\pi}{2}} e^{-ikz}$$

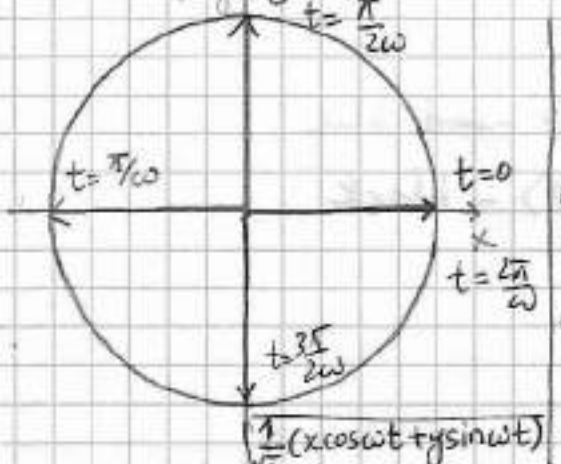
$$= \frac{1}{\sqrt{2}} y \sin(\omega t - kz) + i\sin(\omega t - kz)$$

$i = e^{i\pi/2}$

↑ (relative phase stuff) of $\pi/2$

real value is found be $\sin(\omega t - kz)$

Let's put our state and the point where $z=0$, to the beginning of the coordinate system.



$\frac{1}{\sqrt{2}}(x\cos\omega t + y\sin\omega t)$

if $t=0$, we have the position of our oscillator on the x-axis at $|0\rangle$ (point-1)
Since cosine(0)=1 and sine(0)=0

- When $\omega t = \pi/2$, we have the position of oscillator at the y-axis at point $|1\rangle$. since $\sin(\pi/2)=1$ and $\cos\frac{\pi}{2}=0$
- When $\omega t = \pi$, we have x-axis again, but the value of our function is -1.
- if $\omega t = 3\pi/2$, it is at y-axis but -1.
- When $\omega t = 2\pi$, we close the period & return to initial point.

device for this measurement is called a circular polarizer

it appears that the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ defines the state counter-clock wise and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ is clock wise.

→ right rotating polarization and the rotation is

these two states are orthogonal, so they define basis in the state space

Geometric Representation – Bloch Sphere

In the previous lecture, we discovered three different orthonormal bases in the state-space of one photon polarization.

(d) Rotation polarization

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

$$|\circlearrowright\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$$ (write after finding, the other two from the notes)

- We now know that state space in Quantum Mechanics is a vector space over complex numbers. Because in this complex #s we represent the phase shift as a multiplication by a scalar, which doesn't change the physical state.
- However, the relative phase shift in a superposition state changes the physical state.

(1) First basis we ever mentioned was this.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{—(i)}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

ψ : psi

$\alpha, \beta \in \mathbb{C}$

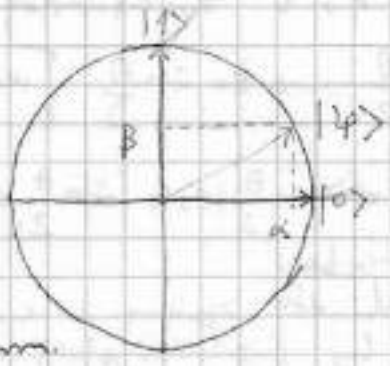
Horizontal polarization $= |0\rangle$

Vertical polarization $= |1\rangle$

$\alpha = a e^{i\xi}$

$\beta = b e^{i\eta}$

} polar form.



If we write our state with polar coefficients.

$$\alpha = a e^{i\xi}$$
$$\beta = b e^{i\eta}$$

$$\Rightarrow \alpha|0\rangle + \beta|1\rangle = a e^{i\xi}|0\rangle + b e^{i\eta}|1\rangle$$

$$= e^{i\xi}\left(a|0\rangle + b\frac{e^{i\eta}}{e^{i\xi}}|1\rangle\right) = e^{i\xi}\left(a|0\rangle + b e^{i(\eta-\xi)}|1\rangle\right)$$

↑ this coefficient is multiplied with the whole state and multiplication with a scalar doesn't change the state so we can omit it.

$$\boxed{\alpha|0\rangle + \beta|1\rangle = a|0\rangle + b e^{i(\eta-\xi)}|1\rangle}$$

but:

$$\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

$$\Rightarrow |\psi\rangle = a|0\rangle + b e^{i(\eta-\xi)}|1\rangle \quad \& \quad \phi = \eta - \xi$$

$a \in \mathbb{R}$, coefficient of the imaginary part has the physical meaning of relative phase shift.

The final expression becomes.

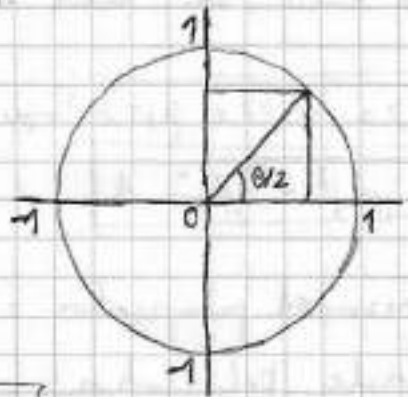
$$\phi = \eta - \xi$$

$$|\psi\rangle = a|0\rangle + b e^{i\phi}|1\rangle \quad \#\#; \quad a^2 + b^2 = 1$$

$a, b \in \mathbb{R}$ and $a^2 + b^2 = 1$ modules of the coefficients of their original decomposition. The sum of their squares is 1. because the state $|\psi\rangle$ is a normalized state.

$a^2 + b^2 = 1 \Rightarrow$ equation of circle with radius 1

$a = \cos\frac{\theta}{2}$, $b = \sin\frac{\theta}{2}$ [WHY DIVIDE IT BY TWO?]

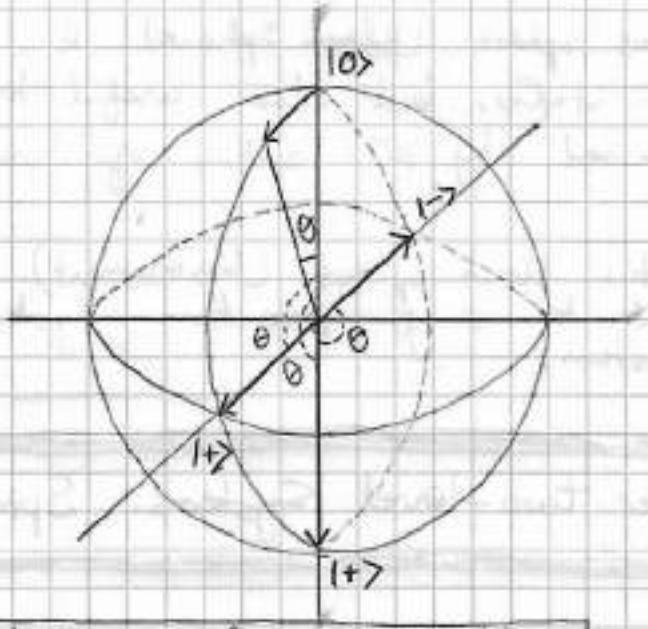


$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2} e^{i\phi}|1\rangle$$

Do you remember:
Any coordinate system where position of a point is defined by two angles?

of course, its a coordinate of a sphere System Surface

BLOCH SPHERE:



• Imagine that we have a sphere
We put our vector $|0\rangle$ on the top
it corresponds to

$$\theta = 0, \quad \phi = 0$$

• Now we will increment the angle θ
θ corresponds to the altitude on the sphere.

ϕ : longitude = 0

• Now when $\theta = \pi/2$
we have this point on equator with zero (0) longitude, which corresponds to the vector $|+\rangle$

• When $\theta = \pi$, we have the state of the bottom of the sphere, which corresponds to the state $|1\rangle$.

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$$

θ: Altitude
ϕ: Longitude

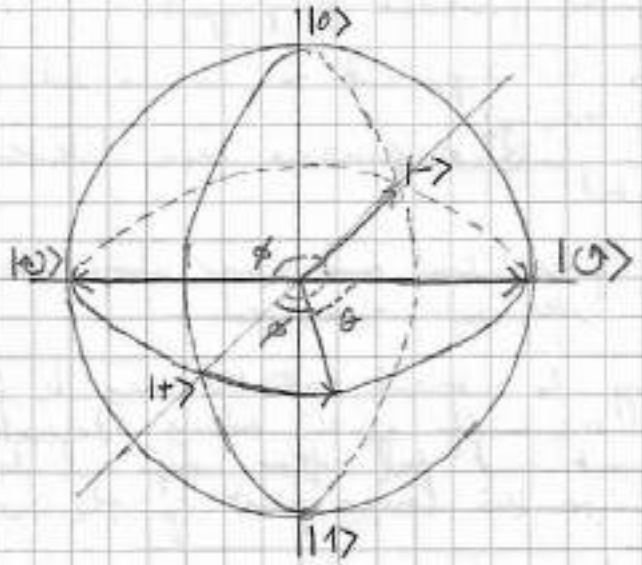
That's why we used $\frac{\theta}{2}$ instead of θ, because
• we wanted states $|0\rangle$ and $|1\rangle$ to be on the opposite points of the sphere.

θ	ϕ	state
0	0	$\|0\rangle$
$\frac{\pi}{2}$	0	$\|+\rangle$
π	0	$\|1\rangle$
$\frac{3\pi}{2}$	0	$\|-\rangle$

THIS sphere is called a BLOCH SPHERE name after Swiss US physicist Felix Bloch.

Until Now we considered states with 0 longitude where $\cos k\phi = 0$.

Lets see what happens when you increment ϕ.



• Let's start the from the state $|+\rangle$

θ	ϕ	state	
$\pi/2$	0	$\|+\rangle$	
$\pi/2$	$\pi/2$	$\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	• (i)
$\frac{\pi}{2}$	$\frac{3\pi}{2}$ ($-\frac{\pi}{2}$)	$\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	• (ii)
$\pi/2$	π	$\|-\rangle$	

(i) & (ii) are basis vectors of rotational basis

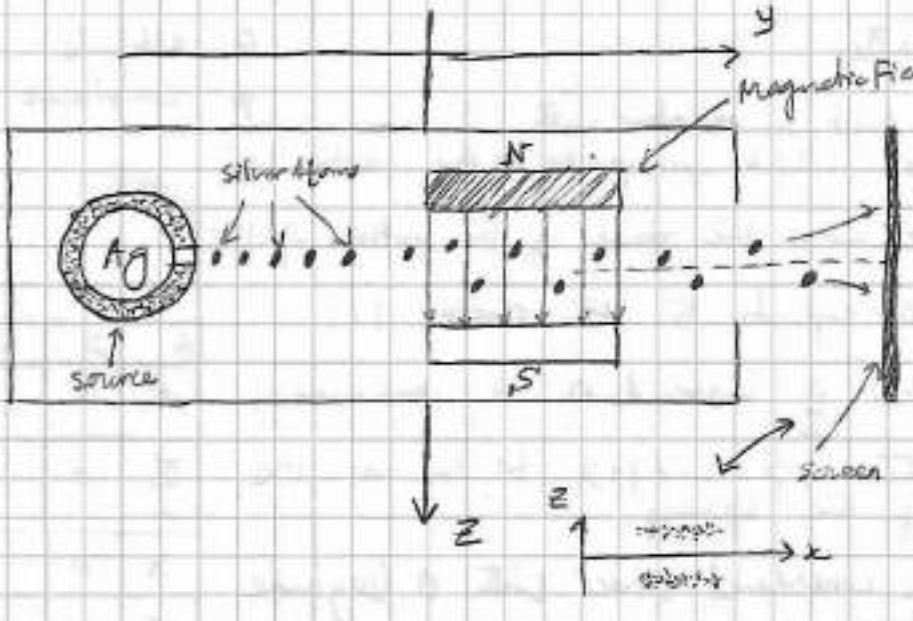
We have all three very important basis $|+\rangle, |-\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle$ geometrically represented on a sphere. And any point on this sphere corresponds to some possible photon polarization with particular direction & phase shift (ϕ).

This sphere (Bloch Sphere) is not only useful for representing the states, but also useful to represent evolution of states caused by the action of various unitary operators.

This Bloch sphere (Instrument) is not only applicable to photons but to any quantum system with two states or two level system.

Other two-level Systems. Spin $\frac{1}{2}$:

Stern–Gerlach Experiment (1922) (z-axis)



- Expose a narrow beam of silver atoms which was passing through the apparatus where they were exposed to the magnetic field. oriented orthogonally to the direction of the particles propagation.
- The direction of magnetic field orientation is important to us so let's call it z. (Silver atoms fly along the axis-y)
- After passing through the magnetic field, particles' positions were detected on the screen placed after the apparatus.
- The purpose of the experiment was to check if electrons and silver atoms interacted with the magnetic field & is their interaction quantized.
- The experimental result showed that they do interact with the magnetic field but in a very strange way, about one half of the atoms deflected by a constant angle to the upper part and the other half of atoms were deflected by a constant angle to the lower part of the screen.
- This result is very important since it shows that atoms have some measurable property which can seriously alter their behaviour in the presence of magnetic fields this property was called the magnetic moment of a particle or spin. The name spin have suggests that Something is spinning. Electrons are charged particles & in Bohr's model

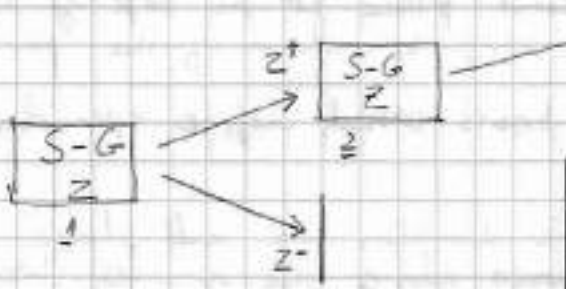
of an atom, they circulate around the positive core producing a magnetic field. The direction of this field depends on the direction and trajectory of this rotation. It is very hard to believe that all electrons in all the silver atoms from the beam rotated in just one plane.

- In terms of Bohr's model with Rotating electrons, this experimental result has no explanation.
- So instead of imagining electrons as some charged rotating balls, we just need to admit that we don't know what they are. But we know that they interact with magnetic fields in this strange way.

First we need to build more Stern-Gerlach Apparatus and we need to place them in series.

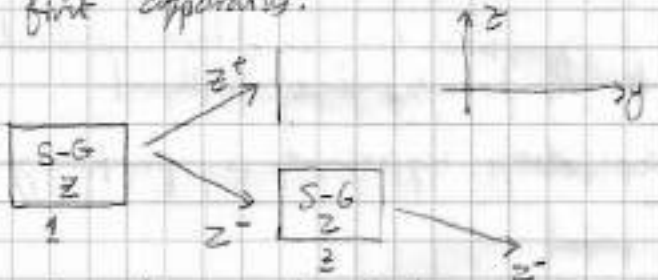
The thing we are going to adjust in these different apparatus is the direction of the magnetic field.

Double S-G. (Z-Z)



Identical apparatus one after another

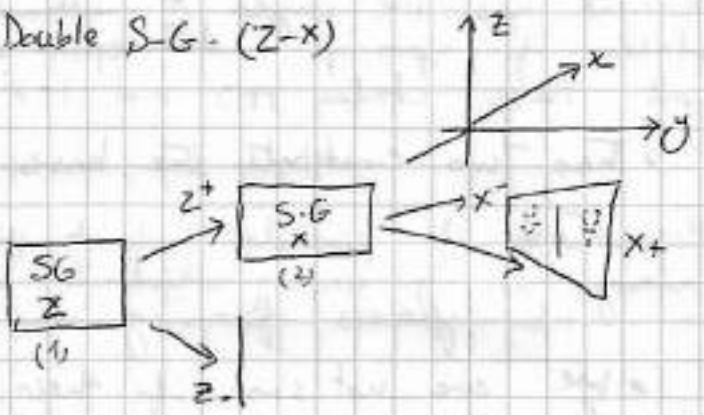
Apparatus 1 splits the silver beam into parts (z^+, z^-) (z^+ deflects up & vice versa)
We will block z^- particles. Thus, allowing only z^+ to enter the second apparatus. This experiment shows us that all particles from z^+ beam also deflect upwards in the second apparatus.
The angle of deflection is also same as the first apparatus.



Same observation as to that of z^+ for the z^- particles.

This follows from the symmetry of this experimental set.

Double S-G. (Z-X)

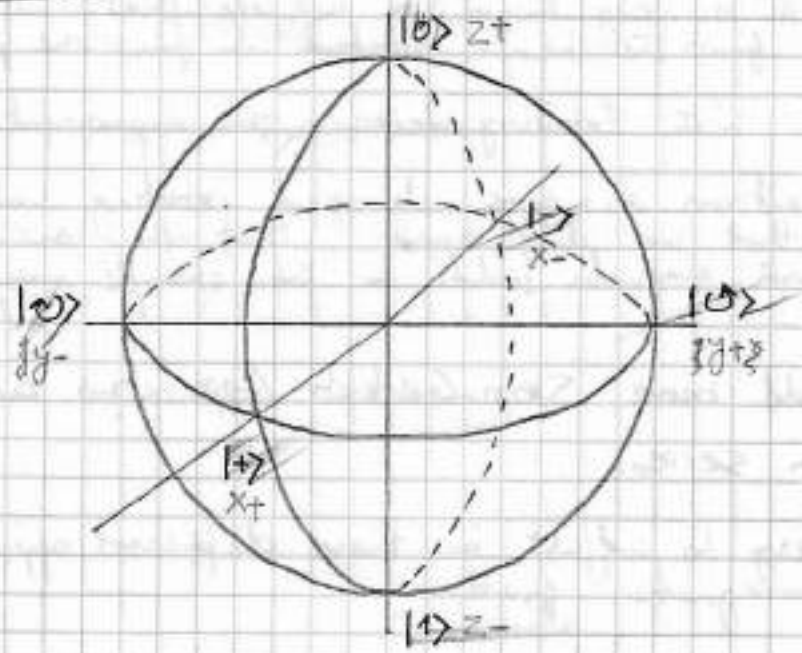


What if we orient the second Stern Gerlach apparatus along the x-axis.
The z^+ particles again interact with the field & form two equal beams with the same constant angle of deflection

Measurement, Is it? (of a 2 level system)

- 2 possible outcomes
- truly random
- collapse to the measured state
- can be measured in different bases.

Bloch Sphere



- We have a two level system, that means we can draw it on a block sphere. The state of the particles that will spin up along the z-axis, we will denote $|0\rangle$ and place it on top of the sphere. The opposite point situates the state $|1\rangle$, spin down of the particles along z-axis.
  - These two states constitute the basis which define spin down along the z-axis.
- x-axis has the angle $\frac{\pi}{2}$ with the z-axis, we will place our states of spin up and spin down along the x-axis we will call these states $|+\rangle$ and $|-\rangle$.
  - These two constitute the basis for the spin along the x-axis
- The state of particles which that haven't spin up or down along the y-axis (which is direction of their propagation) are on the y-axis forming the rotational basis.
  - We are not sure if their rotation has a physical meaning here. But it is an analogue of the rotational basis for photons. Thats why we call it this way.

particles that have this kind of result in Stern-Gerlach experiment (just two measurement outcomes) are called spin one-half (spin $\frac{1}{2}$) particles. They represent a perfectly defined two-level system for us.

Entanglement One qubit is good, but we can't solve a lot of problems with it. For real computational problems, we need more qubits.

$\left\{\begin{array}{l} 1|+\rangle \rightarrow \text{measurement} \\ 2|+\rangle \rightarrow \text{measurement} \\ \vdots \\ 1000|+\rangle \longrightarrow \text{measurement} \end{array}\right.$

At first glance it doesn't present any problems.

Photons, electrons, silver atoms they have plenty of these.

For example if 1000 qubits are required, we can generate 1000 photons easily and its no problem for us to generate all those photons in a superposition state eg $|+\rangle$

Now imagine we did that, now if we measure all those thousand photons each in 0/1 basis

How many possible outcomes can we get? $2^{1000} \sim 10^{300}$

- Each photon can randomly collapse to one of those basis states which gives us 2 opportunities for each photon. Adding just one more digit to it roughly multiplies it by 10 and our number of outcomes, we have almost more than 2000 digits to that humendous number.

– Physical meaning of 2^{1000} or 10^{300}

Since it is the number of outcomes (all possible), it is the size of the basis in the state space of the considered system.

Our space system with 1000 photons is described by a vector in the state space of this dimensionality.

- Generally, the dimensionality of a state space system with n two level particles is 2^n. This gives us almost unlimited computing power.

- By adding one particle to it, we can double the dimensionality of the state space.

WHY DON'T WE USE IT RIGHT NOW?

This is indeed a good question.
To answer it, we first need to recall, how we use data in classical computations.

- Most of algorithms don't process bits of data separately as processing parts of information almost always depends upon other parts of information.

- Consider the example of adding two #'s 13 & 18

$$\begin{array}{r} 1 \leftarrow \\ 13 \\ 18 \\ \hline 31 \end{array}$$

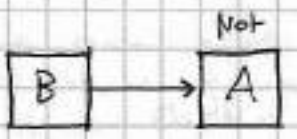
The result of adding 1 and 1 depends on the result of adding 3 & 8.

- So in our hypothetical computer based on photons, processing or changing

The states of some photons will depend on the state of another photons.

- As we remember, we cannot read those states, because in that case, those states would collapse, and destroy the superposition. which was the source of all our magic in the first place.
- It looks like that photons will have to read the state of our photons without our help.

CONDITIONAL NOT



- Imagine two photons A and B
- Now imagine we can make the photon A read the state of photon B.
- Not just to read, but to change its own state accordingly.

This operation is called conditional NOT

We apply the gate NOT to photon A based on the state of photon B.

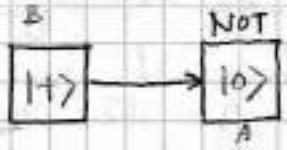
[We want photon A to flip its state to Opposite if photon B is in state 1 and we want it to do nothing if photon B is in state 0]

Please know that we dont read, ourselves, any of those two states. For us the state B doesn't collapse.

Lets assume that we can perform this operation.

For now let us be the photon A in state $|0\rangle$ and photon B in the state $|+\rangle$.

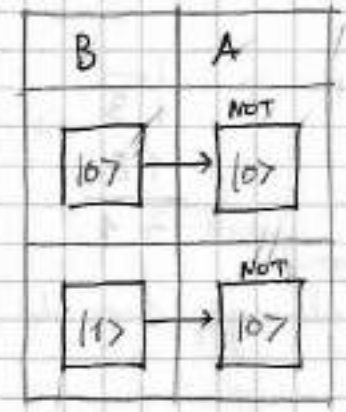
$|+\rangle$ is superposition of $|0\rangle$ and $|1\rangle$



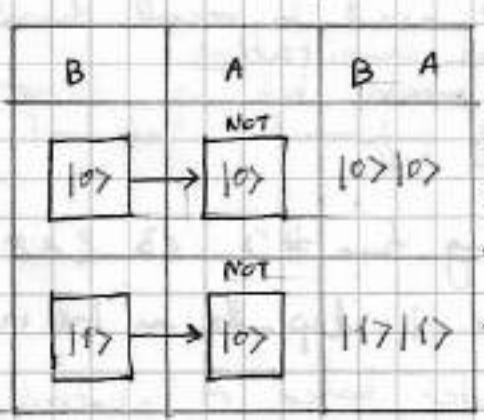
CNOT (Conditional NOT)

What state will we obtain after applying this CNOT gate.?

From a multiverse perspective, photon B exists in two different state in 2 different universes simultaneously ($|0\rangle$ and $|1\rangle$)



CNOT photon A also has many copies in the multiverse but for now the copies are identical.



But when photon A interacts with photon B, it subjectively absorbs different copies of B so it's own state stops being identical

- The copy of A which absorbs $|0\rangle$ does not change BUT
- The copy of A which absorbs $|1\rangle$ flips its state to $|1\rangle$ and we

Bell states and CNOT

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$(|+\rangle)(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$$

$$\rightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

- this state is one of the famous Bells states.
- it describes the state of a two particle system, but the most astonishing thing about it is that these particles don't have their separate states.
- we can't say now that which state has photon A or photon B from now on.
- it is like a superposition but not for a particle but for a system of apparticles
- Though these particles are separate and could be very far from each others, **their states are like glued together or ENTANGLED**. entangled is the right term for these type of states; and the operation we have performed on the paper (this CNOT gate) is an entanglement operation.
- To be able to perform meaningful computations, we must be able to implement this operation with any two particles of our system. ✡

CNOT

B	A	B A
$\|0\rangle$	NOT → $\|0\rangle$	$\|0\rangle\,\|0\rangle$
$\|1\rangle$	NOT → $\|0\rangle$	$\|1\rangle\,\|1\rangle$

✡ can we implement it?

(NOT SO WELL)

There are no experiments (so far), to implement CNOT with photon polarization, but there are some positive results with other two level systems like RYDBERG ATOMS

↳ Rydberg atoms are like atoms with very big radius.

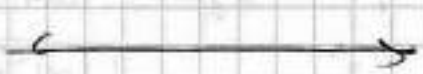
- Big radius is important because we have a physical contradiction here, we need particles to be far enough from each other so we could control the states separately with eg. a laser beam, also we want them to be closed enough to each other, so they would be able to interact and construct these entangled states. Big Radius of atoms, allows us to control them separately when they are placed near each other.
- AND of course there is no way we can arrange these atoms in a physical 3D space ✡

✡ they will be able to form these entangled ensembles in any desired order.

- There can be only limited number of close neighbors for each atom.
- So for implementing entanglement operators, at least for now, we have problems.

BUT KEEP YOUR CHIN UP.

PHYSICISTS ARE WORKING ON THIS



Systems with multiple Qubits

In majority of cases, we need more than 1 bit to perform our computation. Same holds for Quantum Computing

In this part we discuss the mathematical descriptn of a system with multiple qubits

Two QUBITS

$qubit_I$	$qubit_{II}$
$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

- In the adjoining table;

Imagine that we have two particles, each carrying one qubit.
"we have the possible measurement outcomes for these two qubits in our ordinary basis $|0\rangle$ & $|1\rangle$."

it is convenient for us to describe that measurement outcome in some Hilbert space, (some linear space over complex #'s)

- Since we have 4 different measurement outcomes here, this space has to be 4-dimensional.
- Each measurement outcome will be again, one of the basis vectors of this space.

Q1	Q2	Notes
$\|0\rangle$	$\|0\rangle$	$\|00\rangle$
$\|0\rangle$	$\|1\rangle$	$\|01\rangle$
$\|1\rangle$	$\|0\rangle$	$\|10\rangle$
$\|1\rangle$	$\|1\rangle$	$\|11\rangle$

Basis vectors

So we have just need four basis vectors of this space to which we will describe the system with two qubits.

qubit 1	qubit II
$\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$

- Now imagine one of these qubits have this superposition before the measurement.
- Can we describe this state before the measurement in the space we just constructed?
- Yes we can, we can describe it like this

$$\alpha|00\rangle + \beta|01\rangle$$ ← this system is also in a superposition state.

& the probabilities of these measured outcomes is still the same

$$|\alpha|^2 + |\beta|^2 \rightarrow \text{measurement outcomes.}$$

Since the measurement of first qubit always gives us $|0\rangle$ and the measurement of the second qubit is probabilistic for us.

Again, sum of coefficients must be 1.

$$|\alpha|^2 + |\beta|^2 = 1$$

Next page 23

Now let us consider a more complicated situation

Qubit I	Qubit II	vector
$\alpha\|0\rangle + \beta\|1\rangle$	$\gamma\|0\rangle + \delta\|1\rangle$	$\alpha\gamma\|00\rangle + \alpha\delta\|01\rangle + \beta\gamma\|10\rangle + \beta\delta\|11\rangle$ *

- both qubits are in some superposition, we can describe this state in our newly constructed space like *
- it is easy to show that sum of squares of all these coefficients give us 1.

$$|\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 = 1 \quad \leftarrow \text{unitary vector}$$

for any state, e.g. $\alpha\delta|01\rangle$, the probability of obtaining this state is $|\alpha\delta|^2$. This is true because we believe that measurement of two different particles are independent events,

so we can multiply these probabilities like $|\alpha|^2$ to obtain $|0\rangle$ from $\alpha|0\rangle$

and $|\delta|^2$ for obtaining $|1\rangle$ in $\delta|1\rangle$.

probability of $|01\rangle$ is $|\alpha|^2|\delta|^2$

The amazing part is that we cannot construct the whole space like this, because there are vectors in this four-dimensional space, for example the one below:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$ which cannot be constructed through the process we just described & employed above.

But physically this state can exist on two separate particles!

Now common misunderstanding about all this, the real quantum systems, the qubits, they are not situated in some Hilbert spaces, and if we take two of them, they don't initiate some tensor product of these spaces. This is our way & our choice of describing them. Because it is convenient for us to describe two qubits in the space of four dimensions.

We already have named our bases; now we have to show how to enumerate it, we have to decide which column vectors represent these bases:

$$\vec{|0\rangle} = \begin{pmatrix}1\\0\end{pmatrix}, \quad \vec{|1\rangle} = \begin{pmatrix}0\\1\end{pmatrix}$$

Now we have to choose, for each bases vectors, of our newly constructed space that which column vectors represent it and we have many rules we can use for this & most basic rule for us will be *

* $|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\\begin{pmatrix}0\\0\end{pmatrix}\end{pmatrix} \approx$

$\vec{|00\rangle} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$

we take individual vectors & take its tensor product of them

Kronecker Product

$$|01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}0\\1\end{pmatrix}\\ 0\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\\ \begin{pmatrix}0\\0\end{pmatrix}\end{pmatrix} \approx \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\begin{pmatrix}1\\0\end{pmatrix}\\ 1\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} \approx \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\begin{pmatrix}0\\1\end{pmatrix}\\ 1\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} \approx \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

We can apply these rules to the basis vectors and we obtain this →

Of course we can choose other rules for enumeration, but this rule is very convenient, if we use the binary notation here. if we notice $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ are 0, 1, 2, 3 respectively, which is # of our vectors, which corresponds to 1's in the position in the constructed basis vector in 4, dimensions

GENERALIZATION

Now generalizing our discussion:

For a system of n, qubits,

we have 2^n = dimensions

n = 1 ,	2 dimensions
n = 2 ,	4 dimensions
n = 3 ,	8 dimensions
⋮	
n = 10 ,	1024 dimensions
⋮	
n = 1000 ,	2^{1000} dimensions

$\approx (1024)^{100} \approx 10^{300}$ *

* This is why Richard Feynmann was so optimistic about quantum computing.

• One may argue that if we take 1000 of flipping coins, the # of outcomes of reading these coins will be the same to these # of outcomes (10^{300}). But for some reason, no one builds a computer on these flipping coins.

We will try to understand, WHY?

←→

for a binary number in n bits $x = |m_1\, m_2\, m_3 \ldots m_{n-1}\, m_n\rangle$, the basis for the corresponding will have a '1' at $(x+1)^{th}_{10}$ location of the column vector.

WEEK-4

QUANTUM COMPUTING.

LESS FORMULAE, MORE UNDERSTANDING

1. Inner Product
2. Conjugate space
3. Linear operators
4. Hermitian Operators
5. Eigenvalue Equation
6. Some examples
7. The Evolution of a Quantum System

Introduction:

- We are going to learn mathematical language of quantum Mechanics.

→ (Review the materials several times)

- Struggle until as much as could be understood
- Reading Material:
  - "Quantum Mechanics"
    - Claude Cohen-Tannoudji
    - Bernard Diu, • Franck Laloë
    } volume_1.

    Wiley_VCH

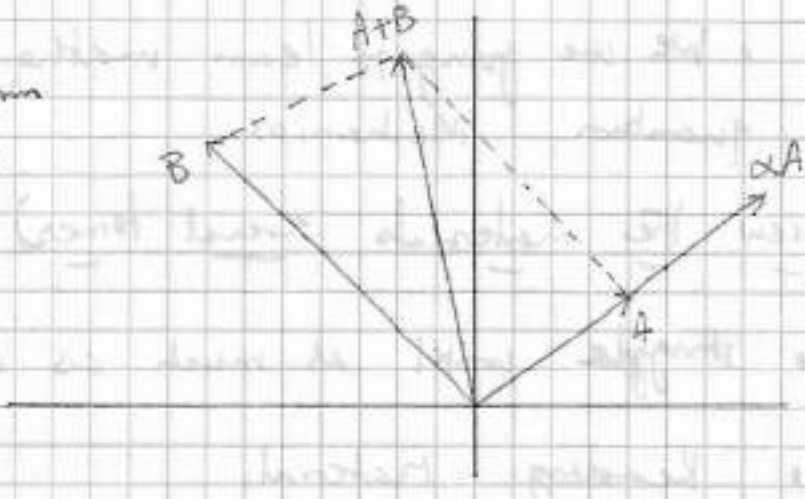
    ↑ (CHAPTER_2)

Week plan

1. Inner Product
2. Conjugate Space
3. Dirac Notation
4. Linear operators
5. Hermitian Conjugation
6. Hermitian & Unitary operators
7. Examples.

Inner Product

Linear Vector Space



For a particular set to form a vector space $\mathbb{F}$, it must satisfy two conditions

1) $\alpha A \in \mathbb{F}$

2) $A+B \in \mathbb{F}$

↓

Operations' Properties

are the conditions for these operations to be defined correctly.

- (1.) — $0 \cdot A = \vec{0}$, $A + \vec{0} = A$ ((+) must be a linear operation)
- (2.) — $\alpha(A+B) = \alpha A + \beta B$ (+ must be)
- (3.) — $A + B = B + A$ (commutative) (+ must be)
- (4.) — $(A+B)+C = A+(B+C) = A+B+C$ (Associative)/ Transitive

Inner / Scalar Product of these two vectors (·) / dot product

$\cdot : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$

$\vec{x}, \vec{y} \in \mathcal{H}$, $\alpha \in \mathbb{C}$

- This operation takes two vectors & returns a scalar.
- Latin letters (a, b, c, ..., z) denote vectors & greek letters denote scalars (fs).
- To be properly defined, inner products must satisfy the written 3 conditions

1. $\vec{x} \cdot \vec{y} = \overline{\vec{y} \cdot \vec{x}}$
2. $\vec{x} \cdot \alpha\vec{y} = \alpha(\vec{x} \cdot \vec{y})$
3. $\vec{x} \cdot \vec{x} \geq 0$ $\quad (\vec{x} \cdot \vec{x} = 0 \iff \vec{x} = \vec{0})$

1. Conjugate Symmetry: order of input vectors does matter for this operation. If we change this order, the result of this operation will be conjugated
2. The second condition is linearity in the second argument

3. Third is positive-definitiveness, which means that for any nonzero vector x,

For any non zero vector $\vec{x}$, the inner product of $\vec{x}\cdot\vec{x} > 0$.

if its 0, then $\vec{x} = \vec{0}$

[CONJUGATE SYMMETERY]

Since the inner product is equal to its conjugate, this is always is always a real value. so, we can rightfully place this last demand of it to be greater than 0. *

1. $\vec{x}\cdot\vec{y} = \overline{\vec{y}\cdot\vec{x}}$

* And if we have this operation defined in our vector space. Then this vector space belongs to the special class of spaces called **Hilbert Spaces**

INNER PRODUCT IS NOT SIMPLE TO LEARN FROM DEFINITION, SO LET'S LOOK AT SOME EXAMPLES"

- INNER PRODUCT IN EUCLIDEAN SPACE

[dimensionality = n.]

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}, \quad \vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{pmatrix}$$

- Let $\vec{x}$, $\vec{y}$ be some vectors with components denoted by x_i and y_i respectively.
- i- defines the position of the component in the vector column.

$[x_i, y_i \in \mathbb{R} \ \forall i]$

$$\vec{x}\cdot\vec{y} = \sum_{i=1}^{n} x_i y_i = \text{scalar}$$

- Let's check if all the demands for an inner product defined like this are met:

(1.) $\vec{x}\cdot\vec{y} = \sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} y_i x_i = \vec{y}\cdot\vec{x}$ [Conjugate Symmetry becomes first symmetry since $x_i, y_i \in \mathbb{R}$]

(2.) $\vec{x}\cdot\alpha\vec{y} = \sum_{i=1}^{n} x_i \alpha y_i = \alpha\sum_{i=1}^{n} x_i y_i = \alpha(\vec{x}\cdot\vec{y})$ [Linearity of 2nd argument is also satisfied, & in euclidean spaces, we have linearity of dot product in 1st argument also]

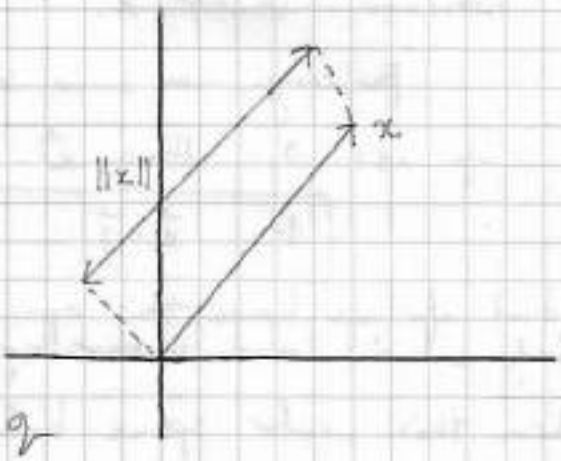
(3.) $\vec{x}\cdot\vec{x} = \sum_{i=1}^{n} x_i x_i = \sum_{i=1}^{n} x_i^2 \geq 0$.

it appears to be 0 if all the squares are zero, which is true only for zero vectors.

• positive definitiveness also is satisfied, since inner product of a vector by itself is sum of squares, which is always greater than zero

$$\|x\| = \sqrt{\vec{x}\cdot\vec{x}} \quad \text{(i)}$$

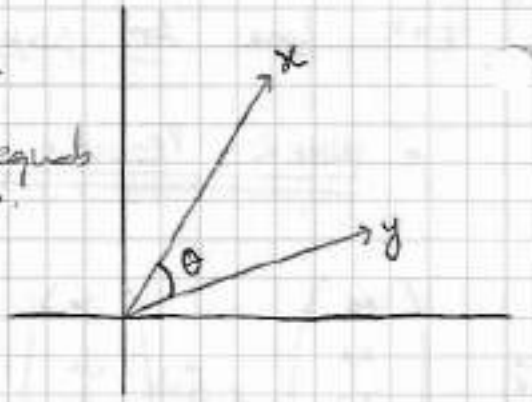
- The concept of multiplication of components & their addition defines an inner product.
- For Euclidean spaces, it also has a geometrical interpretation.
  - First, the inner product of a vector by itself equals, the squared ~~root~~ length of this vector.



  - So we can normalize any vector by dividing it by the square root of it's inner square.

- Second, if you calculate a dot product of two normalized vectors, the result equals to the cosine of the angle b/w them.

$$\cos\theta = \frac{\vec{x}\cdot\vec{y}}{\|x\|\,\|y\|} \quad \text{(ii)}$$



This allows us to perform a very simple orthogonality test.
- if the dot products of two vectors is zero, it means that the cosine of the angle between them is also zero and these vectors are mutually orthogonal ($\cos(n\frac{\pi}{2}) = 0$) $\cos\frac{\pi}{2} = 0$ ← perpendicular

INNER PRODUCT IN HILBERT SPACE (Vector space over complex #s)

$$\vec{x}\cdot\vec{y} = \sum_{i=1}^{n} x_i^* y_i$$

- We define it, pretty much in the same way (multiply the corresponding components (and add up the results)

- But now, these components are complex numbers, and to satisfy the conjugate symmetry demand, we conjugate the components of the first vector in this sum.

An operation defined like this, also satisfies all the demands of an inner product previously mentioned in equations (i) & (ii)

$$\|x\| = \sqrt{\vec{x}\cdot\vec{x}} \quad \text{and} \quad \cos\theta = \frac{|\vec{x}\cdot\vec{y}|}{\|x\|\,\|y\|}$$

The most important result of defining this operation in our vector space is the possibility to define the length of any vector and and the angle b/w any two vectors

- The length of any vector x is, by definition, the square root of the dot product of the vector x by itself.

$$\|x\| = \sqrt{\vec{x} \cdot \vec{x}}$$

- The cosine of angle b/w $\vec{x}$ & $\vec{y}$ is again by definition, is the absolute value of their inner product divided by their lengths.

You/we can see the length and angles in the vector spaces over the complex numbers are defined by analogy in the Euclidean spaces.

$$\cos\theta = \frac{|\vec{x} \cdot \vec{y}|}{\|x\| \, \|y\|}$$

← In the spaces over real numbers, the result of inner product operation is always a real number.

← for spaces over complex numbers, the inner product of two vectors can be a complex number.

and for it to be defined properly as a cosine of some angle, we decided to take absolute value of it.

[the absolute value of a complex # is always real and thus defines the cosine of some angle]

- Thus the angles in Hilbert space in general are not defined intuitively since we can't easily imagine them, but in this strict mathematical way (and since the absolute values are always positive), we don't have negative cosines anymore.
- It means that in Hilbert space over complex numbers, we don't have obtuse angles.

Inner product in Hilbert Space:

Now that we have a great instrument of defining angles and lengths, we can even do it with the vector space of square integrable functions

$$f \cdot g = \int f^* g$$

- If we can define an inner product in this space, we can define such things as functions, length or an angle between two functions.
- And we could say that some function f and g are mutually orthogonal.
- The dot product of two square integrable functions (complex valued) is defined as an integral of the product over the whole space

and again to satisfy the conjugate symmetry demand, the first part (function) in this product is conjugated.

This operation meets all the demands for the dot product:

Orthonormal Basis:

Now we can justify our previous talks about orthonormal basis.

The orthonormal basis consists of vectors which are all mutually orthogonal and have the unit length.

1. $E = \{e_i\}_{i=1}^{n}$, { orthonormal basis }
2. $\vec{e}_i \cdot \vec{e}_i = 1, \quad \forall i$ { unit length }
3. $i = j \iff \vec{e}_i \cdot \vec{e}_j = 0 \quad \forall i,j$ { mutually orthogonal }

Now with a notion of angle and length properly defined. we can check if some basis is orthonormal.

- The inner square of all its elements must be equal to 1.
- The inner product of any two different elements must be 0.

Conjugate Space:

Let us consider some non zero vector $\vec{x}$ in Hilbert vector space $\mathcal{H}$.

- $\vec{x} \in \mathcal{H}$
- $f_x : \vec{y} \to \vec{x} \cdot \vec{y}$, $\forall y \in \mathcal{H}$
- $f_x : \mathcal{H}^*$

- The inner product of $\vec{x}$ by any other vector is a scalar
- This allows us to define a linear functional f_x defined by x
- A functional is a thing that takes in a vector as an input and returns a scalar as an output

- The action of the functional is this

For any vector y, the action of f_x on y is inner product of $\not{x}_{(x)}$ and $\not{y}_{(y)}$.

$$\boxed{f_x : \vec{y} \longrightarrow \vec{x} \cdot \vec{y}}, \quad \forall y \in \mathcal{H}$$

- One could easily see that a functional defined like this is linear.
- The set of all linear functionals over $\mathcal{H}$, also form a ~~linear~~ vector space
- This space is called the conjugate space of $\mathcal{H}$

$$f_x : \mathcal{H}^*$$

Bra-ket Notation :-

So $\mathcal{H}$ is some Hilbert space, and these vectors of this space placed in this Dirac bra-kets called kets.

$|x\rangle \in \mathcal{H}$

$\langle x| \in \mathcal{H}^*$

$\mathcal{H}^*$ is a conjugate space of $\mathcal{H}$ and it consists of linear functions over $\mathcal{H}$ and elements of it, we will replace again in these bra-kets but reversed called bra's. The word bra-ket together form braket.

$|\ \rangle$: ket

$\langle|$: bra

So linear function defined by vector x, we will denote as bra x.

$$f_x = \langle x|$$

the action of this function on any ket $|y\rangle$, which is dot product of x & y, we will denote as following

$$\langle x|y\rangle = \vec{x}\cdot\vec{y}$$

{ bra x & ket y } { our notation for inner product of two vectors }

We remember that "kets" are represented as colums vectors. and its fine to define bra's.

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

It is very natural to represent them as vector rows with conjugated coordinates

$$\langle x| = (x_1^*, x_2^*, x_3^*, \dots, x_n^*)$$

The reason behind this is so the dot product of them becomes a simple matrix product for us with one row & column.

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i = (x_1^*, x_2^*, x_3^*, \dots, x_n^*) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}$$

Summary :-

① $|x\rangle \in \mathcal{H}$ → The state of system in its state space is denoted as ket

② $\langle x| \in \mathcal{H}^*$ → The conjuage space $\mathcal{H}^*$ for space $\mathcal{H}^*$ consist of linear functionals over $\mathcal{H}$. we can construct those functionals with vectors of $\mathcal{H}$

③ $\langle x|y\rangle = \sum_{i}^{n} x_i^* y_i$ ← The action of such functional is inner product

For finite dimensional spaces which present the particular interest for us. The whole space $\mathcal{H}^*$ is constructed this way. This means that for any linear functional f, there exists a ket which defines f as an inner product by this ket

> The vector row $\langle x|$ is called Hermitian conjugate of the vector column $|x\rangle$

Hermitian Conjugation

For now we know how this operation acts on scalars and vector columns

- For any scalar α, the hermitian conjugate is just ~~α adapte~~ α conjugated

$$\boxed{\alpha^* = \overline{\alpha}}$$

- For any ket x, $(|x\rangle)$ its hermitian conjugate is bra x $(\langle x|)$.

$$\boxed{|x\rangle^* = \langle x|}$$ which is a row vector with conjugated components.

- For bra x $(\langle x|)$, its Hermitian conjugate is, by definition ket x $(|x\rangle)$. ~~adjoint~~

$$\boxed{\langle x|^* = |x\rangle}$$

The Hermitian operation performed twice will return us the initial value.

LINEAR OPERATORS

- Upto this point, we considered vectors in a state space. Vectors represent qubits, which we use to store quantum data.
- But for real computation we need more than just to store something
- We should be able to modify it. Usually according to some plan called an Algorithm.

- We need an instrument which is able to modify vectors.
- Or from physical point of view, which modifies the state of a system.
- In general, an operator is a thing which maps vectors to vectors.

Let $\mathcal{H}$ be some Hilbert space; an operator A is called a linear operator if,

$$\boxed{A : \mathcal{H} \to \mathcal{H}}$$

if for any two vectors $\vec{x}$ and $\vec{y}$ and two scalars α and β, the action of A on $(\alpha|x\rangle$ plus $(\beta|y\rangle$ equals to doing.

$$\boxed{A(\alpha|x\rangle + \beta|y\rangle) = \alpha A|x\rangle + \beta A|y\rangle}$$

As we already have established that in quantum computing, we deal with qubits which means that the state spaces that we usually consider are finite dimensional.

For a finite space $\mathcal{H}$, a linear operator A in that space can be represented as a square matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$$

The action of operator A on $\vec{x}$ in this case is simple matrix multiplication.

$$A|x\rangle = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

- After this multiplication, we obtain another vector column.
- ~~To obtain the resultant vectors we multiply the operator matrix by the vector column and~~ Each component of this resultant column is obtained by matrix multiplication of the corresponding row of matrix A and the column x. So we can consider an operator as an ordered

functional. The operator's action on the vector is a vector whose components are the results of the corresponding linear functionals applied to this vector.

Now let's consider some linear operator A with its matrix representation.

AND we are going to apply this operator to the first basis vector of the orthonormal basis.

$$A|e_1\rangle = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} \leftarrow \text{First column of Matrix } A.$$

Obtaining Matrix

$$A|e_k\rangle = \begin{bmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2k} & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix}$$

(column k of the matrix; row k of the basis vector)

- This gives us a very simple way for obtaining matrix representation of any linear operator.
- If we know how an operator acts on this particular basis, then we can construct the matrix columns by columns, by sequentially applying to these basis vectors

* Linear operators in Hilbert space form special structure that mathematicians call Algebra. This means two things.
  - (i) Linear Operators acting in a linear space also form a vector space.
  - (ii) Operators can be multiplied, & the result of this multiplication is a linear operator in the same space.

(MORE DETAILS. NEXT PAGE)

Operations with Operators :

- We start with the notion of linear vector space.
For linear operators to form a vector space, they must properly define two operations. (multiplication by a scalar & Addition)

Capital letters denote operators, while small letters denote scalars.

1. For an operator A and a scalar λ, the action of operator λA is action A and then multiplication by lambda.

$$(\lambda A)|x\rangle = \lambda(A|x\rangle) = A(\lambda|x\rangle)$$

2. For the sum of two linear operators A & B; it is also a linear operator A plus B. It acts on any vector

The matrix of A plus B is a matrix each component of which is obtained by the addition of corresponding components of A and B.

$$A+B = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

Matrix λA is a matrix in which each component of the matrix is multiplied by λ.

$$\lambda A = \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \cdots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \cdots & \lambda a_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda a_{n1} & \lambda a_{n2} & \cdots & \lambda a_{mn} \end{pmatrix}$$

Since we have addition and multiplication with scalar defined. we must also now have special element in this vector space. which is neutral with respect to addition, the 0 element. Represented by a matrix consisting of all 0's

$$O_{m,n} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

we also have to define the operation minus A.

The addition of A and $-A$ gives us this zero operator.

- This allows us to conclude that the matrix $-A$ consists $-A$ of the same matrix A but each element with a minus sign.

$$= \begin{pmatrix} -a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & -a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & -a_{nn} \end{pmatrix}$$

it is easy to show the following:

(1.) The sum operation is commutative.

$$A+B = B+A$$

(2.) associative

$$A+(B+C) = (A+B)+C = A+B+C$$

and distributive with multiplication with a scalar.

(3.) $$\lambda(A+B) = \lambda A + \lambda B$$

Linear operators, thus, form a linear vector space.

What about their multiplication

PRODUCT OF OPERATORS

- The product of two operators A, B is defined like this

$$(AB)|x\rangle = A(B|x\rangle)$$

Associative ☺

- $(AB)C = A(BC) = ABC$

Distributive

- $A(B+C) = AB + AC$

But: Linear operators don't commute

$$AB \neq BA$$

However, for some pairs of operators it is not true. (generally)

$$(AB)|x\rangle = A(B|x\rangle)$$

$$[A,B] = AB - BA$$

- To distinguish these two situations, we have a very simple instrument called the "commutator"
- The commutator of two operators A & B is defined as: (which itself is an operator defined like this

$$[A,B] = AB - BA$$

if $AB - BA \Rightarrow ([A,B] = 0)$

From a physical point of view, these operators represent observables, and its very important to know if a pair of observables commute or not.

So, this commutator is simple but is a very powerful & useful thing.

Hermitian Operators:

A linear functional is a thing that maps vectors to scalars. and we discovered that many linear functionals(H) can be obtained by the vectors of a space by an operation called Hermitian conjugation. — Means that for any linear functional, we can find the vector phi ϕ, whose hermitian conjugate defines this functional

We agreed to represent this functional as a vector now. with conjugated components!

Now imagine that we have some functional defined by some vector phi. & this we are going to define another functional based on this bra of $\langle\phi|$ and some linear operator A.

this new functional, we are going to denote as $\langle\phi|_A$, it will act as follows:

" For any vector psi, we first apply operator A to it and then $\langle\phi|$" this new thing is indeed a linear functional.

→ it takes vectors as inputs & returns scalars as outputs.

→ Since it's a linear functional, there must be some vector ϕ_A which hermitian conjugate defines. and this vector is defined by some initial vector ϕ and operator A.

Action on Left

- $\langle\phi| \in H^*$
- $\langle\phi|_A : \langle\phi|_A |x\rangle = \langle\phi| (A|x\rangle)$
- $\langle\phi|_A = |\phi_A\rangle^*$, $|\phi_A\rangle$ -

This operation for construction of vector row from another vector row with the help of an operator is called the action of the operator onto left

- $\langle\phi|A = \langle\phi|_A$
- $|\phi_A\rangle = (\langle\phi|A)^*$

So with any bra $(\langle|)$ which means any linear functional from the conjugated space H^*, we can apply this operator A like on the left to construct another bra

Action on the left (continued...)

$$\langle\phi|A = (\phi_1^* \ \phi_2^* \ \cdots \ \phi_n^*) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

since $\langle\phi| \in \mathcal{H}^*$

This operation is defined much simpler in matrix representation.

it is again the multiplication of two matrices: (the vector row which represents our initial functional $\langle\phi|$ (bra phi) and the matrix of the operator A, when you multiply a row by a matrix, you obtain another row, this is what happens here. $\langle\phi|A)$ is a row too (The action of A on the left is a matrix multiplication where A stands on the right & its argument on the left of it)

Matrix Element

- When this $\langle\phi|A$ acts on some vector psi $|\psi\rangle$, in the matrix representation, we can write it like this:

$$(\langle\phi|A)(|\psi\rangle) = (\phi_1^* \ \phi_2^* \ \cdots \ \phi_n^*) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}$$

- Row $\langle\phi|$, multiplied by A, then by column psi $|\psi\rangle$

- Since it doesn't matter in which order we are going to rewrite it in Dirac's Notation like this:

$$\boxed{\langle\phi|A|\psi\rangle = \underset{(i)}{(\langle\phi|A)|\psi\rangle} = \underset{(ii)}{\langle\phi|(A|\psi\rangle)}}$$

This thing here is called the <u>matrix element</u> of A corresponding to the vector phi <u>$\langle\phi|$</u> and vector psi <u>$|\psi\rangle$</u>

- This name comes from a single observation, if instead of phi and psi, you take the vectors of the orthonormal basis, with all zeros except one place "i" and "j", then this expression will give you <u>components</u> of matrix A in the row i and column j. So to compute this, we can go two ways first to apply A on the left on phi(i), then compute the scalar product of results if

HERMITIAN ADJOINT:

Now we remember that each bra corresponds to some ket. So $\langle\phi_A|$ also corresponds to some ket $|\phi_A\rangle$.

is there a way to obtain this $|\phi_A\rangle$ from $|\phi\rangle$??

if we think about it, $|\phi_A\rangle$ is defined uniquely by the $|\phi\rangle$ and operator A. as,

$$\boxed{|\phi_A\rangle = A^*|\phi\rangle}$$

in other words, we just defined a way of constructing one vector from another

eg. vector ϕ_A from vector ϕ

& the way of constructing one vector from another is an operation ∴ OPERATORS TRANSFORM VECTORS TO VECTORS (*)

(*) So there must exist some operator A^* which transforms vectors, just like the way we did with ϕ and ϕ_A. We call it A^* to stress on the fact that this operator is connected to operator A.

$$|\phi\rangle \xrightarrow{*} \langle\phi| \xrightarrow{A} \langle\phi|A = \langle\phi_A| \xrightarrow{*} |\phi_A\rangle$$

THE OPERATOR A^* IS CALLED THE ADJOINED OPERATOR OF OPERATOR A

What can we say about A^*?

- First its linear
- Second it's defined by operator A alone.
- There must be a way of constructing A^* from A. for any linear operator A.

→ The most interesting part is this:

$$\boxed{(\langle\phi|A)^* = A^*|\phi\rangle}$$

Since the $\langle\phi|A$ is the hermitian conjugate of $A^*|\phi\rangle$, it could be written as

(Hermitian conjugate of A acting on the left of bra ϕ is A^* acting on the right of phi).

- This allows us to define operations of Hermitian conjugation on operators

Hermitian Conjugation [ON OPERATORS]

- First, transform the complex numbers to their conjugates.

(1.) $\boxed{\alpha \xrightarrow{*} \bar{\alpha} \xrightarrow{*} \alpha}$

- Second, transform kets to bras. (means vectors to linear functionals.)

(2.) $\boxed{|\phi\rangle \xrightarrow{*} \langle\phi| \xrightarrow{*} |\phi\rangle}$

- third, transform bras to kets (means linear functionals to vectors)

- Fourth, transform operators to their adjoints.

(3.) $\boxed{A \xrightarrow{*} A^* \xrightarrow{*} A}$

and it is very convenient for us to notice that when we perform the operation of Hermitian conjugation on some expression, you have to do two simple things.

Steps for process of Hermitian Conjugation:

(i) Substitute each element & expression by its Hermitian Conjugate.

(ii) re-write all elements in the reverse order.

(The second rule is not strict for scalars, it is usual to write them in the beginning of the expression)

$$(\alpha|a\rangle\langle b|\langle c|\ ABC\ |d\rangle)^* \quad \left\{ \text{LIKE THIS} \right.$$

$$= \bar{\alpha}\ \langle d|\ C^* B^* A^*\ |c\rangle\ |b\rangle\ \{\alpha\}$$

Now that we know how the adjoint operator is defined, it will be good for us to discover, how to obtain its matrix. Imagine we have some operator A & we have its matrix.

$$A^* = \begin{bmatrix} a_{11}^* & a_{21}^* & \cdots & a_{n1}^* \\ a_{12}^* & a_{22}^* & \cdots & a_{n2}^* \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}^* & a_{2n}^* & \cdots & a_{nn}^* \end{bmatrix}$$

→ in the previous episode we considered it as action of A on some vector x, i told you that you can imagine it as a separate action of linear functionals represented by the rows of matrix A. Hermitian Conjugate comes vector rows to

it's exactly what we need to expect from Hermitian Conjugation of a matrix. FOR ANY MATRIX A, ITS ~~CONJUGATE~~ ADJOINT MATRIX A^* IS JUST TRANSPOSED MATRIX A WITH COMPONENTS CONJUGATED.

example,

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$\Rightarrow A^* = \begin{bmatrix} a_{11}^* & a_{21}^* & \cdots & a_{n1}^* \\ a_{12}^* & a_{22}^* & \cdots & a_{n2}^* \\ \vdots & & \ddots & \vdots \\ a_{1n}^* & a_{2n}^* & \cdots & a_{nn}^* \end{bmatrix}$$

It is important to notice that some operators as well as some numbers are neutral w.r.t Hermitian conjugation. The numbers are neutral to it if they are Real with zero imaginary part; The operators are neutral if after the transpostion & conjugation of the components, they stay the same operators.

This type of operators which are neutral to Hermitian conjugation are called,

SELF-ADJOINED or Hermitian Operators.

They are very important in Quantum Mechanics because they represent "observables".

An observable is defined by an orthonormal basis in the state space, now we are saying that an observable is a Hermitian operator?? How is that?

Next Episode

Eigenvalue Equation :-

The eigenvalue equation of an operator is the equation of this type.

$$\boxed{A|\phi\rangle = \lambda|\phi\rangle}$$

Here, lambda is an unknown scalar,
$|\phi\rangle$ is an unknown vector.
& A, is an operator under consideration

To solve the eigen value equation, means to find all possible values of λ for which it can hold.

- And for each such Lambda, (λ), to find the set of vectors which satisfy the ~~equation~~ with this λ.
- All Lambdas (λ) satisfying this equation are called the Eigen values of the operator, the vectors corresponding to those Lambdas are

Properties of Eigenvalues & Eigenvectors:

First, if you have some eigenvector phi corresponding to some eigenvalue λ_1, then for any complex number α, $\alpha\phi$ will also be an eigenvector corresponding to this λ_1.

$$A|\phi\rangle = \lambda_1|\phi\rangle \implies A(\alpha|\phi\rangle) = \lambda_1 \alpha|\phi\rangle$$

To eliminate this ambiguity, we can choose to normalize the vectors which are the solution of this equation.

Now suppose that for some eigenvalue (λ_2), there are p, linearly independent eigenvectors,

then it is quite obvious that any vector constructed as a linear combination of these p eigenvectors is also the solution of the eigenvalue equation with λ_2.

$$\forall\ |\phi_K\rangle \in \{|\phi_i\rangle\}_{i=1}^{p}\ ,\quad A|\phi_K\rangle = \lambda_2|\phi_K\rangle \implies$$

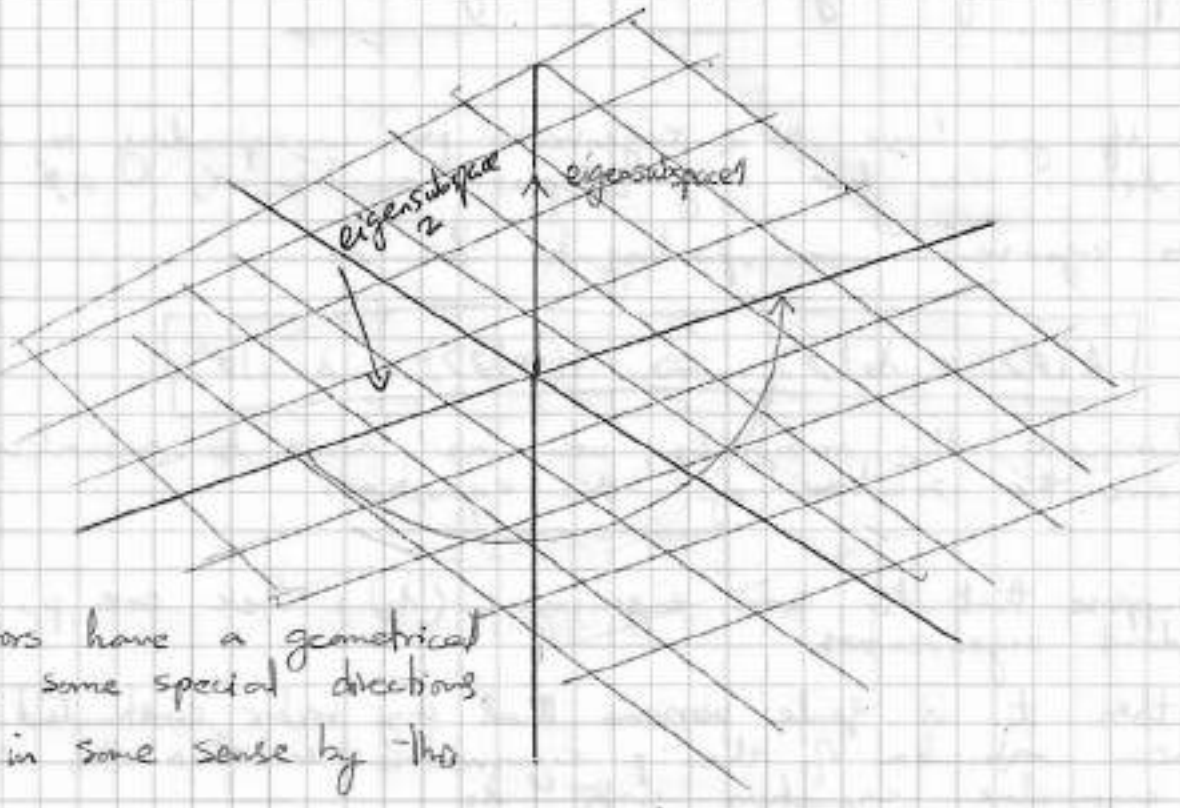
$$\implies A\left(\sum_{i=1}^{p} \alpha_i\ |\phi_i\rangle\right) = \lambda_2\left(\sum_{i=1}^{p} \alpha_i\ |\phi_i\rangle\right)$$

This means that each eigenvalue defines the subspace of the initial space & each vector of this subspace is an eigenvector corresponding to this value.

Eigenvalue which has more than one eigenvector is called a degenerate.

"The degree of degeneracy of an Eigenvalue defines the dimensionality of the eigen subspace"

Example: ROTATION



The eigenvectors have a geometrical meaning of some special directions & touched in some sense by the operator.

- If the operator, for example, rotates the 3D Euclidean space around some axis, then this axis itself would not be touched by this rotation thus it is going to be an eigenvector of such operator with eigenvalue 1.
- Now if this rotation is by an angle ϕ. Then the whole plane orthogonal to this axis preserves the direction of its vectors, they are just multiplied by -1 by this rotation.
  This plane is 2D, which means that this value (eigen) -1 is 2-degenerate in this case.
- and this plane orthogonal to this axis of rotation is 2D eigen subspace corresponding to this value.
- Two different eigenvalues cannot have mutual eigenvectors,

→ In an n-dimensional space, an operator can at most have only n- linearly independent eigenvectors; each such vector corresponds to some eigenvalue, and some of them can correspond to the same degenerate Eigenvalue.

- This whole means that the Eigenvalue quotient of an operator in an n-dimensional space can have at most n- solutions (n- eigenvalues)

Hermitian Operators :-

- The eigenvalue equation is a powerful instrument for operator analysis in general. but from now on, we are going to concentrate on a very special case,
- We will consider only finite dimensional spaces, which we deal with when we consider Qubits, & we are going to examine only Hermitian operators
- Now for Hermitian operators, solutions of Eigen value equation has some additional properties

① "Eigenvalues of an Hermitian Operator are always real."

$$\langle x|A|x\rangle = (\langle x|A)|x\rangle = \lambda^* \|x\|$$

$$\langle x|A|x\rangle = \langle x|(A|x\rangle) = \lambda \|x\|$$

$$A^* = A$$

their complex or imaginary part is 0 always.

② The Eigenvectors of different eigenvalues are mutually orthogonal, this is a very important property: It means - that for a Hermitian Operator in a finite dimensional space, we can construct an orthonormal basis of its eigenvectors. & Even if the some eigenvalues of the operator are degenerate, we still can do that because the Eigen subspace of a degenerate eigenvalue, we can choose any eigen vectors we want.

So we can choose, orthonormal set of vectors there.

"Eigenvectors for different eigenvalues are mutually orthonormal"

$$A|x\rangle = \lambda|x\rangle$$

$$A|y\rangle = \mu|y\rangle$$

$$\langle x|A|y\rangle = \lambda\langle x|y\rangle = \mu\langle x|y\rangle \Rightarrow \langle x|y\rangle = 0$$

each Hermitian operator defines an orthonormal basis, and we remember that each orthonormal basis in the state space defines a set of possible values of the system measurement

"NOW, FINALLY, WE CAN GIVE A STRICT MATHEMATICAL DEFINITION OF AN OBSERVABLE OF A QUANTUM SYSTEM WITH A FINITE DIMENSIONAL

Observable :-

(1) An observable is an Hermitian operator, acting in the state space of a system.

(2) The Eigenvectors of this operator, are the measurement outcomes. They are the states to which the system can collapse after the measurement and when it does, the
(3) classical outcome that we obtain as a result of the measurement, is the eigenvalue which corresponds to that Eigenvector.

WAIT!
we know that the eigenvalues can be degenerates

- so if the system collapses to some vector from the eigen subspace of degenerate eigen value, we obtain only that eigen value & we can tell which vector represents the system now,
- we must admit that in this case, the system collapses not to a single vector, but to the whole eigen subspace,

it is very true, it is much better if you have an observable with all eigen values being non-degenerate.

- But if we don't have one, we can use a set of several commuting observables.

(4) CSCO- Complete Set of Commuting Observables

it can be proved, and this is a fundamental Theorem in quantum Mechanics that if two observables commutes, one can construct an orthonormal basis of their common Eigenvectors

So if you managed to implement a set of commuting observables, such as for each their common eigenvector, corresponds a non degenate eigen value of one of them, we will be able to obtain the most possible information about the state of a Quantum System, using this set of observables. Such sets are called **CSCO - Complete Sets of Commuting Observables**

TIME TO OBSERVE SOME EXAMPLES

Next Page

EXAMPLES

In this lecture we will discover several examples of the hermitian operators

Projection Operator : our first example will be the operator of the following kind

$|\phi\rangle \in \mathcal{H}$, $\|\phi\| = 1$, we choose some unit vector ϕ in our state space. & then in braket notation, we write $|\phi\rangle$ and $\langle\phi|$

$|\phi\rangle\langle\phi|$

ket - bra

Unlike the scalar product, when bra preceeds ket, here we have the reverse order, so it's not a number like in scalar product, but an operator

Let's see how it works,

Consider the action of this operator on some vector ψ from our state space

$|\phi\rangle\langle\phi|\psi\rangle$

Consider the action of this operator on some vector ψ from our state space.

If your write the operator and then vector $|\psi\rangle$

This expression is $|\phi\rangle$ multiplied by scalar product of $\langle\phi|\psi\rangle$ like . When we apply the operator $|\phi\rangle\langle\phi|$ to any vector, we always obtain a vector collinear to ϕ.

- The operator of this kind are called projection operators.
- Since they project the whole space onto just one vector

The matrix representation of such projection operator is a column multiplied by a row

$$|\phi\rangle\langle\phi| = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{pmatrix} \begin{pmatrix} \phi_1^* & \phi_2^* & \cdots & \phi_n^* \end{pmatrix}$$

which gives us the square matrix of the operator.

Now, if you consider a set of mutually orthogonal unit vectors ϕ_i

$$\boxed{P_i = |\phi_i\rangle\langle\phi_i|} \quad , \; i = 1 \dots k \qquad \langle\phi_i|\phi_j\rangle = 0$$

→ for each vector, we can construct a projection

$$\boxed{P = \sum_{i=1}^{k} P_i}$$ ← the sum of these projections is also a projection.

(It projects the whole space onto the subspace generated by the set ϕ_i)

Closure Relation:

If the set ϕ_i forms the orthonormal basis in the considered space, then the sum of all projections P_i becomes the a projection of the space on itself.

Thus it is identity operator

if, $\quad P_i = |e_i\rangle\langle e_i| \quad , \; i = 1, \dots, n \qquad \langle e_i|e_j\rangle = 0$

$$\boxed{P = \sum_{i=1}^{n} |e_i\rangle\langle e_i| = I}$$

This relation which associates the sum of projections to their normal basis and identity is called **CLOSURE RELATION**

And this is very useful for the theorem proving since it allows to substitute identity by the sum of projections at any place of any formula which involves operations.

[WHAT ARE THE SOLUTIONS FOR THE EIGEN EQUATION OF PROJECTIONS

Projections, Eigenvalues:

- $\boxed{(|\phi\rangle\langle\phi|)\,|\phi\rangle = |\phi\rangle\,\langle\phi|\phi\rangle = |\phi\rangle\,, \quad \lambda_1 = 1, \quad \text{degeneracy} = 1}$

for vector ϕ itself, projection on ϕ acts as identity, so ϕ is an eigen vector with eigenvalue 1.

- For any vector which is orthogonal to ϕ, the projection gives us 0.

$$|\psi\rangle \perp |\phi\rangle$$

$$\boxed{(|\phi\rangle\langle\phi|)\,|\psi\rangle = |\phi\rangle\,\langle\phi|\psi\rangle = 0 \quad , \lambda_2 = 0 \; ; \text{degeneracy} = n-1}$$

- which means the second eigenvalue of this operator is 0. The eigensubspace has dimensionality $\boxed{n-1}$
- where n is the dimensionality of the whole space.

You can easily analyze this as any sum of different projections The more linearly independent projectors you take, the more is the degree of degeneracy of the eigen value 1; and less is the degree of degeneracy of the 0.

- The identity is also the sum of projectors and has a single eigenvalue 1, which is n degenerate.

Operator X

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

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

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

(like NOT-Gate in boolean Algebra)

- Now, let's consider the operator called X Matrix of the operator X is to the left
- This is a Quantum Analogue to the classical NOT Gate.
- If you apply X to vector $|0\rangle$, you obtain $|1\rangle$ & vice versa.
- Note that X is a Hermitian Operator
- What are the Eigen Values & Eigen vectors of this operator?

Well since it flips $|1\rangle$ and $|0\rangle$, it is obvious that it preserves the states, which contains these vectors in the same proportions.

$$X|+\rangle = X\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

$$X|-\rangle = X\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|-\rangle$$

The state $|+\rangle$ is an eigen vector with eigenvalue 1

The state $|-\rangle$ is an eigen vector with value -1.

Explanation

$$X|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\right)$$

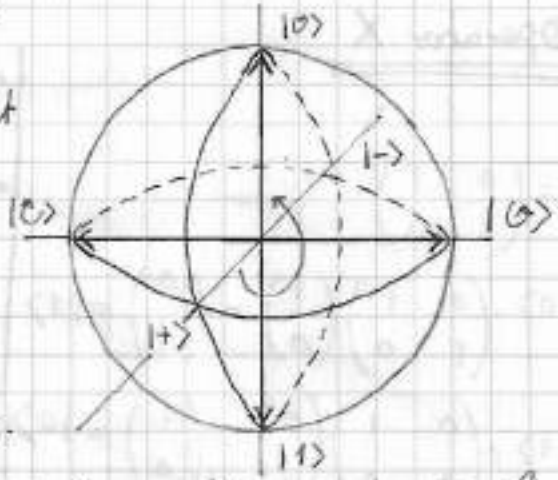
$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}1\\0\end{pmatrix}\right)$$

$$= -\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\right) = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\boxed{X|-\rangle = -|-\rangle}$$

X is just not just an important operator, it is also a good observable (since, it doesn't have degenerate eigen values)

- X is a 2×2 matrix, which means that it acts in a 2D space. Two dimensional space is the state space of one Qubit.
- And Qubit can be represented as a point on the Block Sphere. So let's see how X acts Geometrically on the Block Sphere.



- Vectors $|+\rangle$ and $|-\rangle$ are untouched by it's action.
- Vector $|0\rangle$ comes to $|1\rangle$ and $|1\rangle$ to $|0\rangle$
- Rotational states $|0\rangle$, $|0\rangle$ also flip.
  $|0\rangle + i|1\rangle$ goes to $|0\rangle - i|1\rangle$ & vice versa.
- Operator X is just a rotation around the x-axis on the angle π. & it is so indeed.
- operator X is rotation Around axis X. (looks like the name of the operator was not chosen at random) We have two more Y & Z. Maybe there are rotation

Of course, we have rotation operators for Y & Z too.
they are called Pauli Matrices

Pauli Matrices: (each Pauli Matrix is observable with all eigenvalues being nondegenerate)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- X operator rotates the space around x-axis, by the angle π.
- Y operator rotates the space around y-axis, by the angle π.
- Z operator rotates the space around z-axis, by the angle π.

Eigenvalues & eigenvectors for Y & Z

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} =$$

$$Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix}$$

$$Y|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 0 \\ i \end{pmatrix} + \begin{pmatrix} -i \\ 0 \end{pmatrix}\right)$$

$$=$$

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

Hadamard transform

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

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

$$\boxed{H|0\rangle = |+\rangle}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$\boxed{H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle}$$

$$H|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$H|+\rangle = \frac{1}{2}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

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

$$H|+\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\boxed{H|+\rangle = |0\rangle}$$

$$H|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \frac{1}{2}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

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

$$\boxed{H|-\rangle = |0\rangle}$$

$$H|-\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\boxed{H|-\rangle = |1\rangle}$$

This H is called Hadamard Transform (Jacques Hadamard)
This transforms $|0\rangle$, $|1\rangle$ basis into the Hadamard Basis.
& vice versa. (A lot of algorithms employ this operator)

$|+\rangle$, $|-\rangle$ are Hadamard Basis.

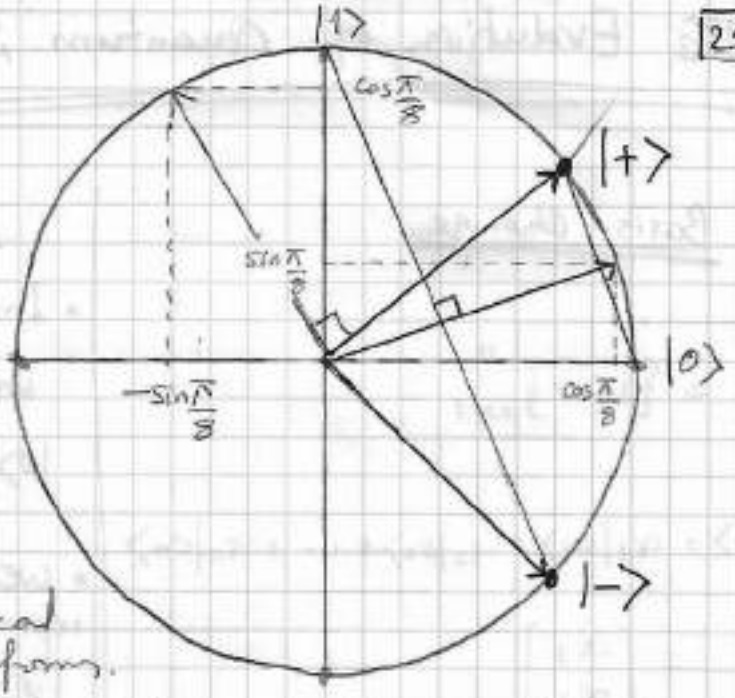
Eigenvalues & Eigenvectors on the next Page!

Hadamard Transform

eigenvalues & eigen vectors

To find that out, you can choose two ways:

a) To solve a characteristics equation for eigen values and reach two systems of linear equations with 1 unknown parameter.



On this picture is Geometrical interpretation of Hadamard Transform.

|0> is mapped to |+>
|1> is mapped to |−>
} it is easy to see that both actions are reflections along the direction pointed in ///

- The vectors collinear to this direction are not modified by the Hadamard Transform
- The vector has angle $\frac{\pi}{8}$ with |0> vector so its easy to compute its components.

$$\cos\frac{\pi}{8} \text{ and } \sin\frac{\pi}{8}$$

- its Eigenvalue is 1. We are now experienced enough to expect that the second eigenvector is orthogonal to the first one.
- $\sin(-\frac{\pi}{8})$ and $\cos(\frac{\pi}{8})$ ← components of 2nd eigen vector
- Hadamard Transform maps it to itself multiplied by −1.

So, we can conclude that the second Eigenvalue is −1

* and no eigenvalues of the HADAMARD TRANSFORM are degenerate.
- Thus, the Hadamard Transform also represents the complete set of <u>hermitian</u> observables.

The Evolution of Quantum Systems :-

Basis Change

$E = \{|e_i\rangle\}_{i=1}^{n}$

$|\phi\rangle = \alpha_1|e_1\rangle + \alpha_2|e_2\rangle + \cdots + \alpha_n|e_n\rangle$

$$= \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$$

$S = \{|s_i\rangle\}_{i=1}^{n}$

- Imagine we have some vector $|\phi\rangle$ we have also the representation of $|\phi\rangle$ in some orthonormal basis
- we are interested in that what representation will have this vector $|\phi\rangle$ in another basis say S. with vectors $s_1, s_2, \ldots, s_n$.
- Lets represent $|\phi\rangle$ as a sum of its components multiplied by the vectors of the basis E.

$$|\phi\rangle = \sum_{i=1}^{n} \alpha_i |e_i\rangle = \sum_{i=1}^{n} \alpha_i I |e_i\rangle \quad \text{—(i)}$$

- we just placed identity operator inside this sum since the identity change nothing.

- As we remember that the identity operator can be substituted by the sum of projections.

$$\boxed{\sum_{j=1}^{n} |s_j\rangle\langle s_j| = I} \quad \text{—(ii)}$$

so eq(i) after substitution of eq (ii) becomes.

$$|\phi\rangle = \sum_{i=1}^{n} \alpha_i \left(\sum_{j=1}^{n} |s_j\rangle\langle s_j| \right) |e_i\rangle$$

(iii) — $\boxed{|\phi| = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{n} |s_j\rangle \langle s_j|e_i\rangle}$ ← This last step is justified by the closure relation.

If you observe (iii), you will find out that there is no more vectors of basis e in it as $\langle s_j|e_i\rangle$ is a scalar product.

We are going to rewrite equation (iii) and represent the whole thing as a column vector but now in basis S.

$$|\phi\rangle = \begin{pmatrix} \sum_{i=1}^{n} \alpha_i \langle s_1|e_i\rangle \\ \sum_{i=1}^{n} \alpha_i \langle s_2|e_i\rangle \\ \vdots \\ \sum_{i=1}^{n} \alpha_i \langle s_n|e_i\rangle \end{pmatrix}$$

Not good enough

← Representation in S

$$|\phi\rangle = \underbrace{\begin{pmatrix} \langle s_1|e_1\rangle & \langle s_1|e_2\rangle & \cdots & \langle s_1|e_n\rangle \\ \langle s_2|e_1\rangle & \langle s_2|e_2\rangle & \cdots & \langle s_2|e_n\rangle \\ \vdots & & & \vdots \\ \langle s_n|e_1\rangle & \langle s_n|e_2\rangle & \cdots & \langle s_n|e_n\rangle \end{pmatrix}}_{U} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

↑ Representation in E.

- Now we have a convenient way of representing any vector in basis S.
- If we have column representation in any basis E, we can apply this matrix & obtain column representation in basis S.
- So U is our **matrix of basis change**

REVERSE OPERATION (Reverse Basis Change)

Suppose we have a vector C in the S representation & we want to obtain the components of C in the E representation.

$$\psi = \begin{pmatrix} \sum_{i=1}^{n} \psi_i \langle e_1|s_i\rangle \\ \sum_{i=1}^{n} \psi_i \langle e_2|s_i\rangle \\ \vdots \\ \sum_{i=1}^{n} \psi_i \langle e_n|s_i\rangle \end{pmatrix} = \begin{pmatrix} \langle e_1|s_1\rangle & \langle e_1|s_2\rangle & \cdots & \langle e_1|s_n\rangle \\ \langle e_2|s_1\rangle & \langle e_2|s_2\rangle & \cdots & \langle e_2|s_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle e_n|s_1\rangle & \langle e_n|s_2\rangle & \cdots & \langle e_n|s_n\rangle \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}$$

$U^{-1} = U^{\dagger}$

representation in E ↑ representation in S.

Since we have this basis conversion matrix U, it is really easy to do.

Before applying it to the vector psi ($|\psi\rangle$), we first need to calculate its adjoint. (That is to transpose it & to conjugate its components)

U^*, the adjoint of U is always reverse.

$$UU^* = U^*U = I.$$ (U^* conceals the actions of U and U conceals the actions of U^*)

Unitary Operators

The operators, who's adjoints are also their reverse are called unitary operators.

$$UU^* = U^*U = I$$

- They transform an orthonormal basis to an orthonormal basis.
- They don't change the lengths of vectors.
- They also preserve the angles.

Examples: ROTATIONS, REFLECTIONS

Important Point: "Any evolution of a Quantum System except for the measurement is described by a unitary Operator"

- It means that when we are going to perform computations on our quantum states, (that is to modify them), we are only allowed to perform unitary transforms. We cannot apply any linear operator we want. All quantum gates we can implement are unitary.
- Quite a strong restriction, sometimes there is a strong desire to implement a gate which is not unitary.
- eg to copy & an unknown quantum state, we just can't.

It is a fundamental law & we can't break it.

- Physically, this means, that one can't distinguish the evolution of a quantum system from evolution of its environment.
- Basis change and it is what the system does when it evolves can be

For example,

Consider a qubit, encoded by photon polarization, then it doesn't matter whether we rotate the photon polarization axis by the angle θ, or we rotate our analyzer by the angle $0 - \theta$. The result of both these actions is the same.

UNITARY OPERATORS

What about the quantum gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

can we use them in quantum Computing?

- Are they unitary?
- Yes, they are! it could be checked by computing the adjoints & performing some matrix multiplications.
- All these quantum gates are self adjoint

Conditional NOT (CNOT, CX)

Another unitary Hermitian Operator (CX, CNOT)

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

$$\begin{aligned} CNOT\ |00\rangle &= |00\rangle \\ CNOT\ |01\rangle &= |01\rangle \\ CNOT\ |10\rangle &= |11\rangle \\ CNOT\ |11\rangle &= |10\rangle \end{aligned}$$

- if first bit is 0, the next one stays unchanged.
- if first bit is 1, the next one flips.
- CNOT is a 4×4 matrix, which means that it acts in the state space of two qubits.
- it modifies the value of second qubit based on the value of the first qubit. It flips qubit 2 if qubit 1 is in the state 1.
- Entanglement operations which in some sense make qubits interact, without this kind of unitary transforms, we can only perform the trivial computations. This quantum gate is our gate to the world of almost unlimited computing power. Unfortunately, this is the gate whose physical

- As an exercise, check its unitarity.
- As more exercises, find its eigenvalues and eigenvectors.

WEEK-5

QUANTUM COMPUTING - LESS FORMULAE MORE UNDERSTANDING

1. No-Cloning Theorem
2. SWAP Operator
3. Quantum Teleportation
4. Quantum Cryptography Protocols
5. BB84
6. E91.

Week plan:-

(1) Quantum Teleportation: (Quantum Data Transmission)

a. No-cloning theorem. (Forbids copying of an "Unknown quantum state")

b. Quantum Algorithms description.

c. Quantum Swap.

(2) Quantum Cryptography:

a. BB84

b. E91

No-Cloning Theorem:-

Q: Can you copy quantum Data?
that is the state of a Quantum System:

Q: What does it mean to copy?

Making a copy means is very close to making an observation.

When you observe a text, "you make a copy of it inside your brain". OR when we make a copy of something from one computer to another, it is like the first computer has observed what was stored by the first computer.

- Observation is a very sensible process in quantum Mechanics. Observation alters the system for us.

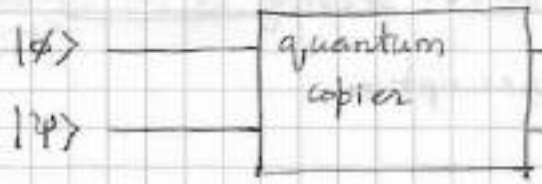
So, is there a way of copying the state of a system without touching it.

- ONLY IF we created a state, we can possibly create it once more but this is not like copying the quantum data. It is more like following the recipe for the state creation. but the recipe itself is classical.
- However, if we don't know the quantum state & there is no recipe to reproduce it, the situation becomes worse, we can't read quantum states without altering them.

without destroying it.

- We ourselves want to observe it, let the other quantum system observe it for us.

- We learned that the evolution of a quantum system is ed unitary,



∴ Making Copies of ∴
∴ Quantum Data ∴

- It means that the state of a quantum system is transformed as if it is modified by some unitary operator

- Now we have two systems;
  (i) $|\phi\rangle$: state of our interest, the state that we want to copy.
  (ii) $|\psi\rangle$: the recipient system, the system which will receive the copy of $|\phi\rangle$

Now, $|\phi\rangle$ & $|\psi\rangle$ are transferred to some quantum copier, which does all the magic for us, such as after it, we have two systems in the state $|\phi\rangle$.

— Copier is not unitary because it glues up two different states.
— Not unitary transforms are not allowed by Quantum mechanics.

This result, the impossibility of copying of an unknown quantum state is known as the No-Cloning theorem.

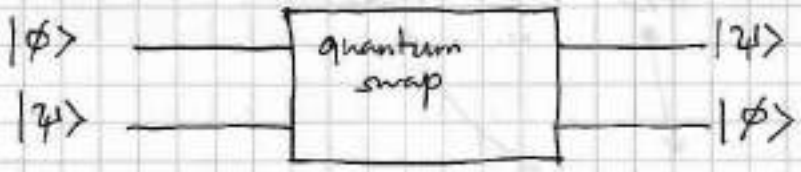
The theorem was formulated and proved independently by James Park, Wooters, Zurek, Dicks (1980) (1970)

"If you doubt the possibility of some procedure in quantum mechanics, the first thing is to check is the unitarity of this procedure"

is the transform unitary?

No!, Because it destroys the information about the state $|\psi\rangle$. Thus it doesn't preserve angles, since states $|\phi\rangle|\psi_1\rangle$ & $|\phi\rangle|\psi_2\rangle$ are both transformed to $|\phi\rangle|\phi\rangle$.

Quantum Swap:

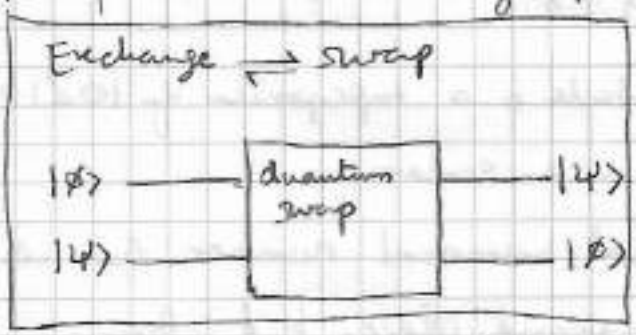


Now, let's consider the upper scheme.

- You can notice that in this case, the state $|\psi\rangle$ isn't destroyed, but there is no copying of state $|\phi\rangle$ either.
- This procedure of swapping of states is indeed unitary & thus possible.
- It is even possible if these two systems are very far from each other.
- The quantum state transfer in this case, when the physical systems don't interact with each other is called teleportation of a quantum state.
- The impossibility of copying of an unknown quantum state is a serious obstacle for many things we would like to do with quantum data.
- It is not the first time when an obstacle becomes a very useful source.
  - Classical cryptography uses practically & decidable tasks in it's asymetric algorithms Quantum cryptography does with no cloning theorem.

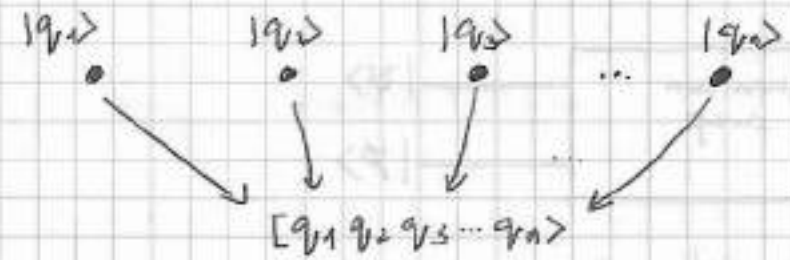
SWAP Operator:-

Now we know that we can't copy quantum states, but we can transfer them & exchange them.



- Let's suppose one quantum particle, that carries the state $|\phi\rangle$, the other particle carries the state $|\psi\rangle$
- We want to design an algorithm that carries state $|\psi\rangle$ to upper particle & state $|\phi\rangle$ to the lower particle. This procedure is called as swap. it must be implemented with some unitary transform U. Before designing this transform, we must agree about the notation.

Notation:



We have several particles, each carrying one qubit, then mathematically, the state of the system containing all these particles is a Tensor product of the all the qubits carried by them

- One qubit is a 2D vector, 2 qubits are described by a 4D vector.
- Tensor Product is not commutative (it means that the order in which we place qubits matters.
- Once we choose an order, we must retain it during the whole reasoning / computation.

(1st) → (last)

Step 1: we enumerate the considered particles. (Left) → (Right)

~~first~~ for example, this state describes 5 qubits.

- $|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle = |01101\rangle$

Quantum

This state describes 5 qubits carried by 5 two level systems.

Dimensionality of this vector = $2^5 = 32$.

For classical computation, we can read this state as a # encoded in binary numeral system (13).

- The following state also describes 5 qubits

$$\frac{1}{\sqrt{2}} |0\rangle \underbrace{(|0\rangle + |1\rangle)}_{\text{the state of 2nd particle is a superposition of } |0\rangle \& |1\rangle} |1\rangle|0\rangle|1\rangle$$

- The coefficient of this superposition $\frac{1}{\sqrt{2}}$ is a scalar.
- This state doesn't encode any classical numeral number for us.

because of this superposition in the second place. but when we measure the state in $|0\rangle|1\rangle$ basis, this superposition will collapse & we will obtain a vector which will encode a binary number $|00101\rangle$ or $|01101\rangle$

Now we agree how we write down the qubits carried by enumerated particles, it is time to arrange the way we will describe quantum algorithms.

Quantum Algorithm :-

* it is a set of unitary operators applied to the state. previous week, we considered several examples of unitary operators,

Unitary Operators

Pauli Matrices: X, Y, Z ; } → One Qubit Gate.

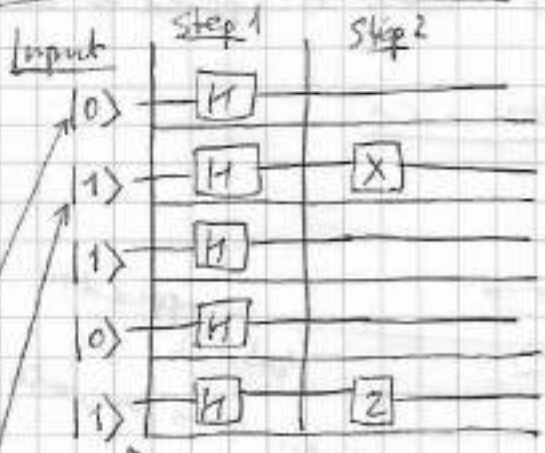
Hadamard Matrix: H

CNOT = CX — (2 Qubit Gate)

- We may want to apply these one, two qubit gates to one separate qubits in our multi qubit state

- So we want a way of describing what operators we want to apply, to which qubits, and in which order

NOTATION ... The Input



$|0\rangle\ |1\rangle\ |1\rangle\ |0\rangle\ |1\rangle = |01101\rangle$

- Here's a straight forward way of doing it.
- We are going to describe the algorithms as 2D schemes or tables.
- On the first column we write the input state (qubit by qubit)
  the state of the first particle on the top, second and then so on (L → R)
- Then from left to right we are going to place operators or quantum gates which we are going to apply to the corresponding qubits

Each column here corresponds to a step in our algorithm. and the row where we write down the gates, corresponds to the Qubits to which this gate is applied.

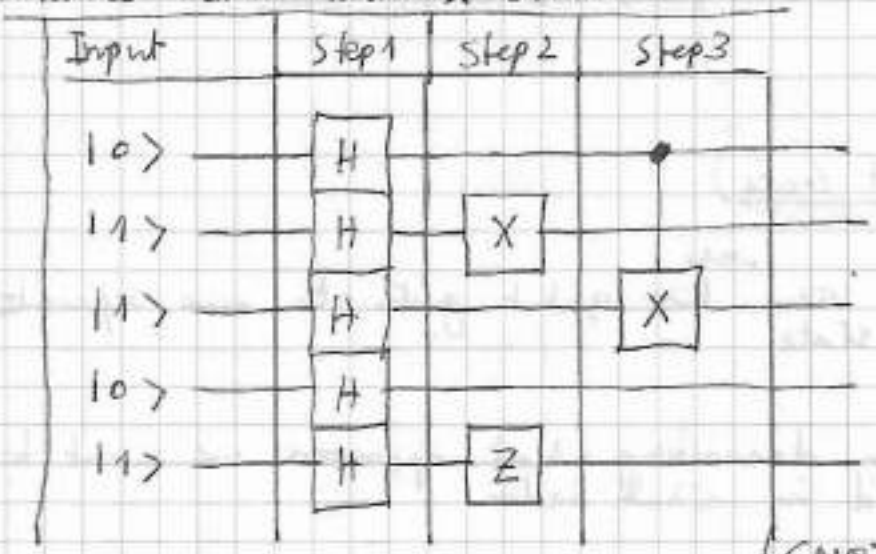
- In this algorithm, we apply Hadamard Gate to all 5 qubits.
- 2nd step we apply X gate to qubit #2; and Z gate to qubit #5.
- Pretty clear & straight forward with 1 qubit gates, but we can create

such as CX (or Controlled NOT [CNOT])

- CNOT acts on two qubits, one of them is control and other controlled. The controlled qubit flips the state when control qubit is in the state 1.

$$CX|00\rangle = |00\rangle$$
$$CX|01\rangle = |01\rangle$$
$$CX|10\rangle = |11\rangle$$
$$CX|11\rangle = |10\rangle$$

In our scheme, we will represent the control qubit with a thick dot • (the one that is reason for the state flip) while the controlled qubit with X Gate.



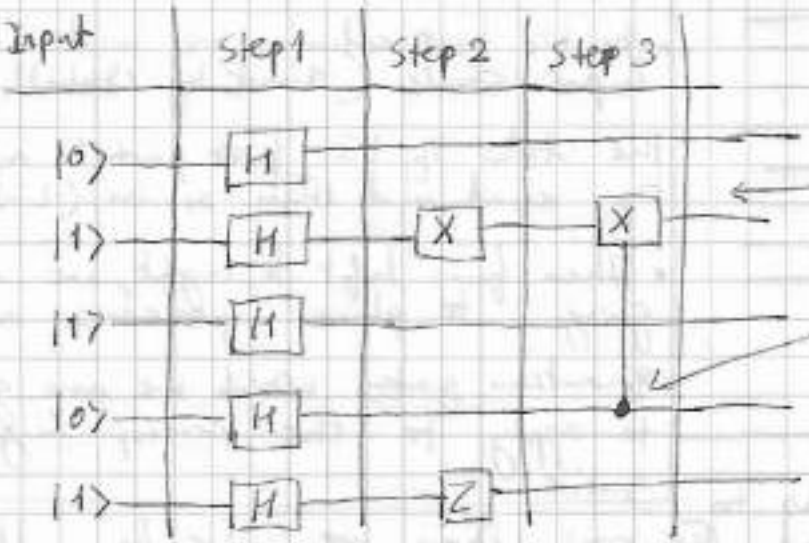
one will connect the dot and the X gate with a line for better clarity

• This notation means that the gate X is applied to the qubit # 3 if qubit 1 is in the state 1.

(CNOT – CX)

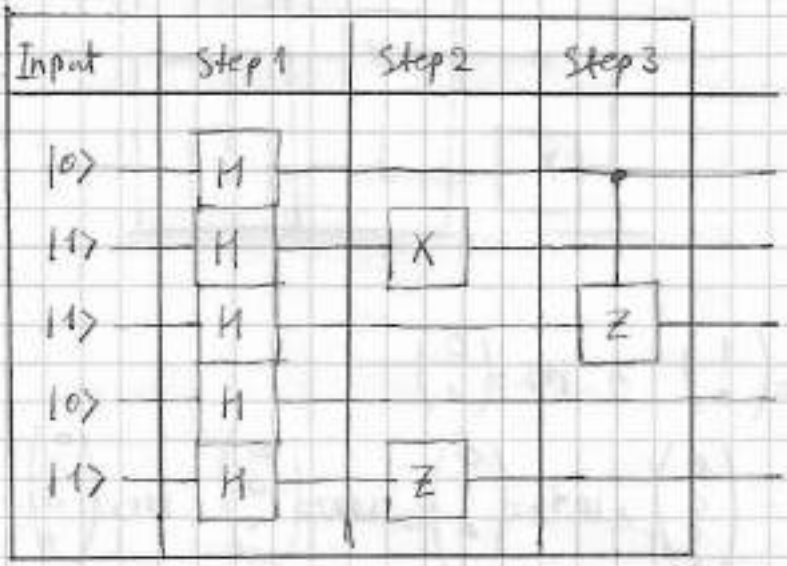
and in the following scheme, Gate X is applied to Qubit #2 if Qubit 4 is in the state 1.

(CNOT – CX)



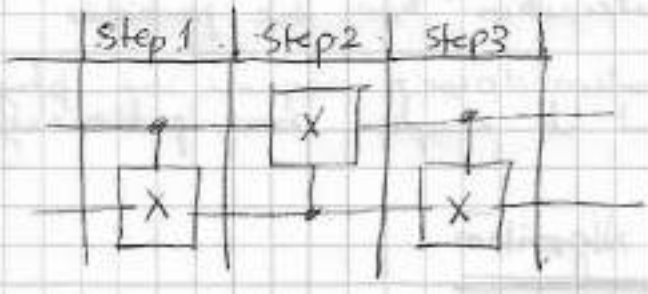
CNOT-(CZ)

In this scheme, qubit the gate Z is applied to Qubit 3 if qubit 1 is in state 1.



{ We can construct this kind of controlled gate from any one Qubit gate }

Quantum Swap Algorithm (Circuit)



{ The algorithm which implements the swapping of two qubits consists of these three sequential CNOTs }

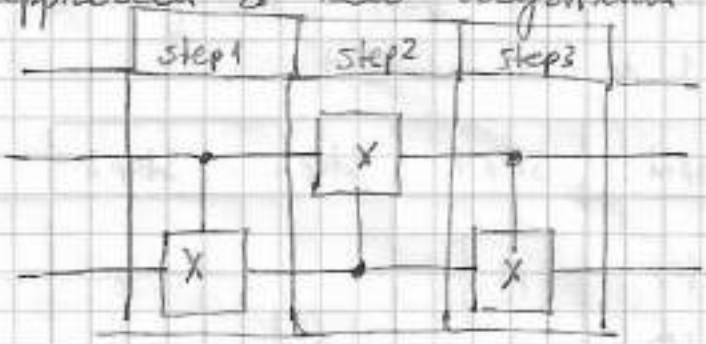
SWAP |00⟩ = |00⟩
SWAP |01⟩ = |10⟩
SWAP |10⟩ = |01⟩
SWAP |11⟩ = |11⟩

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

Does not touch the last vector & first vector

Quantum Teleportation

Now we are ready to approach a new algorithm called "quantum Teleportation."



SWAP $|00\rangle = |00\rangle$

SWAP $|01\rangle = |10\rangle$

SWAP $|10\rangle = |01\rangle$

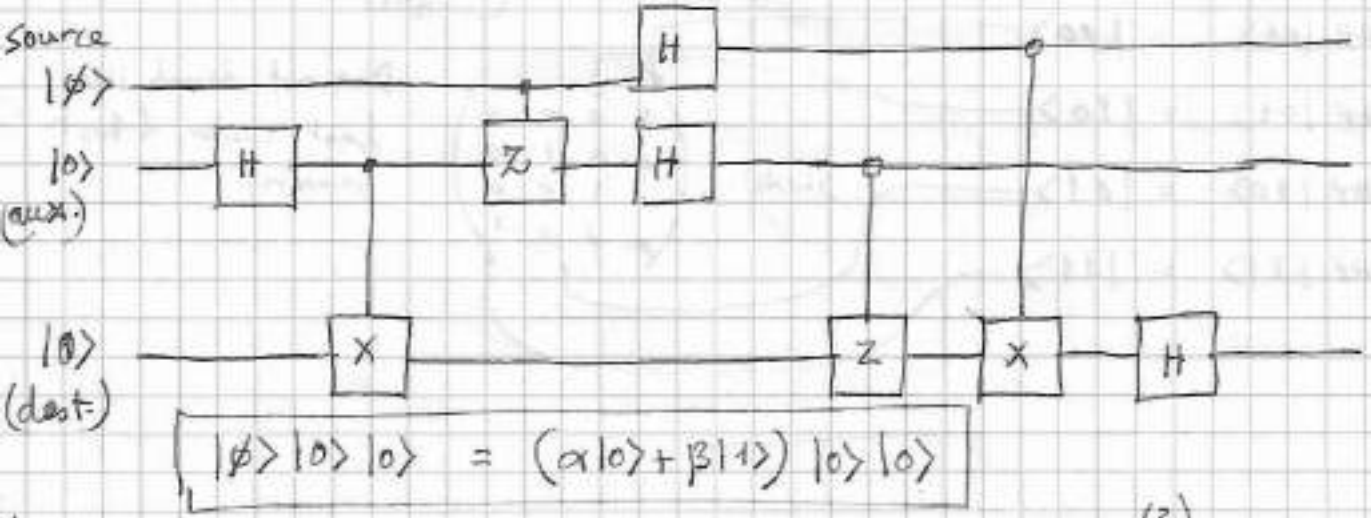
SWAP $|11\rangle = |11\rangle$

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

- The quantum swap algorithm allows us to change the state of two separate particles.
- It requires the particles to interact during this algorithm. because we apply three sequential CNOT operators. & implementation of CNOT involves the physical interaction b/w the particles.
- The quantum Teleportation doesn't require the physical interaction during such swap, but it needs some preliminary preparations.

Teleportation Algorithm



$$|\phi\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle$$

Here is the scheme of the algorithm, we have three (3) qubits here, The first qubit is in some unknown state $|\phi\rangle$ which is a superposition of $|0\rangle$ & $|1\rangle$ $\{\alpha|0\rangle + \beta|1\rangle\}$ α, β are unknown. This is the state that we are going to transfer. 3rd qubit is in the state

and represents the particle which will receive the state $|\phi\rangle$, after the application of our algorithm.

- The second qubit is in state $|0\rangle$ & it is an auxiliary particle which we'll need for our algorithm.
- This algorithm includes several steps

STEP 1:

(1.) The first step is preliminary, it requires an interaction b/w the second auxiliary & 3rd recipient particle.

After this preliminary step, the auxiliary particle must be delivered to the source particle with the state $|\phi\rangle$, the third particle can be moved as far as we want.

Let's assume that during this preliminary step, all three particles are in the same laboratory.

Their states can be written as $|\phi\rangle$, $|0\rangle$, $|0\rangle$.

$$|\phi\rangle\,|0\rangle\,|0\rangle = (\alpha|0\rangle + \beta|1\rangle)\,|0\rangle\,|0\rangle \xrightarrow{H}$$

$$\xrightarrow{H} (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|0\rangle + |1\rangle)|0\rangle \xrightarrow{CX}$$

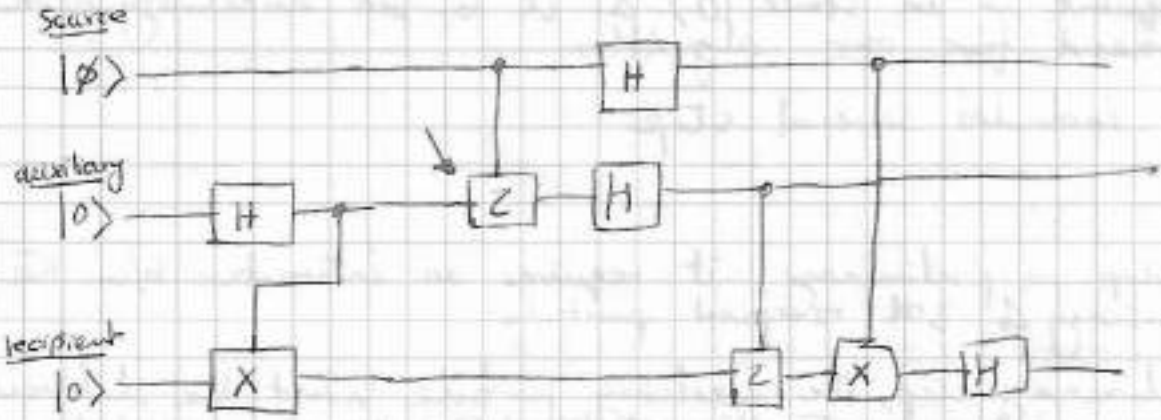
$$\xrightarrow{CX} \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) \leftarrow \text{Bell's state}$$

Entanglement of 2nd and 3rd

Quantum Entanglement is an instrument we are going to use to transfer the quantum state at a very long distance

- For an entangled state we cannot write down separate state for the particles.
- Now particle 2 & 3 donot have separate state but an entangled state. but the particles (THEMSELVES) are separate.
- NOW we can put particle (3) in some isolated container which prevents its interaction with the environment and we can give this (preserves the state) container to a cosmonaut who is ready to start his journey to Mars. He is now at Mars after several months & he sets a camp & now he needs the state $|\phi\rangle$. There is no way we can send him the first particle which holds this ~~state~~ state.

This leads us to the next step in our algorithm.



$$|\phi\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle$$

$$\xrightarrow{H} \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|0\rangle + |1\rangle)|0\rangle$$

$$\xrightarrow{CX} \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$ ← Bell's state (entanglement of 2nd & 3rd particle)

↓ recipient

first particle $|\phi\rangle$ has not interacted with any particle, 3rd recipient particle is on Mars Now its time for us to form this entangled state.

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

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

It will entangle first particle with other two

$$\xrightarrow{CZ} \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle)$$

After this the whole state will be entangled & no particle amongst these three will have its own state.

for the clarity (we opened brackets first & then applied CZ)

- (CZ) changes sign of one vector that has 1st and second component of the vector as 1's.

Now the state of these particles are entangled They are in some sense connected however the particle #3 is very far away

Next step next page

This next step of algorithm asks us to apply Hadamard transform to first & second particles.
it isn't a very challenging task

Hadamard action.

$$\xrightarrow{CZ} \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle\right)$$

$$\xrightarrow{HH} \frac{1}{\sqrt{2}}\left(\alpha\frac{1}{2}\left(|000\rangle + |010\rangle + |100\rangle + |110\rangle\right) + \alpha\frac{1}{2}\left(|001\rangle - |011\rangle + |101\rangle - |111\rangle\right) + \beta|100\rangle - \beta|111\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(\frac{1}{2}\left[\alpha|000\rangle + \alpha|010\rangle + \alpha|100\rangle + \alpha|110\rangle + \alpha|001\rangle - \alpha|011\rangle + \alpha|101\rangle - \alpha|111\rangle + 2\beta|100\rangle - 2\beta|111\rangle\right]\right) \quad (3)$$

$$|011\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|1\rangle$$
$$= \frac{1}{2}\left(|001\rangle - |011\rangle + |101\rangle - |111\rangle\right)$$

$$|000\rangle = \frac{1}{2}\left(|0\rangle+|1\rangle\right)\left(|0\rangle+|1\rangle\right)|0\rangle$$
$$= \frac{1}{2}\left(|000\rangle + |010\rangle + |100\rangle + |110\rangle\right)$$

Check again??

$$= \frac{1}{2\sqrt{2}}\left(\alpha|000\rangle + \alpha|010\rangle + \alpha|100\rangle + \alpha|110\rangle + \alpha|001\rangle - \alpha|011\rangle + \alpha|101\rangle - \alpha|111\rangle + 2\beta|100\rangle - 2\beta|111\rangle\right)$$

$$= \frac{1}{2\sqrt{2}}\left((\alpha+\beta)|000\rangle + (\alpha+\beta)|010\rangle + (\alpha-\beta)|100\rangle + (\alpha-\beta)|110\rangle + (\alpha-\beta)|001\rangle + (\beta-\alpha)|011\rangle + (\alpha+\beta)|101\rangle - (\alpha+\beta)|111\rangle\right) \quad (4)$$

Next step asks us to measure particles 1 & 2 in 0,1 bases

When we measure two particles, we obtain four different results

No expression (4) needs regrouping

(next page)

first qubit

$$= \frac{1}{2}\Big(|00\rangle \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) +$$

$$|01\rangle \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle - \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) +$$

$$|10\rangle \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) +$$

$$|11\rangle \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle - \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right)\Big)$$

* if the measurement of first two we obtain the value $|00\rangle$ the third qubit (which is on Mars) will evolve to this state

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

which is not $|\phi\rangle$ but is pretty close to it.

if our cosmonaut wants state $|\phi\rangle$ out of it, he needs first to apply Hadamard Transform onto it

$$H\left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) = (\alpha|0\rangle + \beta|1\rangle) \quad \text{—(1)}$$

* if the measuremat gives us $|01\rangle$, the state is close to $|\phi\rangle$ & slightly different from previous one.

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

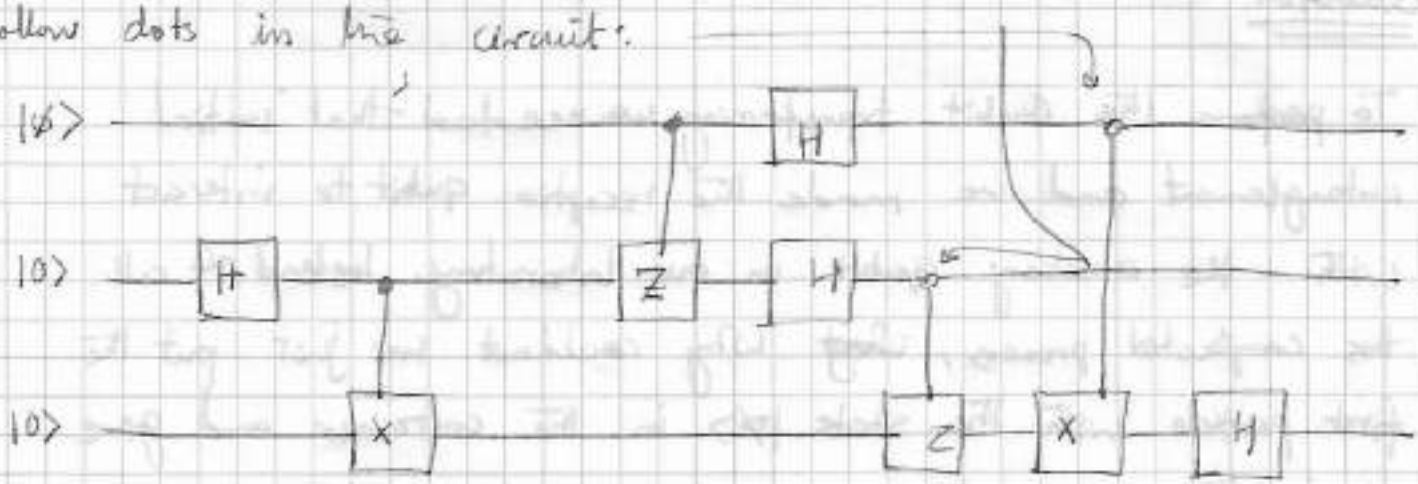
$ZH \rightarrow |\phi\rangle$.

if cosmonaut applies Z gate to the container & then the state becomes same as (1) which could be turned to $|\phi\rangle$ with application of H gate.

$|10\rangle \rightarrow \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right)$ | XH to obtain $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$|11\rangle - \frac{(\alpha-\beta)}{\sqrt{2}}|0\rangle - \frac{(\alpha+\beta)}{\sqrt{2}}|1\rangle$ | ZXH to obtain $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

The uncertainty in cosmonaut's behaviour is emphasized by the hollow dots in the circuit.



The gate operator Z and X, which the cosmonaut needs to apply to his state depending on our measurement result are not conditional like CNOT or CZ; they are simple one qubit operators. But they are controlled by a phone call.

- The measurement of 1st two particles changes changes the state in the cosmonaut container immediately.

The distance doesn't matter in entanglement, but to obtain exactly what he wants ($|\phi\rangle$), the cosmonaut needs to contact us and to know our measurement result.

- Quantum Teleportation allows us to transfer information faster than speed of light? (Definitely not true) we need classical communication to finish the proces & to obtain exactly the same state in the reception qubit as it was in the source qubit.

Question:

To perform the Qubit transferring we needed that initial entanglement and we made the reception qubit to interact with the auxiliary qubit in our laboratory. Instead of all this complicated process, ~~that~~ why could not we just put the first particle with the state $|\phi\rangle$ in the container and give it to the cosmonaut?

Answer..

We could of course, but imagine ~~to the time of~~ that to the time of the spaceship start, the state $|\phi\rangle$ was not yet calculated.
The first particle doesn't take place in the preliminary procedure, we, so, can't prepare it further, even when the third particle is very far. The connection to this third particle, is stored in the second auxiliary particle, and as soon as we are ready, we entangle our state $|\phi\rangle$ with it & thus create the connection of all three of them.

This reasoning explains that the quantum algorithm of quantum teleportation indeed allows us the transfer of quantum data, which couldn't be performed without it.

QUANTUM CRYPTOGRAPHY

- Quantum teleportation is an interesting phenomenon but given the state of current systems, it is not really needed
- On the other hand there are quantum algorithms that are very important even today.
- We have learned that it is not possible to make a copy of an unknown quantum state (No-cloning Theorem)
- This a restriction, but as we see that this restriction becomes an opportunity for the field of cryptography.

- Protecting the message from Eve is not good enough. Alice needs to provide a possibility to Bob to read the encrypted message aswell.

- Lets say Alice & Bob had a chance to meet & they developed a secret key and if the length of key is not less than the length of the message, alice can encrypt the message securely.

RSA
factoring complexity

BB84
no-cloning theorem

↳ Based on computational assymetry of multiplication & factoring
→ For quantum computing both tasks (multiplication, factoring) are easy which makes RSA unbreakable for a large enough dlc (Peter Shor 1994)

but in 1984, 10 years before RSA became useful, two US scientists Charles Bennett and Gilles Brassard invented their cryptographic protocol which is absolutely safe for the shared key creation and distribution. Thanks to No cloning theorem

BB84 (Bennett, Brassard – 1984)

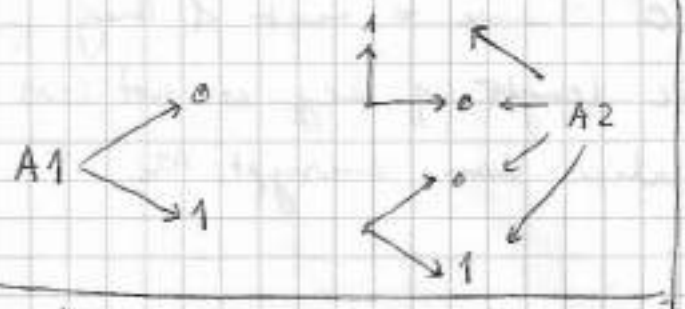
A1 = 0 0 1 1 0 ...
A2 = 0 1 1 1 0 ...

B1 = 1 0 0 1 1 ...

Alice ——— communication channel ———→ Bob

Step 1 : Photons Generation

- The polarization of this photon is defined by the corresponding bit of the sequence A2.
- If the bit from A2 sequence is 1, then she polarized the photon vertically, and horizontally other wise



- If the bit in the sequence A1 is 1, then Alice creates a photon in Hadamard basis
- If the bit in the sequence A2 is 1 → polarize along |+⟩ otherwise |−⟩
- For each photon generated by Alice it is random in two senses
  (i) its basis is random, its value
  (ii) its value in this basis is also random
- Each generated photon, Alice sends to Bob via this communication channel

if A1 == 0:
  if A2 == 0 => horizontal polarization
  if A2 == 1 => vertical polarization
if A1 == 1:
  ~~A2 → Hadamard basis~~
  if A2 == 1 → polarize along |+⟩
  else → polarize |−⟩

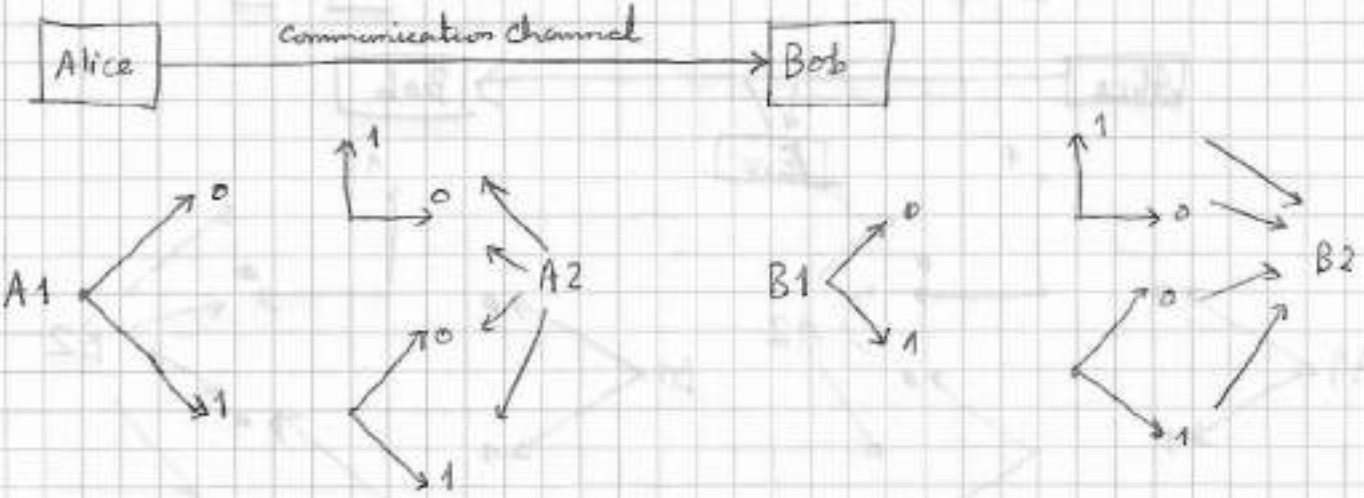
Step 2:

A1 = 0 0 1 1 0 ⋯

A2 = 0 1 1 1 0 ⋯

B1 = 1 0 0 1 1 ⋯

B2 = 0 1 0 1 1 ⋯



- When Bob receives a photon from Alice, he doesn't know its polarization.
  - So he takes 1 bit from his Random segments B1, if the bit is 0, Bob measures it in 01 basis.
  - if the bit is 1 → Bob measures the photon in Hadamard basis
- Now if the corresponding bits in the A1 and B1 sequences appear to be equal, then the photon which was generated using this bit, bob guesses the right measurement basis and he obtains the correct bit for the sequence A2 generated by Alice.
- For those bits which differ in A1 & B1, Bob obtains completely random result for the measured bit.

" BUT AT THIS STEP: BOB DOES NOT KNOW WHICH BITS ARE CORRECT AND WHICH AREN'T."

- so he carefully saves all his measurement results

B1 =	1	0	0	1	1	⋯		A1 =	0	0	1	1	0	⋯
B2 =	0	1	0	1	1	⋯		A2 =	0	1	1	1	0	⋯

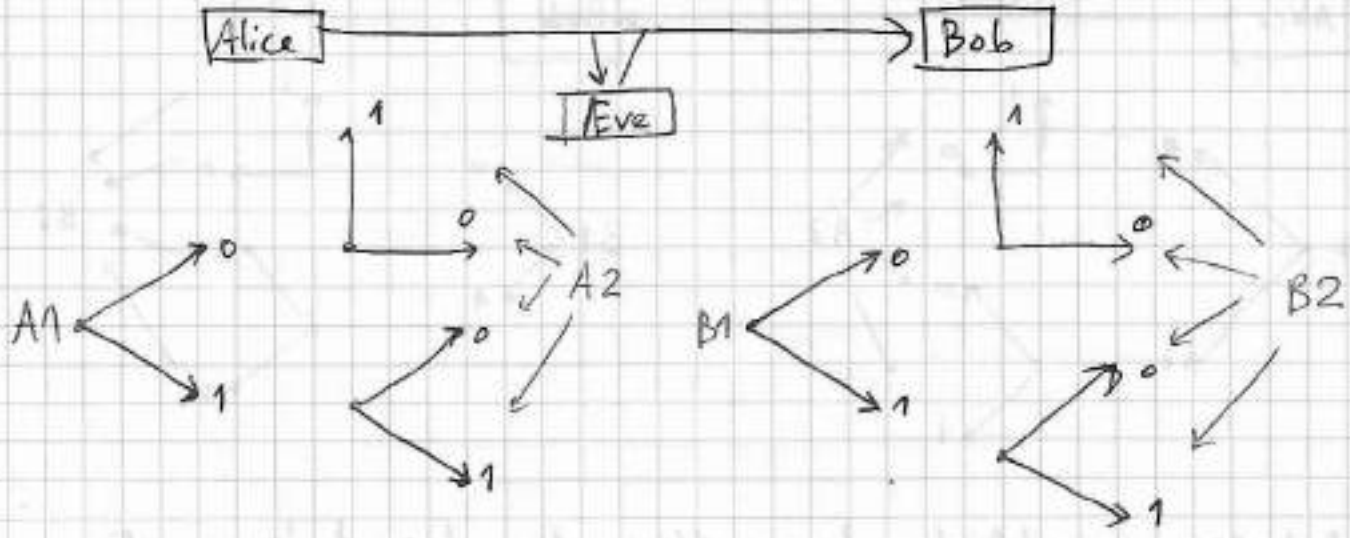
Step 3:

- on step 3, Alice calls Bob using some open & insecure communication channel, and she sends him her A1 segments. (The only requirement

for this channel is that Alice & Bob must be sure that they are talking to each other and not with eve

A1 = 0 0 1 1 0 ...
A2 = 0 1 1 1 0 ...

B1 = 1 0 0 1 1 ...
B2 = 0 1 0 1 1 ...



- Eave may only eavesdrop this channel,
- When Bob has A1 sequence, he knows which photons he measured in correct basis, he then returns to alice the number of photons which he measured correctly, but not the result of the measurement.
- After this step, both Alice and Bob share some bits from A2 sequence & they both know which bits these are.
  Now they have shared secret key composed of these bits.
- ~~[illegible]~~
- What can Eve possibly do?
  1st she could intercept the photons sent by Alice, there is no way she can intercept just a part of the photon, (because they are indivisible). So if she gets a photon, Bob gets nothing & thus Alice & Bob will soon find out that some photons sent by Alice were lost: If this situation happens, they will know that there is an intruder & their key was not generated. But she must send a photon to Bob if she could duplicate the photon, then she might send a duplicate copy of photon to Bob that she received. but it's not possible, thanks to the no cloning theorem. The best thing she can do is to measure the photon & the problem with that is

that eve doesn't know which basis to choose, because she doesn't know the basis chosen by Alice to polarize the photon. She also doesn't know the basis which Bob will choose for his measurement.

Let's count the odds

Eve chooses correct basis : $P1 = \frac{1}{2}$ (win)

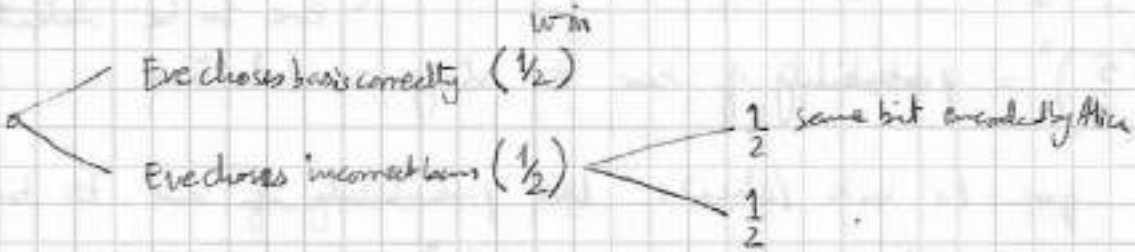
Eve chooses incorrect basis : $P2 = \frac{1}{2}$

- Eve has correct bit : $P3 = \frac{1}{2}$
- Bob has correct bit. $P4 = \frac{1}{2}$ (win)

$$P = P1 + P2*P3*P4 = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

- If, for some photon, Bob doesn't get the basis chosen by Alice correctly, then in the step 3 this photon will be eliminated from consideration by Alice & Bob (No matter what Eve did with this photon)
- So we only have to consider the photons for which Alice & Bob have chosen the same basis.

  For each such situation, there are two possibilities



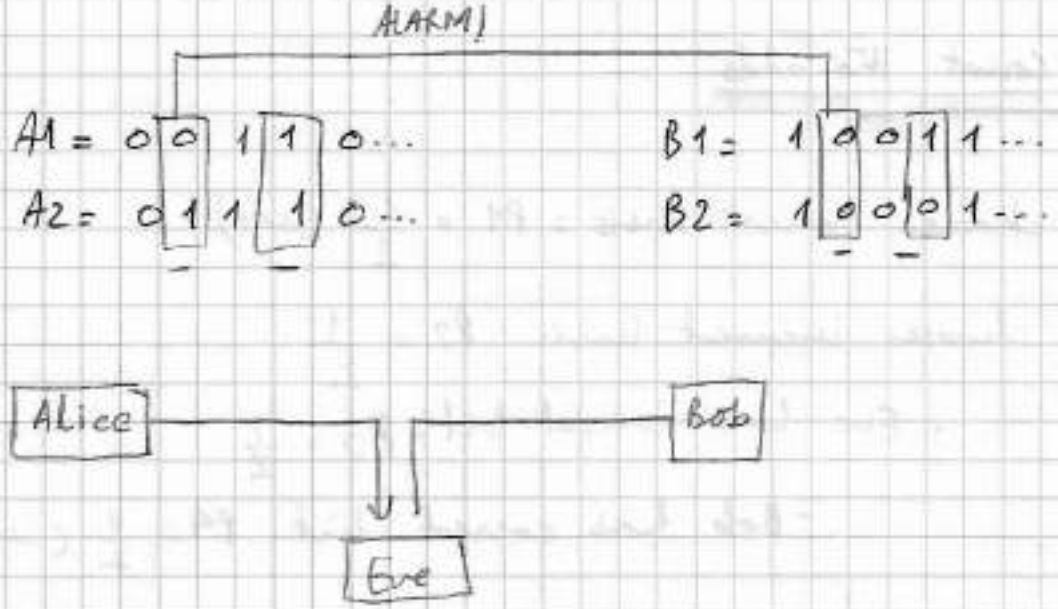
$P = \frac{5}{8}$ (is probability for eve for one bit)

but there are many thousands bits and for eve to obtain all correct bits, the likelihood is very small

Tot. Prob. $= (5/8)^{\#\text{ of bits}}$ (# of intrusions) and intercepts correctly)

Step 4

Final step / Final check



- Alice & Bob have now some shared secret key but they don't know yet if it's similar, because they don't know yet if Eve has interfered or not.
- So they decide to choose some random bits of their shared key & compare them over the open insecure channel.
- This is the final check which easily reveals the actions of Eve.
- The more bits Alice & Bob choose to check, the less is the probability for Eve to be undetected (more is probability for Eve to be detected)

$\left(\frac{5}{8}\right)^n$ = probability of Eve to stay undetected

for 10 bits/checks the probability of eve to become detected becomes $100 - \left(\frac{5}{8}\right)^n \times 100 = 99.09\,\%$

- The bits choosen for the check are removed from the shared key.
- If Eve were detected some bits of the shared key appear to be different at Alice & Bob, then Alice & Bob agree that the key was not generated and they have to repeat the whole procedure again. If the check has passed, alice & bob can be sure that they now have an identical shared key which no one else has.

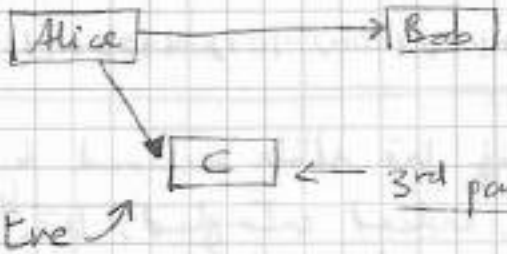
Quantum Cryptographic Protocol

E91

Polish-British — Artur Konrad Ekert — 1991 — E91 Protocol

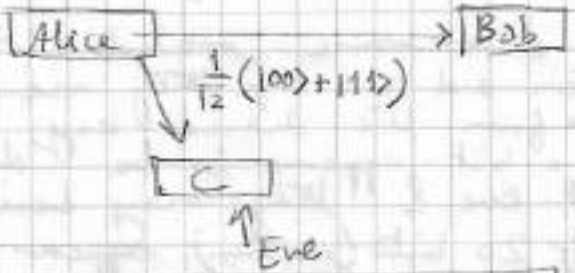
Ekerts thing is simpler

- However it requires the possibility to create pairs of entangled photons, and it has flexibility of moving some of the work of key creation to a third party.
- Lets see everything for ourselves.
  - Alice can delegate the task of key creation to 3rd party
  - Main Advantage: Alice doesn't even have to trust this third party.
  - She along with Bob can always check if there was an intrusion



Now Eve infiltrates the key creation centre as one of its employees.

- Alice, asks the C to create a key to be shared with bob of 2000 bits in length.



- For each bit, C creates a pair of entangled photons in the state $(|00\rangle+|11\rangle)$,
- One of this photon goes to Bob & another to Alice.
- A wonderful property of these bells state is when Alice & bob measure their photons in the 0, 1, basis, they both have the same result, and this result they have is completely random so even the key creation centre does not know it.

- For 2000 random bits, C must create 2000 entangled pairs & send them to Alice & Bob & it is as simple as that.

- Eve can still intrude.

Since its not good for her if Alice & Bob have pairs of entangled electrons ..

She decides to cheat.

→ She can randomly prepare states 00, 11 for each bit & then sends photons to Alice & Bob. so they would still have the same result for each measurement, but Eve would know it since she prepared them.

→ How can alice & bob know this attack? very simple.

- Each time they both get their photons, they agree about the measurment basis.
- With probability 0.5 they either choose 0,1 basis or the Hadamard Basis for each photon pair.
- For this agreement, they could use any insecure channel.

Attack Detection

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{HH} \frac{1}{2\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle + |00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

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

$$|00\rangle \xrightarrow{HH} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$|11\rangle \xrightarrow{HH} \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

- if the state received by Alice & Bob is indeed entangled, then in Hadamard basis, it's just $|++\rangle$, $|--\rangle$, & when Alice & Bob both measure the state in H basis, they both obtain the same results

- but if alice & bob receive the state $|00\rangle$, for example, then in the Hadamard basis, they will both have plus, plus, minus, & probability for them to obtain same measurement result just becomes $\frac{1}{2}$.
- So after Alice & Bob receive & measure 2000 bits, they can randomly choose & check some of them and see if they are equal. The more bits they check, & remove from the shared key, the more confidence they gain, if some bit appears to be different in Alice & Bob's key, then they detect Eve & they may decide to change the key creation center. Even if 20 bits (random) appear to be equal, they can 99% be sure that there was no intrusion & they have the perfect shared key that nobody else has.

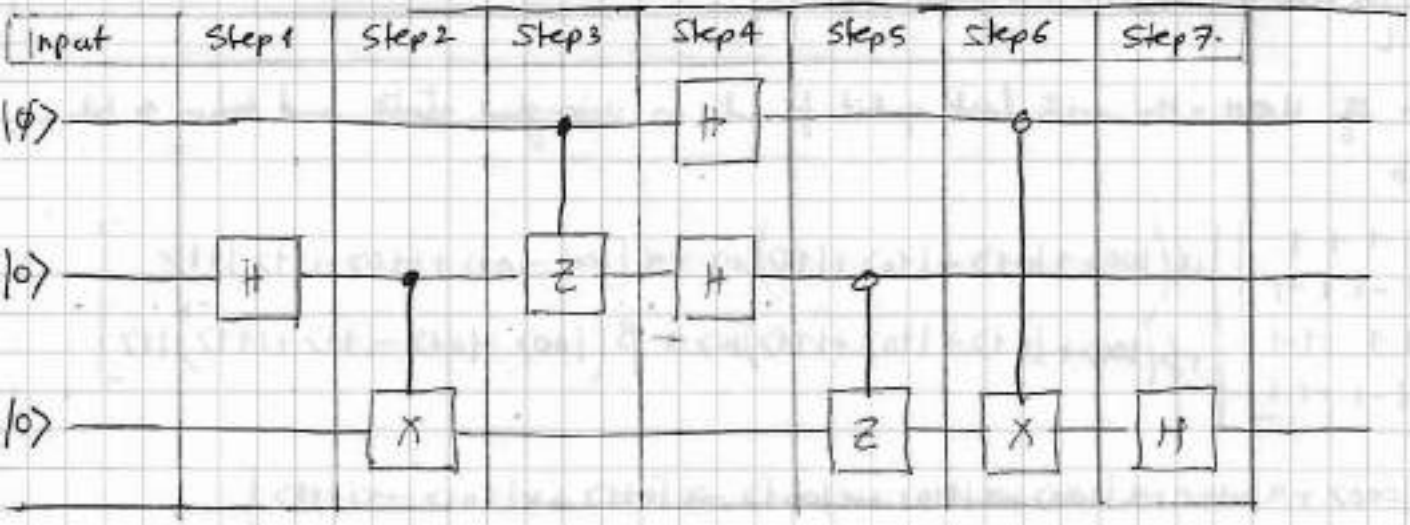
END-END

SPBSU Russia
Dr. Sergey Bozhenov

Next Recommended Course: "Introduction to Quantum Computing"

Supplementary :

Quantum Teleportation Circuit Explained



Identities / values.

parallel wires : Tensor product ⊗

series wires : Matrix Product

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \; ; \; |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \; ; \; |01\rangle = |0\rangle \otimes |1\rangle = |0\rangle|1\rangle.$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \quad , \quad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad , \quad Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$CX = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \quad , \quad CZ = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix}$$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Input :

$$= |\phi\rangle|0\rangle|0\rangle \quad \leftarrow \text{Tensor product}$$

Step 1 (H-Action)

$$= |\phi\rangle H|0\rangle|0\rangle = |\phi\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}|\phi\rangle(|00\rangle + |10\rangle)$$

Step 2 (CX-Action)

$$= \frac{1}{\sqrt{2}}|\phi\rangle CX(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}|\phi\rangle(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Step 3

$$= CZ\left[\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right] = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle)$$

Step 4 (HH:-Action)

$$= \frac{1}{\sqrt{2}} H_4 \left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle\right]$$

Application of $H \otimes H = H_4$ with last qubit fixed in entangled state and Action on first two qubits

$$= \frac{1}{\sqrt{2}} \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} \alpha\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)|0\rangle + \alpha\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]|1\rangle \\ +\beta\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)|0\rangle - \beta\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right)|1\rangle \end{bmatrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} \alpha|000\rangle + \alpha|010\rangle + \alpha|100\rangle + \alpha|110\rangle + \alpha|001\rangle - \alpha|011\rangle + \alpha|101\rangle - \alpha|111\rangle \\ +\beta|000\rangle + \beta|010\rangle - \beta|100\rangle - \beta|110\rangle - \beta|001\rangle + \beta|011\rangle + \beta|101\rangle - \beta|111\rangle \end{bmatrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} (\alpha+\beta)|000\rangle + (\alpha+\beta)|010\rangle + (\alpha-\beta)|100\rangle + (\alpha-\beta)|110\rangle + (\alpha-\beta)|001\rangle - (\alpha-\beta)|011\rangle \\ +(\alpha+\beta)|101\rangle - (\alpha+\beta)|111\rangle \end{bmatrix} \quad \text{(i)}$$

Step 5, 6, 7 These steps require us to measure the particle in $0, 1_s$ bases

When we measure two particles, we obtain four different results. for next, we will regroup eq(i) as follows.

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} (\alpha+\beta)|000\rangle + (\alpha-\beta)|001\rangle \\ +(\alpha+\beta)|010\rangle - (\alpha-\beta)|011\rangle \\ +(\alpha-\beta)|100\rangle + (\alpha+\beta)|101\rangle \\ +(\alpha-\beta)|110\rangle - (\alpha+\beta)|111\rangle \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} |00\rangle\left[(\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\right] \\ +|01\rangle\left[(\alpha+\beta)|0\rangle - (\alpha-\beta)|1\rangle\right] \\ +|10\rangle\left[(\alpha-\beta)|0\rangle + (\alpha+\beta)|1\rangle\right] \\ +|11\rangle\left[(\alpha-\beta)|0\rangle - (\alpha+\beta)|1\rangle\right] \end{bmatrix}$$

moving $\frac{1}{\sqrt{2}}$ to inside of the bracket

$$= \frac{1}{2} \begin{pmatrix} |00\rangle & \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) \\ |01\rangle & \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle - \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) \\ |10\rangle & \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \\ |11\rangle & \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle - \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \end{pmatrix}$$

- if we get $|00\rangle$ in our measurment in Lab

the third qubit which is far far away will evolve to

$$\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

which is some what close to $|\phi\rangle$

the person far away just needs to apply H onto it to get the original sunset state

- for $|01\rangle \Rightarrow \frac{\alpha+\beta}{\sqrt{2}}|0\rangle - \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$

then cosmonaut needs to apply Z and then H to reach $|\phi\rangle$

- for $|10\rangle \Rightarrow \frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle$

first X and then H to reach $|\phi\rangle$

- for $|11\rangle \Rightarrow \frac{\alpha-\beta}{\sqrt{2}}|0\rangle - \frac{\alpha+\beta}{\sqrt{2}}|1\rangle$

first Z, then X, then H to reach $|\phi\rangle$.

THE MEASUREMENT PROBLEM

Questionaire sent to Physicists:

How do you understand the measurement problem?

(1) It is a pseudo problem (17%)

(2) It is solved by Decoherence (29%)

(3) It is/will be solved some other way (16%)

(4) It is a severe difficulty (6%)

(5) I don't know (32%)

DECOHERENCE

In quantum mechanics, we describe a system by a wave function, that is a vector, it can be expanded in a basis, which is a set of vectors of length 1.

The wave function is usually denoted with a Greek letter ψ.

$$|\psi\rangle = a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + \dots$$

- coefficients $a_n, \forall n \in \mathbb{N}$ could be complex numbers.

Simplest case $|\psi\rangle = a_1|1\rangle + a_2|2\rangle$ → Values of an observable that you could measure

Once you have expanded the wave function in the basis belonging to the measurement outcomes, then the square of the coefficients for basis vectors gives you the probability of getting the measurement outcome.

$$\boxed{\begin{aligned} p(|1\rangle) &= a_1 a_1^* \\ p(|2\rangle) &= a_2 a_2^* \end{aligned}} \quad \left\{ \text{Probabilities of measuring } |1\rangle \text{ \& } |2\rangle \text{ resp.} \right.$$

eg $$\boxed{a_1 = \underbrace{\frac{1}{\sqrt{2}}}_{} \Rightarrow \underbrace{a_1 a_1^* = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}}_{} = \frac{1}{2} \hat{=} 50\%}$$

Since the $\boxed{\sum p_i = 1.}$ } Absolute squares must add upto 100%

$$\Rightarrow \boxed{a_1 a_1^* + a_2 a_2^* = 1}$$

- If you have a state that is in superposition of possible measurement outcomes, you never measure that superposition. you only measure one or the other.

But the coefficients can be complex numbers:

$$\Rightarrow \boxed{|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}} e^{i\theta} |2\rangle}$$

θ: phase

$$\Rightarrow \boxed{e^{i\theta} = \cos\theta + i \sin\theta}$$

Now to take into account that the superposition is not the only thing in our system. we prepare a state at some initial time, and then it travels to the detector. A detector is a device, that amplifies a signal. A little quantum particle comes in at one end & a number comes out at the other end.

- This means that the superposition that we want to measure interacts with many other particles both along the way to the detector & in the detector. This is what you want to describe with <u>decoherence</u>.
- These constant little bumps that the superposition has to endure, are described in an easy way is that each bump changes the phase of the state (θ) by tiny little bit.
- To see what effect it has if you do great many of these little bumps, we first have to calculate the density matrix of the <u>WAVE FUNCTION</u> (it will become clear later why?)
-

the density matrix ρ is ket-bra product of the wave function with itself:

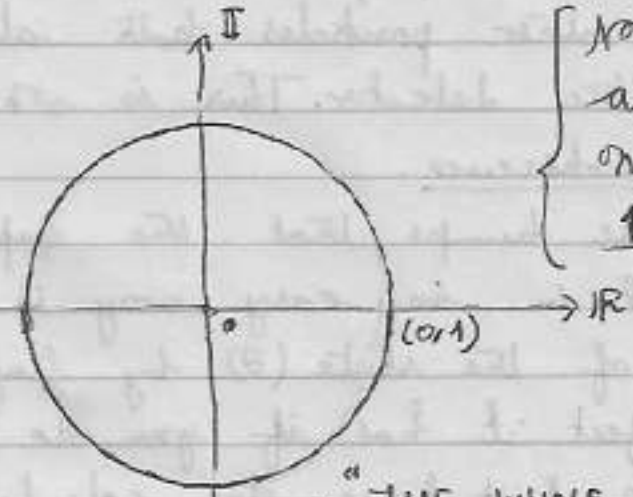
$$\rho = |\psi \times \psi| = \begin{pmatrix} a_1 a_1^* & a_2 a_2^* \\ a_1 a_1^* & a_2 a_1^* \end{pmatrix}$$

eg. $$|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}} e^{i\theta}|2\rangle$$

$$\Rightarrow \quad \rho = \begin{bmatrix} 1/2 & \frac{1}{2}e^{-i\theta} \\ \frac{1}{2}e^{i\theta} & 1/2 \end{bmatrix}$$

Each time this particle bumps into some other particle, this phase θ slightly changes (randomly), and what you actually measure is the average over all those random changes.

- So understanding decoherence comes down to averaging this complex number. To see what goes on helps if we draw this complex plane.



On this circle, you therefore find all the numbers of the form $e^{i\theta}$ with $\theta \in \mathbb{R}$

Now, every number with absolute value of 1 lies on this circle with radius 1

if $\theta \in [0, 2\pi]_{Rd}$ you go once around the circle. [Euler's Formula]

"THE WHOLE MAGIC OF DECOHERENCE IS IN THE FOLLOWING INSIGHT"

→ If you randomly select points on the circle & average over them, then the average, will not lie on the circle, instead, will converge to the middle of the circle. which is at Zero.

Let's see the density matrix again.

$$\rho = \begin{bmatrix} 1/2 & \frac{1}{2}e^{-i\theta} \\ \frac{1}{2}e^{i\theta} & 1/2 \end{bmatrix}$$

if we average over these random kicks, then the off-diagonal entries go to zero (0). Nothing happens with the diagonal.

That is DECOHERENCE.

- REASON THIS IS CALLED DECOHERENCE? The random changes to the phase destroy the ability of the state to make an interference pattern with itself. If you randomly shift around the phase of a wave you don't get any pattern

A state that has a well defined phase and can interfere with itself is called "coherent"

- But the terminology isn't the interesting part, the interesting bit is what has happened with the density matrix.

$$\rho' = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

$\therefore$ { looks completely unremarkable, just a matrix with some entry on the diagonal and 0 on off diagonal.

"But what's interesting is that there is no wave function that will give you this density matrix"

$$\rho = |\psi \times \psi| = \begin{pmatrix} a_1 a_1^* & a_1 a_2^* \\ a_2 a_1^* & a_2 a_2^* \end{pmatrix}$$

for $a_1 a_2^* = 0$, has to be zero.

but then, one of the diagonal entries is also zero, which isn't what the decohered Density Matrix ρ' looks like.

So, the matrix we got after decoherence, no longer corresponds to the a wave function. That's why we use density matrices in the first place. Every wave function gives you a density matrix.

But not every density matrix gives you a wave function

$$|\psi\rangle \longrightarrow |\psi \times \psi| = \rho$$

and $$\rho \not\longrightarrow |\psi \times \psi| = |\psi\rangle$$

} If you want to describe how a system loses coherence you therefore need to use density matrices.

What does this density matrix ρ' after decoherence describes?

→ It describes classical probabilities. The diagonal elements describes the probability for each of the possible outcome of measurements like in quantum Mechanics.

but quantum-ness of the system, that was in the ability of the wave function to interfere with itself has gone away with the off-diagonal entries.

- Decoherence converts quantum probabilities to classical probabilities.
- It therefore explains why we never observe any quantum behavior in ~~on~~ everyday life.
- It is because this quantum behaviour goes away very quickly with all the many interactions that every particle constantly has, whether or not you measure them.
- Decoherence gives you the right classical probabilities but it doesn't tell you what happens with the system itself. To see this, keep in mind, that density matrix in general doesn't describe a collection of particles or a sequence of measurements. It might well just describe one single particle. & after you've measured the particle, it is with probability 1, either in $|1\rangle$ state or in the $|2\rangle$ (other).
- But this correspond to a density matrix which has one diagonal entry 1, & all other entries as zero.

- The state after measurement is not in 50/50 probability state (that isn't a thing). [Decoherence doesn't tell you what happens with the system itself, it merely gives you probabilities after what you observe. This is why Decoherence only partially solves the measurement problem. It tells you why we don't normally observe quantum effects for large objects. It doesn't tell you however, how it

happened that a particle ends up in one and only one possible measurement outcome.