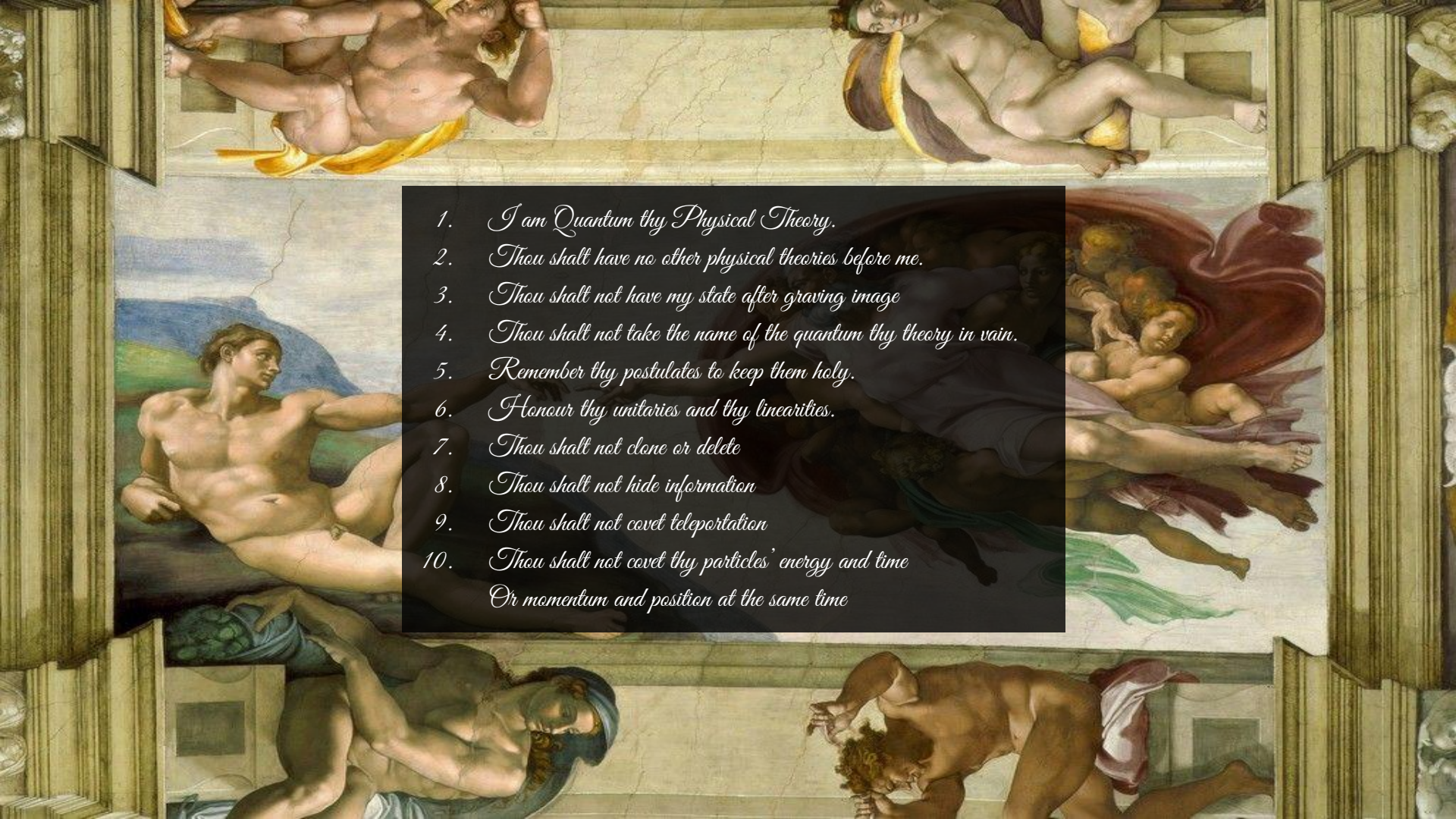




Ψ

Ten Quamandents



- 
1. *I am Quantum thy Physical Theory.*
  2. *Thou shalt have no other physical theories before me.*
  3. *Thou shalt not have my state after graving image*
  4. *Thou shalt not take the name of the quantum thy theory in vain.*
  5. *Remember thy postulates to keep them holy.*
  6. *Honour thy unitaries and thy linearities.*
  7. *Thou shalt not clone or delete*
  8. *Thou shalt not hide information*
  9. *Thou shalt not covet teleportation*
  10. *Thou shalt not covet thy particles' energy and time  
Or momentum and position at the same time*

# Introduction

Alapan Chaudhuri and Zeeshan Ahmed

April 30, 2021

- On Formulation of Quantum Mechanics
- Implications
- No-go Theorems
- Proof Sketch
- Inference

# On Formulation of Quantum Mechanics

*Quantum Mechanics is really simple once you take the physics out of it.*

- Scott Aaronson

# On the Formulations of Quantum Mechanics

Quantum Mechanics had a really dysfunctional and troubled childhood. And more often than not, we are taught of how it grew rather than what it stands for.

As a by-product, quantum mechanics comes across as some strange physical theory. However, that is no where near the whole picture.

Quantum Theory is just as much (if not more) an extension of Classical Probability – as it is a physical theory that describes the nature of the universe.

# On the Formulation of Quantum Mechanics

Just as Classical Probability Theory, Quantum Mechanics can be fundamentally formulated by pure thought alone without any particular appeal to experiment.

It is what we get upon conserving the  $L_2$  norm rather than the  $L_1$  norm (as in Classical Probability) along with addition of the continuity axiom and the idea of measurement.

Thus, the axiomatic formulation of Quantum Mechanics can be stated as follows.

- The state of a system encodes probability of outcomes in a vector, say  $[\alpha_1, \alpha_2, \dots, \alpha_n]$ , such that  $\sum_{\forall i} |\alpha_i|^2 = 1$ , or that the  $L_2$  norm is preserved.
- There exists a continuous reversible transformation on a system between any two pure states of that system. This is called the axiom of continuity.
- Measurement in a standard basis results in a collapse of the state to whatever outcome is obtained. The outcome is governed by the probability distribution.



Let us not worry about measurement or continuity, for a while, and deal with the idea of preservation of norm.

Classical Probability involves preservation of  $L_1$  norm and thus all associated transformations are required to be  $L_1$  preserving and they are referred to as stochastic matrices.

In case of Quantum Mechanics, all transformations require to be  $L_2$  norm preserving and the matrices which possess this property, upon introducing complex numbers as well, are UNITARY MATRICES!

But what about other norms? Or, is it that God is partial to  $L_1$  and  $L_2$ ?

Turns out that God is indeed partial!

## Theorem

*Let  $T$  be a linear transformation such that it preserves  $L_p$ . Then, if  $T$  is a non-trivial transformation such that it doesn't involve re-shuffling of the elements of the vector – then  $p = 1$  or  $p = 2$ .*

# On Composite Systems

Building upon our major axioms we also need a formulation for building composite systems.

- Associated with every system, exists degree of freedom and dimension.
- Degree of Freedom of a system ( $K$ ) denotes the minimum number of probability measurements needed to determine the state.
- Dimension of a system ( $N$ ) denotes the maximum number of states that can be reliably distinguished from one another in a single shot measurement.
- A composite system consisting of two subsystems  $A$  and  $B$  having dimension  $N_A$  and  $N_B$  respectively, and number of degrees of freedom  $K_A$  and  $K_B$  respectively, has dimension  $N = N_A N_B$  and number of degrees of freedom  $K = K_A K_B$ .

Now, let's see if we can derive some of the idiosyncrasies of Quantum Mechanics from the above mentioned axioms.

Moreover, we shall also discuss the two most basic constraints which serve as the backbone of no-go theorems.

- Linearity
- Unitarity

Any consequences of linearity and unitarity of quantum theory must be respected.

Why do we use complex numbers, instead of real numbers?

The axiom of continuity requires us to operate on a field which is algebraically closed. Thus, we need complex numbers.

In simpler terms, if you want every unitary operation to have a square root, then you have to go to the complex numbers.

Why is quantum computing reversible?

Any quantum gate must thus be implemented as a unitary operator and is therefore reversible.

All operators must be unitary.

Because they must preserve norm.



# Why Linearity?

All transformations must be linear.

When, we stated out our axioms – linearity was implied in the idea of state transformation.

However, let us move out of our formulation and think about why linearity might be necessary.

# Why Linearity?

The first compelling argument for linearity was made by Wigner and Bargmann who proved that quantum dynamics must be linear if it does not change absolute values of inner products of state vectors.

However, the assumption – upon which this argument stands – is not strong enough.

# Why Linearity?

In fact, Steven Weinberg among others have indeed come up with non-linear formulations of Quantum Mechanics.

So, can we come up with an argument that is stronger?

# Why Linearity?

Fortunately, we can! And, guess what? It is inherently based on Computational Complexity.

## Theorem

*If quantum mechanics were non-linear, then one could build a computer to solve NP-complete problems in polynomial time.*

# No-go Theorems

Theorems which imply limitations on the operations that can be performed in a quantum system.

First we start off by stating the general No go theorem.

## Theorem

*Given an arbitrary state  $|\psi\rangle \in \mathcal{H}^2$  of an unknown qubit and a blank state  $|\Sigma\rangle \in \mathcal{H}^2$ , there does not exist a isometric map  $\mathcal{M} : \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2 \rightarrow \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2$  that will transform*

$$|\psi\rangle \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow |\psi\rangle \otimes |\mathcal{F}(\psi)\rangle \otimes |Q\rangle$$

$\mathcal{F}$  can also be expressed as a matrix  $K$ . which means that  $|\mathcal{F}(\psi)\rangle = K|\psi\rangle$ .

The cases are:

- $K$  is a unitary matrix  $U$
- $K$  is an anti-unitary matrix  $A$
- $K$  is a linear combination of  $U$  and  $A$ , that is  $K = \sqrt{\lambda}U + \sqrt{1-\lambda}A$  where  $0 \leq \lambda \leq 1$ .

We assume an existence of  $K$  for a given  $\mathcal{F}$  and perform the operation on an arbitrary qubit blank state pair and later show that such  $K$  can't exist without violating the underlying assumptions of its linearity and unitarity.



# Proof: Unitary Transformation

Let  $|\mathcal{F}(\psi)\rangle = U|\psi\rangle$  where  $U$  is a unitary operation.

Without the loss of generality, we can assume  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .

Now writing the equation with the new values:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |q\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha U|0\rangle + \beta U|1\rangle) \otimes |q\rangle$$

We can combine the first 2 qubits to represent the tensor product implicitly

$$\begin{aligned} &(\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |q\rangle \rightarrow \\ &[\alpha^2|0\mathcal{F}(0)\rangle + \beta^2|1\mathcal{F}(1)\rangle + \alpha\beta(|0\mathcal{F}(1)\rangle + |1\mathcal{F}(0)\rangle)] \otimes |q\rangle \end{aligned}$$

Comparing the 2 forms of the equations, we can see that the equations only satisfy for the cases where  $\alpha = 1$  or  $\beta = 1$ .

# Proof: Anti-Unitary Transformation

Let  $|\mathcal{F}(\psi)\rangle = A|\psi\rangle$  where  $A$  is a anti-unitary operation.

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |q\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha^* A|0\rangle + \beta^* A|1\rangle) \otimes |q\rangle$$

Following the same pattern as the last time.

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |q\rangle \rightarrow$$

$$[|\alpha|^2|0\rangle\mathcal{F}(0)\rangle + |\beta|^2|1\rangle\mathcal{F}(1)\rangle + \alpha\beta^*|0\rangle\mathcal{F}(1)\rangle + \alpha^*\beta|1\rangle\mathcal{F}(0)\rangle] \otimes |q\rangle$$

Similar conclusion can be drawn for anti-unitary transformation.

# Proof: Linear Combination of both

Now for the last case, where  $K = \sqrt{\lambda}U + \sqrt{1-\lambda}A$  where  $0 \leq \lambda \leq 1$ .

$$\begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |Q\rangle \\ \rightarrow & \sqrt{\lambda}\alpha|0\rangle \otimes U|0\rangle \otimes |Q_0\rangle + \sqrt{1-\lambda}\alpha^*|0\rangle \otimes A|0\rangle \otimes |Q_0\rangle \\ & + \sqrt{\lambda}\beta|1\rangle \otimes U|1\rangle \otimes |Q_1\rangle + \sqrt{1-\lambda}\beta^*|1\rangle \otimes A|1\rangle \otimes |Q_1\rangle \end{aligned}$$

The other form being:

$$\begin{aligned} |\psi\rangle \otimes |\mathcal{F}(\psi)\rangle \otimes |Q\psi\rangle = & [\sqrt{\lambda}\alpha^2|0\rangle \otimes U|0\rangle + \sqrt{1-\lambda}|\alpha|^2|0\rangle \otimes A|0\rangle \\ & + \sqrt{\lambda}\beta^2|1\rangle \otimes U|1\rangle + \sqrt{1-\lambda}|\beta|^2|1\rangle \otimes A|1\rangle + \sqrt{\lambda}\alpha\beta|0\rangle \otimes U|1\rangle + \sqrt{1-\lambda}\alpha\beta^* \\ & |0\rangle \otimes A|1\rangle + \sqrt{\lambda}\alpha\beta|1\rangle \otimes U|0\rangle + \sqrt{1-\lambda}\alpha^*\beta|1\rangle \otimes A|0\rangle] \otimes |Q\psi\rangle. \end{aligned}$$

(Don't try to read these equations, they are too big and boring)

Although No go generalization did not come before its "corollaries". We will still consider the following as its corollaries.

- No Cloning theorem  $\rightarrow \mathcal{F}(\psi) = \psi$
- No Anti Cloning theorem  $\rightarrow \mathcal{F}(\psi) = \psi$
- No Deletion theorem  $\rightarrow$  Can reverse No Cloning Theorem

We will further show some of No go theorems and their proofs.

# No Cloning Theorem

Alapan Chaudhuri and Zeeshan Ahmed

April 30, 2021

- Introduction
- Cloning
- No Cloning
- Theorem Statement
- Proof Sketch
- Proof
- Another Proof
- Conclusion



Suppose that Shreyas and Kunwar are light-years apart, but they each possess one qubit such that the two qubits are entangled with each other.

We know that entanglement leads to several non-local effects. For example, if the entangled system they possess can be represented as  $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$  and Shreyas measures his own qubit then he also learns the state of Kunwar's qubit almost instantaneously.

But does that mean both of them can communicate at a speed faster than light?

Unfortunately, (especially for sci-fi enthusiasts) NO!

Now, the main reason why they can not communicate faster than light is due to the fact that upon Shreyas measuring his qubit, Kunwar is still unable to tell which basis his qubit is in.

So is there any way by which Kunwar can find out in what basis Shreyas's qubit was measured such that faster than light communication would be possible?

Kunwar is smart. He figures out that if he can make unlimited copies of his qubit, surely then he can find out in which basis Shreyas's measurement was made.

AWESOME! So now these two best friends can finally chat at a rate faster than light rather than being stuck alone in some remote galaxy in the universe?

# Cloning



# No Cloning

There exists no possible method by which we can create a independent and identical copy of any arbitrary unknown quantum state.

And guess what? We can PROVE it!

# Theorem Statement

There  $\nexists$  no unitary operator  $U$  on  $H \otimes H$  such that for any normalized state  $|\psi\rangle \in H$  such that  $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$

**OR**

for any normalized states  $|\psi\rangle, |\phi\rangle \in H$  such that  
$$U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle.$$



Let us try to clone a single qubit say,  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .

- Suppose there exists a transformation such that it takes  $|\psi\rangle$  and say  $|0\rangle$  and result in  $|\psi\rangle$  and  $|\psi\rangle$  respectively.
- Then, by the postulates of quantum mechanics, the transformation must be unitary and should seem as below.

$$\begin{aligned} & (\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \xrightarrow{U} (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) \\ \implies & (\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \xrightarrow{U} \alpha^2 |00\rangle + \alpha\beta |01\rangle + \alpha\beta |10\rangle + \beta^2 |11\rangle \\ \implies & \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{bmatrix} = U \begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} \end{aligned}$$

However, the above transformation results in quadratic terms and thus for sure it can not be unitary!

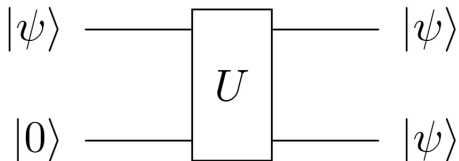


Figure: Cloning Transformation

Consider  $U$  to be a unitary transformation which can clone any arbitrary qubit.

Expressing the transformation in 2 different ways:

$$(\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \xrightarrow{U} (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle)$$

$$\alpha |00\rangle + \beta |10\rangle \xrightarrow{U} \alpha U|00\rangle + \beta U|10\rangle$$

Simplifying both the RHS

$$\begin{aligned} (\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle &\xrightarrow{U} \alpha^2 |00\rangle + \alpha\beta |01\rangle + \alpha\beta |10\rangle + \beta^2 |11\rangle \\ &\xrightarrow{U} \alpha |00\rangle + \beta |11\rangle \end{aligned}$$

Both the form of RHS must be equal:

$$\alpha^2 |00\rangle + \alpha\beta |01\rangle + \alpha\beta |10\rangle + \beta^2 |11\rangle = \alpha |00\rangle + \beta |11\rangle$$

From the equations we can see  $(\alpha = 0, \beta = 1)$  or  $(\alpha = 1, \beta = 0)$ . This proves the existence of a *general* transformation which can clone a qubit.

# Another Proof

We can also prove that a single universal unitary operator  $U$  doesn't exist such that it can clone any arbitrary quantum state.

Suppose,  $|v\rangle$  and  $|w\rangle$  are two arbitrary quantum states such that,  $U|v\phi\rangle = |vv\rangle$  and  $U|w\phi\rangle = |ww\rangle$ . Here,  $|\phi\rangle$  serves as a normalized ancilla qubit.

Moreover, we know that unitary transformations are inner-product preserving or in other words,  $\langle a|a\rangle = \langle a|U^\dagger U|a\rangle, \forall$  states  $|a\rangle$ .

In that case, we shall have,

$$\langle v|w\rangle\langle\phi|\phi\rangle = \langle v|w\rangle = |\langle v|w\rangle|^2$$

Thus, either  $\langle v|w\rangle = 1$  or  $\langle v|w\rangle = 0$ , which implies that such a unitary  $U$  can copy perfectly if and only if  $|v\rangle$  and  $|w\rangle$  belong to the same orthonormal basis.

As a result, no universal  $U$  can clone a general quantum state. This proves the no-cloning theorem.



The impossibility of cloning any arbitrary quantum state is truly fundamental and has a ton of implications – for example as follows.

- Can't use classical error correction techniques for quantum error-correction
- Inherent indistinguishability of quantum states
- Implies several other no-go theorems like no-deleting and no-teleportation among others
- Validates no-communication theorem
- Black hole complementarity

However, it is to be also noted that the fact that perfect cloning is impossible does not imply that imperfect cloning is also not possible.

In fact for any arbitrary qubit, it is indeed possible to copy it such that the clones have a non-perfect fidelity and theoretical bounds do exist for the same.

# Conclusion



**Figure:** Shreyas is sad because he can't communicate with Kunwar instantaneously.

# No Deletion Theorem

Rahul Goel and Ishaan Shah

# Theorem Statement

- ▶ No deleting theorem is a no-go theorem which says that given two copies of a qubit it is impossible to delete or change the state of one qubit without affecting the state of the other qubit.
- ▶ More formally we can say that:  
There exists no transformation such that

$$|\psi\rangle_A |\psi\rangle_B \rightarrow |\psi\rangle_A |0\rangle_B$$

## Before we get into the math

- ▶ How can we create two copies of any arbitrary state? (No-Cloning Theorem)
  - ▶ No-Cloning states that you can't make copies of an unknown state. However, over here we can create two qubits in the same state by applying the same quantum circuit on them.
- ▶ Can't we just measure a one qubit out of the two and say that the qubit got deleted?
  - ▶ Consider the state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Then,

$$|\psi\rangle |\psi\rangle = \alpha^2 |0\rangle |0\rangle + \beta^2 |1\rangle |1\rangle + \alpha\beta(|0\rangle |1\rangle + |1\rangle |0\rangle)$$

- ▶ If we measure the second qubit and get 0 then the state of the first qubit will also collapse to

$$|\psi\rangle = \frac{\alpha^2 |0\rangle + \alpha\beta |1\rangle}{\sqrt{\alpha^4 + \alpha^2\beta^2}}$$

## Alice plays with Bob

- ▶ Alice prepares a box in some quantum state and hands it to Bob, but doesn't tell him the state.
- ▶ Bob sticks the box in his deletion machine. He isolates the machine from the rest of the laboratory.
- ▶ Is it possible for this machine to “delete” the box, such that afterwards, the state of the machine and box together is some fixed, pre-determined state that doesn't depend on the original state of the box? **NO**.
- ▶ Hypothetically, we can put destroyed box together in the same orientation to get the information.

## Alice plays with Bob - Continued

- ▶ Alice prepares a two quantum states and hands it to Bob, but doesn't tell him the states.
- ▶ Bob sticks both boxes in his deletion machine. He isolates the machine from the rest of the laboratory.
- ▶ Is it possible for this machine to “delete” exactly one of the quantum states while keeping the other quantum state intact? **NO**.
- ▶ The reason will be explained later.



## Proof by Contradiction

Let us assume there exists an Unitary Operatator  $U$  which works on two qubits to delete one of the qubit as follows:

$$U(|0\rangle_A |0\rangle_B |\phi\rangle) = |0\rangle_A |0\rangle_B |\phi_0\rangle$$

$$U(|1\rangle_A |1\rangle_B |\phi\rangle) = |1\rangle_A |0\rangle_B |\phi_1\rangle$$

Here,  $|\phi\rangle$  denotes the ancillary bits used by the operator for the purpose of reverseability.

## Proof by Contradiction - Continued

Now consider a state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . When we apply the deletion operation on the pair of states  $|\psi\rangle|\psi\rangle$ , we get the following results.

$$\begin{aligned} U(|\psi\rangle_A |\psi\rangle_B |\phi\rangle) &= U(\alpha^2 |0\rangle_A |0\rangle_B + \beta^2 |1\rangle_A |1\rangle_B + \alpha\beta(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)) |\phi\rangle \\ &= U(\alpha^2 |0\rangle_A |0\rangle_B) + U(\beta^2 |1\rangle_A |1\rangle_B) + U(\alpha\beta(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)) \\ &= \alpha^2 |0\rangle_A |0\rangle_B |\phi'\rangle + \beta^2 |1\rangle_A |0\rangle_B |\phi'\rangle + \alpha\beta U(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) |\phi\rangle \end{aligned}$$

The last part in the expression is an entangled state. We can define it as  $\Phi$

$$U(|\psi\rangle_A |\psi\rangle_B |\phi\rangle) = \alpha^2 |0\rangle_A |0\rangle_B |\phi'\rangle + \beta^2 |1\rangle_A |0\rangle_B |\phi'\rangle + \alpha\beta U(|\Phi\rangle) |\phi\rangle$$

## Proof by Contradiction - Continued

- ▶ Thus, we see a contradiction.
- ▶ In the first calculation, the final state is defined in terms of  $a$ ,  $b$ ,  $0$ ,  $1$ , and  $\psi'$ .
- ▶ But in the other calculation, we see an additional entangled state in the final expression.
- ▶ The two calculations are not equal in general, and  $U$  cannot exist (proof by contradiction).

## We present an alternative proof

- ▶ Assume that the no-deletion theorem is invalid.
- ▶ That is there exists a quantum operation that does the following.

$$|\psi\rangle |\psi\rangle \rightarrow |\psi\rangle |0\rangle$$

- ▶ We know that quantum gates are reversible. (Since they can be represented by unitary matrices)
- ▶ This means that there should exist a quantum gate that does the following operation.

$$|\psi\rangle |0\rangle \rightarrow |\psi\rangle |\psi\rangle$$

- ▶ This means that we can in fact create a copy of  $\psi$ .
- ▶ Contradiction with the no-cloning theorem.
- ▶ Thus no-deletion theorem is valid.

# No Hiding Theorem

Pulak Malhotra

# Hiding Classical Information

- ▶ Classical information can be hidden in two ways:
  - ▶ Moving the system
  - ▶ Encrypting the message
- ▶ In case of encryption the information is stored in the correlation of different subsystems. For example, in XOR encryption if we encrypt the message  $M$  the using a secret key  $K$  then from the encrypted  $M \oplus K$  alone we cannot decipher the information but using the correlation between  $K$  and  $M$  the information can be retrieved out by doing  $M \oplus K \oplus K = M$

# Hiding in Quantum Systems

- ▶ No hiding disallows encryption like hiding phenomenon in quantum system
- ▶ Missing information must be encoded in the Hilbert space and not in the correlation of different subsystems

## Perfect Hiding Process

- ▶ Take an input state  $\rho_I$  encode it in a larger hilbert space  $|\psi\rangle_I \rightarrow |\Psi\rangle_{OA}$
- ▶ If  $\sigma_O = \text{Tr}(|\psi\rangle_{OA} \langle\psi|)$  is independant of input state then this is a hiding process



## No Hiding Theorem

- ▶ No-hiding theorem states that if information is lost from a system via decoherence then it moves to the subspace of the environment.
- ▶ Let  $|\psi\rangle_I \rightarrow |\Psi\rangle_{OA}$  with  $|\psi\rangle_I \langle\psi|_I = \rho_I$ .  
The hiding process transforms  $\rho_I \rightarrow \sigma_O = \sum_k p_k |K\rangle \langle K|$  with  $\sigma_O$  fixed for all  $\rho$ , and  $\sigma_O = \text{Tr}(|\Psi\rangle_{OA} \langle\Psi|)$

$$|\Psi\rangle_{OA} = \sum_K \sqrt{p_k} |k\rangle_O \otimes (|q_k\rangle \otimes |\psi\rangle)_A \quad (1)$$

# Proof of No Hiding Theorem

- ▶ If  $|\psi\rangle\langle\psi| \rightarrow \sigma = \sum_k p_k |k\rangle\langle k|$  then in the purified hilbert space  $|\psi\rangle|A\rangle \rightarrow |\Psi\rangle = \sum_K \sqrt{p_k} |k\rangle |A_k(\psi)\rangle$  by schmidt decomposition, where  $p_k$  are the  $K$  non zero eigen values of the density matrix  $\sigma$ ,  $\{|k\rangle\}$  are its eigenvectors and  $\{|A_k\rangle\}$  are the orthonormal states of the ancilla.
- ▶ Let  $|\psi\rangle = \sum_n c_n |\psi_n\rangle$  for some orthonormal basis  $\{|\psi_n\rangle\}$   
When hiding process acts on  $|\psi_n\rangle$ , we have,  
 $|\psi_n\rangle|A\rangle = \sum_K \sqrt{p_k} |k\rangle |A_k(\psi_n)\rangle$  where  $\langle A_k(\psi_n) | A_k(\psi_m) \rangle = \delta_{nm}$
- ▶ By linearity,  $\sum_n c_n |\psi_n\rangle|A\rangle \rightarrow \sum_n c_n \sum_k \sqrt{p_k} |k\rangle |A_k(\psi_n)\rangle$   
This implies  $|A_k(\psi)\rangle = \sum_n c_n |A_k(\psi_n)\rangle$
- ▶ By unitarity,  $|A_k(\psi_n)\rangle = |q_k\rangle \otimes |\psi_n\rangle$

## Proof of No Hiding Theorem

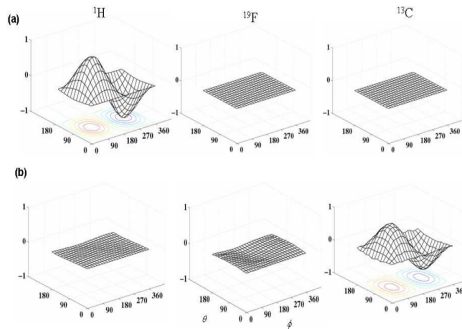
$$\begin{aligned}|A_k(\psi)\rangle &= \sum_n c_n |A_k(\psi_n)\rangle \\&= \sum_n c_n |q_k\rangle \otimes |\psi_n\rangle \\&= |q_k\rangle \otimes \sum_n c_n |\psi_n\rangle \\&= |q_k\rangle \otimes |\psi\rangle\end{aligned}$$

Finally,

$$|\psi\rangle |A\rangle \rightarrow \sum_K \sqrt{p_k} |k\rangle \otimes |q_k\rangle \otimes |\psi_n\rangle$$

# Experimental Verification

- ▶ Experimentally tested in 2011 using nuclear magnetic resonance
- ▶ Use quantum state randomization of a qubit as one example of the hiding process and show that the missing information can be fully recovered up to local unitary transformations in the ancilla qubits.



# Applications of No hiding theorem

- ▶ Thermalization
- ▶ Black hole evaporation
- ▶ Quantum teleportation
- ▶ State randomization

## References

- ▶ Wikipedia - No hiding theorem
- ▶ Conservation of Quantum Information talk by Prof. Arun K. Pati
- ▶ Experimental Test of Quantum No-Hiding Theorem  
(<https://arxiv.org/abs/1004.5073v1>)