Quantum Solovay randomness

Tejas Bhojraj

UW-Madison

Waterloo, June 2018

Reference: 'Martin-Löf random quantum states', by Nies and Scholz. I will first discuss this paper and then outline some answers to the questions posed in it.

All the quantum physics needed for this talk

All the quantum physics needed for this talk....in one slide.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of 'classical' states.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of ‘classical’ states.
- It’s dimension is the number of classical states it is a superposition of.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of 'classical' states.
- It's dimension is the number of classical states it is a superposition of.
- A measurement of the system collapses it into one of the classical states. Measuring a classical state does not cause any collapse. Hence they are called 'classical'.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of 'classical' states.
- It's dimension is the number of classical states it is a superposition of.
- A measurement of the system collapses it into one of the classical states. Measuring a classical state does not cause any collapse. Hence they are called 'classical'.
- Let us formalize this.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of ‘classical’ states.
- It’s dimension is the number of classical states it is a superposition of.
- A measurement of the system collapses it into one of the classical states. Measuring a classical state does not cause any collapse. Hence they are called ‘classical’.
- Let us formalize this.
- We represent a n-dimensional system by a matrix $\psi\psi^*$ where $\psi \in \mathbb{C}^n$ is a unit column vector (ψ^* is the complex conjugate transpose of ψ).

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of 'classical' states.
- It's dimension is the number of classical states it is a superposition of.
- A measurement of the system collapses it into one of the classical states. Measuring a classical state does not cause any collapse. Hence they are called 'classical'.
- Let us formalize this.
- We represent a n-dimensional system by a matrix $\psi\psi^*$ where $\psi \in \mathbb{C}^n$ is a unit column vector (ψ^* is the complex conjugate transpose of ψ).
- Fix a orthonormal basis $b_1, .., b_n$ of $\mathbb{C}^n$. The $b_i b_i^*$ s will be the classical states.

All the quantum physics needed for this talk....in one slide.

- First, a sketch. We will formalize it soon.
- A quantum mechanical system is a superposition of 'classical' states.
- It's dimension is the number of classical states it is a superposition of.
- A measurement of the system collapses it into one of the classical states. Measuring a classical state does not cause any collapse. Hence they are called 'classical'.
- Let us formalize this.
- We represent a n-dimensional system by a matrix $\psi\psi^*$ where $\psi \in \mathbb{C}^n$ is a unit column vector (ψ^* is the complex conjugate transpose of ψ).
- Fix a orthonormal basis $b_1, .., b_n$ of $\mathbb{C}^n$. The $b_i b_i^*$ s will be the classical states.
- A measurement is represented by a matrix H with eigenvectors $b_1, .., b_n$ with eigenvalues equalling 0 or 1. So, H is a Hermitian projection.

Okay, I tried but I need two.

Okay, I tried but I need two.

- Measuring H on $\psi\psi^*$ causes the system to collapse to one of the classical states $b_i b_i^*$ and the outcome of the measurement is e_i where $Hb_i = e_i b_i$ (i.e, the eigenvalue corresponding to b_i.)

Okay, I tried but I need two.

- Measuring H on $\psi\psi^*$ causes the system to collapse to one of the classical states $b_i b_i^*$ and the outcome of the measurement is e_i where $Hb_i = e_i b_i$ (i.e, the eigenvalue corresponding to b_i.)
- The probability of collapsing $\psi\psi^*$ to $b_i b_i^*$ on measurement is $|\langle \psi, b_i \rangle|^2$.

Okay, I tried but I need two.

- Measuring H on $\psi\psi^*$ causes the system to collapse to one of the classical states $b_i b_i^*$ and the outcome of the measurement is e_i where $Hb_i = e_i b_i$ (i.e, the eigenvalue corresponding to b_i.)
- The probability of collapsing $\psi\psi^*$ to $b_i b_i^*$ on measurement is $|\langle \psi, b_i \rangle|^2$.
- By orthonormality, we see that measurements do not collapse classical states.

Okay, I tried but I need two.

- Measuring H on $\psi\psi^*$ causes the system to collapse to one of the classical states $b_i b_i^*$ and the outcome of the measurement is e_i where $Hb_i = e_i b_i$ (i.e, the eigenvalue corresponding to b_i.)
- The probability of collapsing $\psi\psi^*$ to $b_i b_i^*$ on measurement is $|\langle\psi, b_i\rangle|^2$.
- By orthonormality, we see that measurements do not collapse classical states.
- One can check that the expected value of measuring H on $\psi\psi^*$ is Trace$(H\psi\psi^*)$.

Qubits

- A qubit is a 2-dimensional system.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.
- Denote V_0, V_1 by $|0\rangle$ and $|1\rangle$.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.
- Denote V_0, V_1 by $|0\rangle$ and $|1\rangle$.
- So, $(\mathbb{C}^2)^{\otimes n} := H_n$ has a orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n$. The basis vector given by this σ is

$$|\sigma(0)\rangle \otimes |\sigma(1)\rangle \otimes \ldots \otimes |\sigma(n-1)\rangle = \bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle$$

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.
- Denote V_0, V_1 by $|0\rangle$ and $|1\rangle$.
- So, $(\mathbb{C}^2)^{\otimes n} := H_n$ has a orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n$. The basis vector given by this σ is

$$|\sigma(0)\rangle \otimes |\sigma(1)\rangle \otimes ... \otimes |\sigma(n-1)\rangle = \bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle$$

- If $|\psi\rangle \in H_n$ is a unit vector, the matrix $|\psi\rangle\langle\psi|$ is said to be a *pure state*.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.
- Denote V_0, V_1 by $|0\rangle$ and $|1\rangle$.
- So, $(\mathbb{C}^2)^{\otimes n} := H_n$ has a orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n$. The basis vector given by this σ is

$$|\sigma(0)\rangle \otimes |\sigma(1)\rangle \otimes ... \otimes |\sigma(n-1)\rangle = \bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle$$

- If $|\psi\rangle \in H_n$ is a unit vector, the matrix $|\psi\rangle\langle\psi|$ is said to be a *pure state*.
- A *mixed state* is a convex combination of 2 or more pure states.

Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector v by $|v\rangle$ and v^* by $\langle v|$.
- Let H be a Hermitian operator on $\mathbb{C}^2$ with eigenpairs $(V_1, 1)$ and $(V_0, 0)$ with V_1 and V_0 forming a orthonormal basis.
- Denote V_0, V_1 by $|0\rangle$ and $|1\rangle$.
- So, $(\mathbb{C}^2)^{\otimes n} := H_n$ has a orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n$. The basis vector given by this σ is

$$|\sigma(0)\rangle \otimes |\sigma(1)\rangle \otimes \ldots \otimes |\sigma(n-1)\rangle = \bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle$$

- If $|\psi\rangle \in H_n$ is a unit vector, the matrix $|\psi\rangle\langle\psi|$ is said to be a *pure state*.
- A *mixed state* is a convex combination of 2 or more pure states.
- A pure state is a *single* quantum system while a mixed state is a probabilistic mixture of pure states.

The Density Matrix

- The mixed and pure states are called density matrices.

The Density Matrix

- The mixed and pure states are called density matrices.
- In fact, *any* Hermitian, positive semidefinite matrix with trace $= 1$ gives a state and is a density matrix.

The Density Matrix

- The mixed and pure states are called density matrices.
- In fact, *any* Hermitian, positive semidefinite matrix with trace = 1 gives a state and is a density matrix.
- If a Hermitian ρ on H_n has Trace(ρ)=1, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. If the eigenpairs are (α_i, ψ_i), then

$$\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i| \quad (1)$$

The sum is convex as 1=Tr(ρ)=$\sum_i \alpha_i$. So, ρ gives a state.

The Density Matrix

- The mixed and pure states are called density matrices.
- In fact, *any* Hermitian, positive semidefinite matrix with trace = 1 gives a state and is a density matrix.
- If a Hermitian ρ on H_n has Trace(ρ)=1, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. If the eigenpairs are (α_i, ψ_i), then

$$\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i| \tag{1}$$

  The sum is convex as $1=\text{Tr}(\rho)=\sum_i \alpha_i$. So, ρ gives a state.
- The density matrix $\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i|$ gives a system which is in $|\psi_i\rangle\langle\psi_i|$ with probability α_i

The Density Matrix

- The mixed and pure states are called density matrices.
- In fact, *any* Hermitian, positive semidefinite matrix with trace = 1 gives a state and is a density matrix.
- If a Hermitian ρ on H_n has Trace(ρ)=1, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. If the eigenpairs are (α_i, ψ_i), then

$$\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i| \tag{1}$$

  The sum is convex as 1=Tr(ρ)=$\sum_i \alpha_i$. So, ρ gives a state.
- The density matrix $\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i|$ gives a system which is in $|\psi_i\rangle\langle\psi_i|$ with probability α_i
- Notation: $L(H_n)$ denotes the space of 2^n by 2^n matrices.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.
- So, a composite system is a product state (pure tensor).

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.
- So, a composite system is a product state (pure tensor).
- The pure tensors do not exhaust the set of density matrices in $L(H_{n+1})$.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.
- So, a composite system is a product state (pure tensor).
- The pure tensors do not exhaust the set of density matrices in $L(H_{n+1})$.
- Take a $\rho \in L(H_{n+1})$ which is not a pure tensor.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.
- So, a composite system is a product state (pure tensor).
- The pure tensors do not exhaust the set of density matrices in $L(H_{n+1})$.
- Take a $\rho \in L(H_{n+1})$ which is not a pure tensor.
- It is not a composite of states in $L(H_n)$ and $L(H_1)$.

- So far we have seen: a system of n qubits is modeled by a density matrix in $L(H_n)$.
- A system in $H_{n+1} = H_n \otimes H_1$ which is a composite of systems $\sigma \in L(H_n)$ and $\tau \in L(H_1)$ is described by $\rho = \sigma \otimes \tau \in L(H_n) \otimes L(H_1)$.
- So, a composite system is a product state (pure tensor).
- The pure tensors do not exhaust the set of density matrices in $L(H_{n+1})$.
- Take a $\rho \in L(H_{n+1})$ which is not a pure tensor.
- It is not a composite of states in $L(H_n)$ and $L(H_1)$.
- Such a ρ is called entangled.

Partial Trace

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.
- What does 'ignoring' mean?

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.
- What does 'ignoring' mean?
- It means we need a $\tau \in L_n$ which describes measurements of the first n qubits of ρ.

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.
- What does 'ignoring' mean?
- It means we need a $\tau \in L_n$ which describes measurements of the first n qubits of ρ.
- I.e, we need a τ such that for any hermitian $O \in L_n$,

$$Tr(\tau O) = Tr(\rho(O \otimes I)).$$

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.
- What does 'ignoring' mean?
- It means we need a $\tau \in L_n$ which describes measurements of the first n qubits of ρ.
- I.e, we need a τ such that for any hermitian $O \in L_n$,

$$Tr(\tau O) = Tr(\rho(O \otimes I)).$$

- (Recall: The expectation of measuring O on ϕ is $Tr(\phi O)$.)

Partial Trace

- Given $\rho \in L_{n+1}$ we want to find the state given by ignoring the last qubit.
- What does 'ignoring' mean?
- It means we need a $\tau \in L_n$ which describes measurements of the first n qubits of ρ.
- I.e, we need a τ such that for any hermitian $O \in L_n$,

$$Tr(\tau O) = Tr(\rho(O \otimes I)).$$

- (Recall: The expectation of measuring O on ϕ is $Tr(\phi O)$.)
- If $\rho = \lambda \otimes \sigma$ for a $\lambda \in L_n$ and $\sigma \in L_1$ then,

$$Tr(\rho(O \otimes I)) = Tr(\lambda O \otimes \sigma I) = Tr(\lambda O)\, Tr(\sigma) = Tr(\lambda O)$$

  So, $\tau = \lambda$ works.
- If ρ is entangled, the choice of τ is not so obvious

- Denote $L(H_n)$ by L_n. Define

$$T_1 : L_{n+1} \longrightarrow L_n$$

by $T_1(A \otimes B) := A * Tr(B)$ for any $A \in L_n, B \in L_1$ and then extending it linearly.

- Denote $L(H_n)$ by L_n. Define

$$T_1 : L_{n+1} \longrightarrow L_n$$

by $T_1(A \otimes B) := A * Tr(B)$ for any $A \in L_n, B \in L_1$ and then extending it linearly.

- This defines T_1 since if $\rho \in L_{n+1}$, it is a *finite sum* of the form

$$\rho = \sum_i \alpha_i (A_i \otimes B_i)$$

for scalars α_i, $A_i \in L_n$ and $B_i \in L_1$.(After modding out by the usual $\equiv$)

- Denote $L(H_n)$ by L_n. Define

$$T_1 : L_{n+1} \longrightarrow L_n$$

by $T_1(A \otimes B) := A * Tr(B)$ for any $A \in L_n, B \in L_1$ and then extending it linearly.

- This defines T_1 since if $\rho \in L_{n+1}$, it is a *finite sum* of the form

$$\rho = \sum_i \alpha_i (A_i \otimes B_i)$$

for scalars α_i, $A_i \in L_n$ and $B_i \in L_1$.(After modding out by the usual $\equiv$)

- It turns out that $T_1(\rho)$ is the required τ

- There is a arrangement of the bases of H_n which makes computing the partial trace easy.

- There is a arrangement of the bases of H_n which makes computing the partial trace easy.
- Details (skip)
  Recall that H_n has a orthonormal basis comprised of elements of the form

$$\bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle \text{ for a } \sigma \in 2^n$$

  Order them as follows: given $\sigma < \tau$, define

  1. $\sigma 0 < \sigma 1$
  2. $\sigma 1 > \tau 0$
  3. $\sigma i < \tau i$ for $i = 0, 1$

  For $A \in L(H_n), B \in L(H_1)$,

$$A \otimes B = \begin{bmatrix} Ab_{00} & Ab_{01} \\ Ab_{10} & Ab_{11} \end{bmatrix} \text{ if } B = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix}$$

Finding the Partial Trace of an Operator from it's Matrix

- Let $\rho \in L_{n+1}$

$$\rho = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

be with each block in L_n

Finding the Partial Trace of an Operator from it's Matrix

- Let $\rho \in L_{n+1}$

$$\rho = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

  be with each block in L_n
- By the arrangement of the basis elements, we see that

$$T_1(\rho) = A + D$$

The Partial Trace of an Entangled State is Mixed

- Let $\psi = (|1\rangle \otimes |1\rangle + |0\rangle \otimes |0\rangle)/\sqrt{2} = (|11\rangle + |00\rangle)/\sqrt{2}$

The Partial Trace of an Entangled State is Mixed

- Let $\psi = (|1\rangle \otimes |1\rangle + |0\rangle \otimes |0\rangle)/\sqrt{2} = (|11\rangle + |00\rangle)/\sqrt{2}$
- The pure state representing it is

$$|\psi\rangle\langle\psi| = (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)/2$$

The Partial Trace of an Entangled State is Mixed

- Let $\psi = (|1\rangle \otimes |1\rangle + |0\rangle \otimes |0\rangle)/\sqrt{2} = (|11\rangle + |00\rangle)/\sqrt{2}$
- The pure state representing it is

$$|\psi\rangle\langle\psi| = (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)/2$$

- It's matrix is

$$\begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}$$

- and partial trace is

$$T_1(\rho) = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$$

The Partial Trace of an Entangled State is Mixed

- Let $\psi = (|1\rangle \otimes |1\rangle + |0\rangle \otimes |0\rangle)/\sqrt{2} = (|11\rangle + |00\rangle)/\sqrt{2}$
- The pure state representing it is

$$|\psi\rangle\langle\psi| = (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)/2$$

- It's matrix is

$$\begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}$$

- and partial trace is

$$T_1(\rho) = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$$

- which has rank $= 2$ and so is not a pure state. (Pure states have rank 1)

Table of Contents

- Now we consider a system of countably infinitely many qubits.

- Now we consider a system of countably infinitely many qubits.
- For each n, let $T_n : L_n \longrightarrow L_{n-1}$ be the partial trace.

- Now we consider a system of countably infinitely many qubits.
- For each n, let $T_n : L_n \longrightarrow L_{n-1}$ be the partial trace.
- A sequence of density matrices, $(S_n)_{n\in\omega}$ with $S_n \in L_n$ is *coherent* if $T_n(S_n) = S_{n-1}$ for all n.

- Now we consider a system of countably infinitely many qubits.
- For each n, let $T_n : L_n \longrightarrow L_{n-1}$ be the partial trace.
- A sequence of density matrices, $(S_n)_{n\in\omega}$ with $S_n \in L_n$ is *coherent* if $T_n(S_n) = S_{n-1}$ for all n.
- It models a sequence of infinitely many qubits where for all n, the first n qubits are obtained by ignoring the last qubit from the first $n+1$ qubits.

- Now we consider a system of countably infinitely many qubits.
- For each n, let $T_n : L_n \longrightarrow L_{n-1}$ be the partial trace.
- A sequence of density matrices, $(S_n)_{n\in\omega}$ with $S_n \in L_n$ is *coherent* if $T_n(S_n) = S_{n-1}$ for all n.
- It models a sequence of infinitely many qubits where for all n, the first n qubits are obtained by ignoring the last qubit from the first $n+1$ qubits.
- The set of such coherent sequences is called quantum Cantor space.

- Now we consider a system of countably infinitely many qubits.
- For each n, let $T_n : L_n \longrightarrow L_{n-1}$ be the partial trace.
- A sequence of density matrices, $(S_n)_{n \in \omega}$ with $S_n \in L_n$ is *coherent* if $T_n(S_n) = S_{n-1}$ for all n.
- It models a sequence of infinitely many qubits where for all n, the first n qubits are obtained by ignoring the last qubit from the first $n+1$ qubits.
- The set of such coherent sequences is called quantum Cantor space.
- A coherent sequence will also be called a state.

Quantum Σ_1^0 Classes

- A Σ_1^0 class $S \subseteq 2^\omega$ can be written as

$$S = \bigcup_n [\![A_n]\!]$$

where

1. $A_n \subseteq 2^n$
2. An index for A_n as a computable set can be obtained uniformly in n.
3. $[\![A_n]\!] \subseteq [\![A_{n+1}]\!]$

Quantum Σ_1^0 Classes

- A Σ_1^0 class $S \subseteq 2^\omega$ can be written as

$$S = \bigcup_n [\![A_n]\!]$$

where

1. $A_n \subseteq 2^n$
2. An index for A_n as a computable set can be obtained uniformly in n.
3. $[\![A_n]\!] \subseteq [\![A_{n+1}]\!]$

- Extend this to the quantum setting.

Quantum Σ_1^0 Classes

- A Σ_1^0 class $S \subseteq 2^\omega$ can be written as

$$S = \bigcup_n [\![A_n]\!]$$

  where

  1. $A_n \subseteq 2^n$
  2. An index for A_n as a computable set can be obtained uniformly in n.
  3. $[\![A_n]\!] \subseteq [\![A_{n+1}]\!]$

- Extend this to the quantum setting.
- A Hermitian projection $P \in L_n$ is said to be *special* if it's entries are in $\mathbb{C}_{alg}$ (roots of $\mathbb{Q}$ polynomials); hence computable.

Definition: q-Σ^0_1 class

$S = (P_n)_n$ a sequence of special projections is a q-Σ^0_1 class if

1. $P_n \in L_n$
2. An index for P_n as a computable matrix can be obtained uniformly in n.
3. $\text{rng}(P_n) \subseteq \text{rng}(P_{n+1})$.

Definition: q-Σ^0_1 class

$S = (P_n)_n$ a sequence of special projections is a q-Σ^0_1 class if

1. $P_n \in L_n$
2. An index for P_n as a computable matrix can be obtained uniformly in n.
3. $\mathrm{rng}(P_n) \subseteq \mathrm{rng}(P_{n+1})$.

- Let $\rho = (\rho_n)_n$ be a state.

Definition: q-Σ^0_1 class

$S = (P_n)_n$ a sequence of special projections is a q-Σ^0_1 class if

1. $P_n \in L_n$
2. An index for P_n as a computable matrix can be obtained uniformly in n.
3. $\text{rng}(P_n) \subseteq \text{rng}(P_{n+1})$.

- Let $\rho = (\rho_n)_n$ be a state.
- Each $P_n \in L_n$ is a measurement of the first n qubits.

Definition: q-Σ_1^0 class

$S = (P_n)_n$ a sequence of special projections is a q-Σ_1^0 class if

1. $P_n \in L_n$
2. An index for P_n as a computable matrix can be obtained uniformly in n.
3. $\text{rng}(P_n) \subseteq \text{rng}(P_{n+1})$.

- Let $\rho = (\rho_n)_n$ be a state.
- Each $P_n \in L_n$ is a measurement of the first n qubits.
- So, S is a sequence of measurements on longer and longer initial segments of a state, ρ.

Definition

$\rho(S) := lim_n Tr(\rho_n P_n) = sup_n Tr(\rho_n P_n)$

- Take the classical Σ^0_1 class S as before.

$$S = \bigcup_n [\![A_n]\!]$$

The measure of S is $lim_n(2^{-n}|A_n|)$.

- Take the classical Σ^0_1 class S as before.

$$S = \bigcup_n [\![A_n]\!]$$

  The measure of S is $lim_n(2^{-n}|A_n|)$.
- Analogously, we define the 'measure' of $G = (P_n)_n$, a q-Σ^0_1 to be $lim_n 2^{-n}\text{rank}(P_n)$.

- Take the classical Σ^0_1 class S as before.

$$S = \bigcup_n [\![A_n]\!]$$

The measure of S is $lim_n(2^{-n}|A_n|)$.

- Analogously, we define the 'measure' of $G = (P_n)_n$, a q-Σ^0_1 to be $lim_n 2^{-n}\text{rank}(P_n)$.
- If we define the state $\tau := (2^{-n} I_{2^n})_n$, then $\tau(G) = lim_n 2^{-n}\text{rank}(P_n)$.

- Take the classical Σ_1^0 class S as before.

$$S = \bigcup_n [\![A_n]\!]$$

The measure of S is $lim_n(2^{-n}|A_n|)$.

- Analogously, we define the 'measure' of $G = (P_n)_n$, a q-Σ_1^0 to be $lim_n 2^{-n}\text{rank}(P_n)$.
- If we define the state $\tau := (2^{-n} I_{2^n})_n$, then $\tau(G) = lim_n 2^{-n}\text{rank}(P_n)$.
- With this notion of measure, we can finally define randomness...

Table of Contents

Quantum Martin-Löf Randomness

Definition: quantum-Martin-Löf test (q-MLT)

A uniformly computable sequence $(G_m)_m$ of $q - \Sigma_0^1$ classes is a (q-MLT) if $\tau(G_m) \leqslant 2^{-m}$ for each m.

Definition: Passing and Failing a q-MLT at order δ

A state ρ fails a q-MLT $G = (G_m)_m$ at *order* δ if $\rho(G_m) > \delta$ for each m. ρ passes G at order δ if it does not fail G at order δ. I.e, $\exists m, \rho(G_m) \leqslant \delta$.

Definition: Passing a q-MLT

ρ passes a q-MLT $G = (G_m)_m$ if it passes G at order δ for all $\delta > 0$. I.e, $inf_m \rho(G_m) = 0$. ρ is *quantum-Martin-Löf Random (q-MLR)* if it passes each q-MLT.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.
- Work in progress: Characterize computable q-MLR states.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leqslant 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leqslant 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of τ is uniform and so has maximum entropy.

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leqslant 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of τ is uniform and so has maximum entropy.
- Entropy may provide a characterization?

Computable states can be random

- The state $\tau = (2^{-n} I_{2^n})_n$ is computable.
- By definition of a q-MLT, τ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leqslant 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of τ is uniform and so has maximum entropy.
- Entropy may provide a characterization?
- Partial progress: If $\rho = (\rho_n)_n$ is computable, then

$$\exists c \forall n [H(\rho_n) > n - c] \Rightarrow \rho \text{ is q-MLR} \Rightarrow \liminf_n [H(\rho_n)/n] = 1.$$

.

Questions

- Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?

Questions

- Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?
- We define such a notion and show it to be equivalent to q-MLR.

Questions

- Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?
- We define such a notion and show it to be equivalent to q-MLR.
- Q (Nies and Scholz): Is the set of q-MLR states closed under taking finite convex combinations?

Questions

- Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?
- We define such a notion and show it to be equivalent to q-MLR.
- Q (Nies and Scholz): Is the set of q-MLR states closed under taking finite convex combinations?
- Yes.

Questions

- Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?
- We define such a notion and show it to be equivalent to q-MLR.
- Q (Nies and Scholz): Is the set of q-MLR states closed under taking finite convex combinations?
- Yes.
- The proof uses the equivalence of q-SR and q-MLR.

Definitions

A Quantum Solovay Test (q-ST)

is a uniformly computable sequence of q-Σ^0_1 sets, $(S^k)_{k\in\omega}$ such that

$$\sum_{k\in\omega} \tau(S^k) < \infty$$

Failing and Passing a (q-ST) at level δ

Let $0 < \delta < 1$. ρ fails the q-ST $(S^k)_{k\in\omega}$ at level δ if $\exists^\infty k$ such that $\rho(S^k) > \delta$. Otherwise, ρ passes $(S^k)_{k\in\omega}$ at level δ.

-

Failing and Passing a (q-ST) at level δ

Let $0 < \delta < 1$. ρ fails the q-ST $(S^k)_{k\in\omega}$ at level δ if $\exists^\infty k$ such that $\rho(S^k) > \delta$. Otherwise, ρ passes $(S^k)_{k\in\omega}$ at level δ.

-

Quantum Solovay Randomness (q-SR)

ρ passes a q-ST $(S^k)_{k\in\omega}$ if for all δ, ρ passes $(S^k)_{k\in\omega}$ at level δ. ρ is q-SR if it passes all q-STs.

-

Theorem (B.)

For all states ρ, ρ is q-SR if and only if ρ is q-MLR.

Theorem (B.)

For all states ρ, ρ is q-SR if and only if ρ is q-MLR.

- ($\Longrightarrow$) A q-MLT is a q-ST $\square$.

Theorem (B.)

For all states ρ, ρ is q-SR if and only if ρ is q-MLR.

- ($\Longrightarrow$) A q-MLT is a q-ST $\square$.
- ($\Longleftarrow$) let $\rho = (\rho_n)_{n\in\omega}$ fail a q-ST $(S^k)_{k\in\omega}$ at level δ. Build a q-MLT $(G^m)_{m\in\omega}$, with $G^m = (G^m_n)_{n\in\omega}$, which ρ fails at level $\delta^2/72$.

Theorem (B.)

For all states ρ, ρ is q-SR if and only if ρ is q-MLR.

- ($\Longrightarrow$) A q-MLT is a q-ST $\square$.
- ($\Longleftarrow$) let $\rho = (\rho_n)_{n\in\omega}$ fail a q-ST $(S^k)_{k\in\omega}$ at level δ. Build a q-MLT $(G^m)_{m\in\omega}$, with $G^m = (G^m_n)_{n\in\omega}$, which ρ fails at level $\delta^2/72$.
- WLOG, $S^k_n = \varnothing$ for $n > k$.

Theorem (B.)

For all states ρ, ρ is q-SR if and only if ρ is q-MLR.

- $(\Longrightarrow)$ A q-MLT is a q-ST $\square$.
- $(\Longleftarrow)$ let $\rho = (\rho_n)_{n\in\omega}$ fail a q-ST $(S^k)_{k\in\omega}$ at level δ. Build a q-MLT $(G^m)_{m\in\omega}$, with $G^m = (G^m_n)_{n\in\omega}$, which ρ fails at level $\delta^2/72$.
- WLOG, $S^k_n = \varnothing$ for $n > k$.
- Notation:

$$A^m_t = \{\psi \in \mathbb{C}^{2^t}_{alg} : ||\psi|| = 1, \sum_{k \leqslant t} \mathrm{Tr}(|\psi\rangle\langle\psi| S^k_t) > \frac{2^m\delta}{6}\},$$

for $t, m \in \omega$. We may skip the proof in the interests of time and go straight to the application.

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

- Towards a contradiction,

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

- Towards a contradiction,
- let there be a q-MLT, $(G^m)_{m \in \omega}$ and a $\delta > 0$ such that $\forall m \in \omega$, $\rho(G^m) > \delta$.

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

- Towards a contradiction,
- let there be a q-MLT, $(G^m)_{m\in\omega}$ and a $\delta > 0$ such that $\forall m \in \omega$, $\rho(G^m) > \delta$.
- So, $\forall m \in \omega$, $\exists n$ such that $\mathrm{Tr}(\rho_n G_n^m) > \delta$ where $\rho_n = \sum_{i<k} \alpha_i \rho_n^i$.

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

- Towards a contradiction,
- let there be a q-MLT, $(G^m)_{m \in \omega}$ and a $\delta > 0$ such that $\forall m \in \omega$, $\rho(G^m) > \delta$.
- So, $\forall m \in \omega$, $\exists n$ such that $\mathrm{Tr}(\rho_n G_n^m) > \delta$ where $\rho_n = \sum_{i<k} \alpha_i \rho_n^i$.
- I.e, $\forall m \in \omega$, $\exists n$ such that

$$\delta < \mathrm{Tr}(\sum_{i<k} \alpha_i \rho_n^i G_n^m) = \sum_{i<k} \alpha_i \mathrm{Tr}(\rho_n^i G_n^m).$$

Corollary (B.): The set of q-MLR states is convex

A finite convex combination of q-MLR states is q-MLR: If $(\rho^i)_{i<k}$ are q-MLR and $\sum_{i<k} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-MLR.

- Towards a contradiction,
- let there be a q-MLT, $(G^m)_{m \in \omega}$ and a $\delta > 0$ such that $\forall m \in \omega$, $\rho(G^m) > \delta$.
- So, $\forall m \in \omega$, $\exists n$ such that $\mathrm{Tr}(\rho_n G^m_n) > \delta$ where $\rho_n = \sum_{i<k} \alpha_i \rho^i_n$.
- I.e, $\forall m \in \omega$, $\exists n$ such that

$$\delta < \mathrm{Tr}(\sum_{i<k} \alpha_i \rho^i_n G^m_n) = \sum_{i<k} \alpha_i \mathrm{Tr}(\rho^i_n G^m_n).$$

- By convexity there must be an i such that $\mathrm{Tr}(G^m_n \rho^i_n) > \delta$

- So, $\forall m\ \exists n, i$ such that $\mathrm{Tr}\left(\rho_n^i G_n^m\right) > \delta$.

- So, $\forall m \; \exists n, i$ such that $\mathrm{Tr}\left(\rho_n^i G_n^m\right) > \delta$.
- There are only finitely many i s.

- So, $\forall m \; \exists n, i$ such that $\text{Tr}\left(\rho_n^i G_n^m\right) > \delta$.
- There are only finitely many i s.
- By pigeonhole, there is an i such that $\exists^\infty m$ with $\text{Tr}\left(\rho_n^i G_n^m\right) > \delta$, for some n.

- So, $\forall m \; \exists n, i$ such that Tr $(\rho^i_n G^m_n) > \delta$.
- There are only finitely many i s.
- By pigeonhole, there is an i such that $\exists^\infty m$ with Tr $(\rho^i_n G^m_n) > \delta$, for some n.
- So, $\exists^\infty m$ with $\rho^i(G^m) > \delta$.

- So, $\forall m\ \exists n, i$ such that Tr $(\rho^i_n G^m_n) > \delta$.
- There are only finitely many i s.
- By pigeonhole, there is an i such that $\exists^\infty m$ with Tr $(\rho^i_n G^m_n) > \delta$, for some n.
- So, $\exists^\infty m$ with $\rho^i(G^m) > \delta$.
- So, ρ^i fails the q-Solovay test $(G^m)_{m\in\omega}$ and hence is not q-MLR by our previous result.

Thank You

Table of Contents

Constructing the q-MLT test

- Build $G^m = (G^m_n)_n$: Procedure to build G^m_n.

Constructing the q-MLT test

- Build $G^m = (G^m_n)_n$: Procedure to build G^m_n.
- Say we are given C^m_{n-1}, a maximal (under set inclusion) orthonormal subset of A^m_{n-1}, and $G^m_{n-1} = \{|\psi\rangle\langle\psi| : \psi \in C^m_{n-1}\}$. Let

$$D^m_n = \{|\psi\rangle \otimes |i\rangle : i \in \{1, 0\}, \psi \in C^m_{n-1}\}.$$

Easy to see that $D^m_n \subseteq A^m_n$ since $C^m_{n-1} \subseteq A^m_{n-1}$.

Constructing the q-MLT test

- Build $G^m = (G^m_n)_n$: Procedure to build G^m_n.
- Say we are given C^m_{n-1}, a maximal (under set inclusion) orthonormal subset of A^m_{n-1}, and $G^m_{n-1} = \{|\psi\rangle\langle\psi| : \psi \in C^m_{n-1}\}$. Let

$$D^m_n = \{|\psi\rangle \otimes |i\rangle : i \in \{1, 0\}, \psi \in C^m_{n-1}\}.$$

  Easy to see that $D^m_n \subseteq A^m_n$ since $C^m_{n-1} \subseteq A^m_{n-1}$.
- Let C^m_n be S where S is a maximal orthonormal set such that $D^m_n \subseteq S \subseteq A^m_n$.
  Let $G^m_n = \{|\psi\rangle\langle\psi| : \psi \in C^m_n\}$.
  End

Verification

Lemma

For each m, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set.

Verification

Lemma

For each m, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set.

- Given C^m_{n-1}, we built C^m_n in stages t. $C^m_{n,0} = D^m_n$. To compute $C^m_{n,s}$ given $C^m_{n,s-1}$, check if:

$$\exists \tau \in A^m_n \text{ such that } \forall \psi \in C^m_{n,s-1}, \langle \tau|\psi\rangle = 0.$$

This check is decidable as $Th(\mathbb{C}_{alg})$ is.

Verification

Lemma

For each m, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set.

- Given C^m_{n-1}, we built C^m_n in stages t. $C^m_{n,0} = D^m_n$. To compute $C^m_{n,s}$ given $C^m_{n,s-1}$, check if:

$$\exists \tau \in A^m_n \text{ such that } \forall \psi \in C^m_{n,s-1}, \langle \tau | \psi \rangle = 0.$$

  This check is decidable as $Th(\mathbb{C}_{alg})$ is.
- If yes, find a witness τ and set $C^m_{n,s} = \{\tau\} \cup C^m_{n,s-1}$. If no, set $C^m_n = C^m_{n,s-1}$ and stop. By finite dimensionality, at some stage we must stop.

Verification

Lemma

For each m, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set.

- Given C^m_{n-1}, we built C^m_n in stages t. $C^m_{n,0} = D^m_n$. To compute $C^m_{n,s}$ given $C^m_{n,s-1}$, check if:

  $$\exists\tau \in A^m_n \text{ such that } \forall\psi \in C^m_{n,s-1}, \langle\tau|\psi\rangle = 0.$$

  This check is decidable as $Th(\mathbb{C}_{alg})$ is.
- If yes, find a witness τ and set $C^m_{n,s} = \{\tau\} \cup C^m_{n,s-1}$. If no, set $C^m_n = C^m_{n,s-1}$ and stop. By finite dimensionality, at some stage we must stop.
- So, $(G^m_n)_{n\in\omega}$ is a uniformly computable sequence.

Verification

Lemma

For each m, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set.

- Given C^m_{n-1}, we built C^m_n in stages t. $C^m_{n,0} = D^m_n$. To compute $C^m_{n,s}$ given $C^m_{n,s-1}$, check if:

$$\exists \tau \in A^m_n \text{ such that } \forall \psi \in C^m_{n,s-1}, \langle \tau | \psi \rangle = 0.$$

  This check is decidable as $Th(\mathbb{C}_{alg})$ is.
- If yes, find a witness τ and set $C^m_{n,s} = \{\tau\} \cup C^m_{n,s-1}$. If no, set $C^m_n = C^m_{n,s-1}$ and stop. By finite dimensionality, at some stage we must stop.
- So, $(G^m_n)_{n\in\omega}$ is a uniformly computable sequence.
- By construction, range$(G^m_{n-1} \otimes I_2) \subset$ range(G^m_n). □

Lemma

$(G^m)_{m\in\omega}$ is a q-MLT.

Lemma

$(G^m)_{m\in\omega}$ is a q-MLT.

- $$1 \geqslant \sum_k \tau(S^k) \geqslant \sum_k 2^{-n}\mathrm{Tr}(S^k_n),$$

  by definition

Lemma

$(G^m)_{m\in\omega}$ is a q-MLT.

- $$1 \geqslant \sum_k \tau(S^k) \geqslant \sum_k 2^{-n}\mathrm{Tr}(S_n^k),$$
  by definition
- For fixed m, n we have that,
  $$\begin{aligned} 2^n &\geqslant \sum_k \mathrm{Tr}(S_n^k) \\ &\geqslant \sum_k \mathrm{Tr}(\sum_{\psi\in C_n^m} |\psi\rangle\langle\psi|S_n^k) \\ &= \sum_{\psi\in C_n^m}\sum_k \mathrm{Tr}(|\psi\rangle\langle\psi|S_n^k) \\ &> |C_n^m|\frac{2^m\delta}{6} \\ &= \mathrm{Tr}(G_n^m)\frac{2^m\delta}{6}. \quad \square \end{aligned}$$

Lemma:

ρ fails $(G^m)_m$ at level $\delta^2/72$. Or, for all $m \in \omega$, there is an n such that

$$\mathrm{Tr}(\rho_n G_n^m) \geqslant \frac{\delta^2}{72}.$$

Lemma:

ρ fails $(G^m)_m$ at level $\delta^2/72$. Or, for all $m \in \omega$, there is an n such that

$$\mathrm{Tr}(\rho_n G_n^m) \geqslant \frac{\delta^2}{72}.$$

- Let m be arbitrary.

Lemma:

ρ fails $(G^m)_m$ at level $\delta^2/72$. Or, for all $m \in \omega$, there is an n such that

$$\mathrm{Tr}(\rho_n G_n^m) \geqslant \frac{\delta^2}{72}.$$

- Let m be arbitrary.
- Fix a n so that there exist 2^m many ks less than n such that $\mathrm{Tr}(\rho_n S_n^k) > \delta$.

Lemma:

ρ fails $(G^m)_m$ at level $\delta^2/72$. Or, for all $m \in \omega$, there is an n such that

$$\mathrm{Tr}(\rho_n G_n^m) \geqslant \frac{\delta^2}{72}.$$

- Let m be arbitrary.
- Fix a n so that there exist 2^m many ks less than n such that $\mathrm{Tr}(\rho_n S_n^k) > \delta$.
- Case 1: ρ_n is algebraic:

$$\rho_n = \sum_{i \leqslant 2^n} \alpha_i |\psi^i\rangle\langle\psi^i|$$

$\sum_{i \leqslant 2^n} \alpha_i = 1$ and for each i, $|\psi^i\rangle \in \mathbb{C}^{2^n}_{alg}$ and $||\psi^i|| \leqslant 1$.

- Fix $i \leqslant 2^n$; let $\psi = \psi^i$. Write

$$\psi = c_o\psi_o + c_p\psi_p$$

where $\psi_o \in \text{range}(G_n^m)$ and $\psi_p \in \text{range}(G_n^m)^\perp$ are unit vectors, $c_o, c_p \in \mathbb{C}$ and $|c_0|^2 + |c_p|^2 = ||\psi||^2 \leqslant 1$.

- Fix $i \leqslant 2^n$; let $\psi = \psi^i$. Write

$$\psi = c_o\psi_o + c_p\psi_p$$

where $\psi_o \in \text{range}(G_n^m)$ and $\psi_p \in \text{range}(G_n^m)^\perp$ are unit vectors, $c_o, c_p \in \mathbb{C}$ and $|c_0|^2 + |c_p|^2 = ||\psi||^2 \leqslant 1$.

- For a k, let $S_n^k = S$. An easy, but long, calculation shows:

$$Tr(S|\psi\rangle\langle\psi|) \leqslant$$

$$|c_o|^2\langle S\psi_o|S\psi_o\rangle + |c_p|^2\langle S\psi_p|S\psi_p\rangle + 2|c_o||c_p||\langle S\psi_p|S\psi_o\rangle|$$

- By Cauchy-Schwarz:

$$
\begin{aligned}
|\langle S\psi_p|S\psi_o\rangle| &\leqslant ||S\psi_o||||S\psi_p|| \\
&\leqslant (\max\{||S\psi_o||, ||S\psi_p||\})^2 \\
&\leqslant ||S\psi_o||^2 + ||S\psi_p||^2.
\end{aligned}
$$

- By Cauchy-Schwarz:

$$\begin{aligned}|\langle S\psi_p|S\psi_o\rangle| &\leqslant ||S\psi_o||||S\psi_p|| \\ &\leqslant (\max\{||S\psi_o||, ||S\psi_p||\})^2 \\ &\leqslant ||S\psi_o||^2 + ||S\psi_p||^2.\end{aligned}$$

- Using this and that $|c_o|, |c_p| \leqslant 1$,
  $\mathrm{Tr}(S|\psi\rangle\langle\psi|)$

$$\begin{aligned}&\leqslant |c_o|^2\langle S\psi_o|S\psi_o\rangle + |c_p|^2\langle S\psi_p|S\psi_p\rangle + 2|c_o||c_p|(||S\psi_o||^2 + ||S\psi_p||^2) \\ &\leqslant |c_o|\langle S\psi_o|S\psi_o\rangle + |c_p|\langle S\psi_p|S\psi_p\rangle + 2|c_o|||S\psi_o||^2 + 2|c_p|||S\psi_p||^2 \\ &= 3(|c_o|\langle S\psi_o|S\psi_o\rangle + |c_p|\langle S\psi_p|S\psi_p\rangle)\end{aligned}$$

By the choice of n, pick $M \subseteq \{1, 2 \ldots n\}$ such that $|M| = 2^m$ and $\mathrm{Tr}(\rho_n S_n^k) > \delta$ for each k in M.

$$\begin{aligned}
2^m \delta &< \sum_{k \in M} \mathrm{Tr}(\rho_n S_n^k) \\
&= \sum_{k \in M} \mathrm{Tr}\Big(\sum_{i \leqslant 2^n} \alpha_i |\psi^i\rangle\langle\psi^i| S_n^k \Big) \\
&= \sum_{k \in M} \sum_{i \leqslant 2^n} \alpha_i \mathrm{Tr}(|\psi^i\rangle\langle\psi^i| S_n^k) \\
&= \sum_{i \leqslant 2^n} \alpha_i \sum_{k \in M} \mathrm{Tr}(|\psi^i\rangle\langle\psi^i| S_n^k) \\
&\leqslant \sum_{i \leqslant 2^n} \alpha_i \sum_{k \in M} 3(|c_o^i| \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + |c_p^i| \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle).
\end{aligned}$$

So,

$$\frac{2^m\delta}{3} < \sum_{i\leqslant 2^n} \alpha_i \sum_{k\in M} \left(|c_o^i|\left\langle S_n^k \psi_o^i | S_n^k \psi_o^i \right\rangle + |c_p^i|\left\langle S_n^k \psi_p^i | S_n^k \psi_p^i \right\rangle\right)$$

$$= \sum_{i\leqslant 2^n} \alpha_i |c_o^i| \sum_{k\in M} \left\langle S_n^k \psi_o^i | S_n^k \psi_o^i \right\rangle + \sum_{i\leqslant 2^n} \alpha_i |c_p^i| \sum_{k\in M} \left\langle S_n^k \psi_p^i | S_n^k \psi_p^i \right\rangle$$

So,

$$\frac{2^m\delta}{3} < \sum_{i\leqslant 2^n} \alpha_i \sum_{k\in M} \left(|c_o^i|\left\langle S_n^k\psi_o^i|S_n^k\psi_o^i\right\rangle + |c_p^i|\left\langle S_n^k\psi_p^i|S_n^k\psi_p^i\right\rangle\right)$$

$$= \sum_{i\leqslant 2^n} \alpha_i|c_o^i| \sum_{k\in M} \left\langle S_n^k\psi_o^i|S_n^k\psi_o^i\right\rangle + \sum_{i\leqslant 2^n} \alpha_i|c_p^i| \sum_{k\in M} \left\langle S_n^k\psi_p^i|S_n^k\psi_p^i\right\rangle$$

- We now bound the second sum on the right-hand side.

So,

$$\frac{2^m\delta}{3} < \sum_{i\leqslant 2^n} \alpha_i \sum_{k\in M} (|c_o^i|\langle S_n^k\psi_o^i|S_n^k\psi_o^i\rangle + |c_p^i|\langle S_n^k\psi_p^i|S_n^k\psi_p^i\rangle)$$
$$= \sum_{i\leqslant 2^n} \alpha_i|c_o^i| \sum_{k\in M} \langle S_n^k\psi_o^i|S_n^k\psi_o^i\rangle + \sum_{i\leqslant 2^n} \alpha_i|c_p^i| \sum_{k\in M} \langle S_n^k\psi_p^i|S_n^k\psi_p^i\rangle$$

- We now bound the second sum on the right-hand side.
- Make a key use of the maximality of the orthonormal subset chosen during the construction.

- $\forall i,\ \psi_p^i \in \mathrm{range}(G_n^m)^{\perp} \cap \mathbb{C}_{alg}^{2^n}$.

- $\forall i$, $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$.
- Hence, ψ_p^i is perpendicular to each element of C_n^m.

- $\forall i$, $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$.
- Hence, ψ_p^i is perpendicular to each element of C_n^m.
- If $\psi_p^i \in A_n^m$, then $\{\psi_p^i\} \cup C_n^m$ is a orthonormal subset of A_n^m strictly containing C_n^m, contradicting the maximality of C_n^m.

- $\forall i$, $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$.
- Hence, ψ_p^i is perpendicular to each element of C_n^m.
- If $\psi_p^i \in A_n^m$, then $\{\psi_p^i\} \cup C_n^m$ is a orthonormal subset of A_n^m strictly containing C_n^m, contradicting the maximality of C_n^m.
- So, $\psi_p^i \notin A_n^m$ for each i.

- $\forall i$, $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$.
- Hence, ψ_p^i is perpendicular to each element of C_n^m.
- If $\psi_p^i \in A_n^m$, then $\{\psi_p^i\} \cup C_n^m$ is a orthonormal subset of A_n^m strictly containing C_n^m, contradicting the maximality of C_n^m.
- So, $\psi_p^i \notin A_n^m$ for each i.
- But, $\psi_p^i \in \mathbb{C}_{alg}^{2^n}$ and $||\psi_p^i|| = 1$. So the only way $\psi_p^i \notin A_n^m$ is if

- $\forall i$, $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$.
- Hence, ψ_p^i is perpendicular to each element of C_n^m.
- If $\psi_p^i \in A_n^m$, then $\{\psi_p^i\} \cup C_n^m$ is a orthonormal subset of A_n^m strictly containing C_n^m, contradicting the maximality of C_n^m.
- So, $\psi_p^i \notin A_n^m$ for each i.
- But, $\psi_p^i \in \mathbb{C}_{alg}^{2^n}$ and $||\psi_p^i|| = 1$. So the only way $\psi_p^i \notin A_n^m$ is if
- $$\sum_{k \leqslant n} \text{Tr}(|\psi_p^i\rangle\langle\psi_p^i|S_n^k) \leqslant \frac{2^m\delta}{6}.$$

Recall

We are trying to bound from above the second term on the right hand side of

$$\frac{2^m\delta}{3} < \sum_{i\leqslant 2^n} \alpha_i |c_o^i| \sum_{k\in M} \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + \sum_{i\leqslant 2^n} \alpha_i |c_p^i| \sum_{k\in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle$$

- So, bound the sum as follows:

$$\sum_{i \leqslant 2^n} \alpha_i |c_p^i| \sum_{k \in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle$$

$$\leqslant \sum_{i \leqslant 2^n} \alpha_i |c_p^i| \frac{2^m \delta}{6} < \sum_{i \leqslant 2^n} \alpha_i \frac{2^m \delta}{6} \leqslant \frac{2^m \delta}{6}$$

- So, bound the sum as follows:

$$\sum_{i \leqslant 2^n} \alpha_i |c_p^i| \sum_{k \in M} \left\langle S_n^k \psi_p^i | S_n^k \psi_p^i \right\rangle$$

$$\leqslant \sum_{i \leqslant 2^n} \alpha_i |c_p^i| \frac{2^m \delta}{6} < \sum_{i \leqslant 2^n} \alpha_i \frac{2^m \delta}{6} \leqslant \frac{2^m \delta}{6}$$

- This means:

$$\sum_{i \leqslant 2^n} \alpha_i |c_o^i| \sum_{k \in M} \left\langle S_n^k \psi_o^i | S_n^k \psi_o^i \right\rangle > \frac{2^m \delta}{6}$$

- $|\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle| \leqslant 1$ and $|M| = 2^m$

- $|\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle| \leqslant 1$ and $|M| = 2^m$
- So, cancel the 2^ms to get:

$$\frac{\delta}{6} < \sum_{i \leqslant 2^n} \alpha_i |c_o^i|.$$

- $|\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle| \leqslant 1$ and $|M| = 2^m$
- So, cancel the 2^ms to get:

$$\frac{\delta}{6} < \sum_{i \leqslant 2^n} \alpha_i |c_o^i|.$$

- As $\sum_{i \leqslant 2^n} \alpha_i = 1$, by Jensen's inequality:

$$\frac{\delta^2}{36} < \Big(\sum_{i \leqslant 2^n} \alpha_i |c_o^i| \Big)^2 \leqslant \sum_{i \leqslant 2^n} \alpha_i |c_o^i|^2$$

- $|\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle| \leqslant 1$ and $|M| = 2^m$
- So, cancel the 2^ms to get:

$$\frac{\delta}{6} < \sum_{i \leqslant 2^n} \alpha_i |c_o^i|.$$

- As $\sum_{i \leqslant 2^n} \alpha_i = 1$, by Jensen's inequality:

$$\frac{\delta^2}{36} < \Big(\sum_{i \leqslant 2^n} \alpha_i |c_o^i| \Big)^2 \leqslant \sum_{i \leqslant 2^n} \alpha_i |c_o^i|^2$$

- Finally, it is easy to see that

$$Tr(\rho_n G_n^m) = \sum_{i \leqslant 2^n} \alpha_i \mathrm{Tr}(|c_o^i \psi_o^i\rangle\langle c_o^i \psi_o^i|)$$

$$= \sum_{i \leqslant 2^n} \alpha_i |c_o^i|^2 > \frac{\delta^2}{36}$$

- Case 2: ρ_n is not expressible as a convex sum of algebraic projections.
- Since $\{\psi \in \mathbb{C}_{alg}^{2^n} : ||\psi|| \leqslant 1\}$ is dense in the closed unit ball in $\mathbb{C}^{2^n}$, using case 1, we see that $Tr(\rho_n G_n^m) > \dfrac{\delta^2}{72}$