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

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 $\psi \psi^* \dagger$ where $\psi$ is a unit column vector ($\psi^*$ is the complex conjugate transpose of $\psi$). Fix a orthonormal basis $b_1, \ldots, b_n$ of $\mathbb{C}^n$. The $b_i b_i^*$ will be the classical states. A measurement is represented by a matrix $H$ with eigenvectors $b_1, \ldots, b_n$ with eigenvalues equalling 0 or 1. So, $H$ is a Hermitian projection.
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. Its 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 \( \psi \psi^\dagger \) where \( \psi \) is a unit column vector \( (\psi^\dagger \) is the complex conjugate transpose of \( \psi \)).

Fix a orthonormal basis \( b_1, \ldots, b_n \) of \( \mathbb{C}^n \). The \( b_i b_i^\dagger \)s will be the classical states. A measurement is represented by a matrix \( H \) with eigenvectors \( b_1, \ldots, b_n \) with eigenvalues equalling 0 or 1. So, \( H \) is a Hermitian projection.
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.
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’.

Let us formalize this.

We represent a n-dimensional system by a matrix $\psi\psi^*$ where $\psi$ is a unit column vector ($\psi^*$ is the complex conjugate transpose of $\psi$).

Fix a orthonormal basis $b_1,..,b_n$ of $C^n$. The $b_i b_i^{\ast}$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.
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.
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 ($\psi^*$ is the complex conjugate transpose of $\psi$).
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 ($\psi^*$ is the complex conjugate transpose of $\psi$).

Fix a orthonormal basis $b_1, \ldots, b_n$ 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 ($\psi^*$ is the complex conjugate transpose of $\psi$).
- Fix a orthonormal basis $b_1, \ldots, b_n$ of $\mathbb{C}^n$. The $b_ib_i^*$ s will be the classical states.
- A measurement is represented by a matrix $H$ with eigenvectors $b_1, \ldots, b_n$ 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 $H b_i = e_i b_i$ (i.e., the eigenvalue corresponding to $b_i$.)
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 $H b_i = e_i b_i$ (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 $\text{Trace}(H\psi\psi^*)$. 
A qubit is a 2-dimensional system.
Qubits

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

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector \( \nu \) by \( |\nu\rangle \) and \( \nu^* \) by \( \langle \nu| \).
- 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 an orthonormal basis.
Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector \( \nu \) by \( |\nu\rangle \) and \( \nu^* \) by \( \langle \nu| \).
- 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 \( |1\rangle \).
A qubit is a 2-dimensional system.

Bra-Ket notation: denote a column vector \( \nu \) by \( |\nu\rangle \) and \( \nu^* \) by \( \langle \nu| \).

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 an orthonormal basis.

Denote \( V_0, V_1 \) by \( |0\rangle \) and \( |1\rangle \).

So, \((\mathbb{C}^2)^\otimes n := H_n\) has an orthonormal basis comprised of elements of the form: Fix a \( \sigma \in 2^n \). The basis vector given by this \( \sigma \) 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. A pure state is a single quantum system while a mixed state is a probabilistic mixture of pure states.
A qubit is a 2-dimensional system.

Bra-Ket notation: denote a column vector \( \mathbf{v} \) by \(|\mathbf{v}\rangle\) and \(\mathbf{v}^*\) by \(\langle \mathbf{v} |\).

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 an orthonormal basis.

Denote \( V_0, V_1 \) by \(|0\rangle\) and \(|1\rangle\).

So, \((\mathbb{C}^2)^\otimes n := H_n\) has an orthonormal basis comprised of elements of the form: Fix a \( \sigma \in 2^n \). The basis vector given by this \( \sigma \) 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 qubit is a 2-dimensional system.

Bra-Ket notation: denote a column vector $v$ by $|v\rangle$ and $v^\ast$ 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 an orthonormal basis.

Denote $V_0, V_1$ by $|0\rangle$ and $|1\rangle.$

So, $(\mathbb{C}^2)^\otimes n := H_n$ has an orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n.$ The basis vector given by this $\sigma$ 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.
Qubits

- A qubit is a 2-dimensional system.
- Bra-Ket notation: denote a column vector $\nu$ by $|\nu\rangle$ and $\nu^*$ by $\langle\nu|$.
- 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 an orthonormal basis.
- Denote $V_0, V_1$ by $|0\rangle$ and $|1\rangle$.
- So, $(\mathbb{C}^2)^\otimes n := H^n$ has an orthonormal basis comprised of elements of the form: Fix a $\sigma \in 2^n$. The basis vector given by this $\sigma$ 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.
- A pure state is a single quantum system while a mixed state is a probabilistic mixture of pure states.
The mixed and pure states are called density matrices.
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 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 $\rho$ on $H_n$ has $\text{Trace}(\rho)=1$, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. If the eigenpairs are $(\alpha_i, \psi_i)$, then

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

The sum is convex as $1=\text{Tr}(\rho)=\sum_i \alpha_i$. So, $\rho$ 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 $\rho$ on $H_n$ has $\text{Trace}(\rho)=1$, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i < 2^n}$. If the eigenpairs are $(\alpha_i, \psi_i)$, then

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

(1)

The sum is convex as $1=\text{Tr}(\rho)=\sum_i \alpha_i$. So, $\rho$ 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 $\alpha_i$.
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 $\rho$ on $H_n$ has $\text{Trace}(\rho)=1$, then it has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. If the eigenpairs are $(\alpha_i, \psi_i)$, then

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

The sum is convex as $1=\text{Tr}(\rho)=\sum \alpha_i$. So, $\rho$ 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 $\alpha_i$.
- 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 $L(H_n)$. 

Tejas Bhojraj (UW-Madison)  
Quantum Solovay randomness  
Waterloo, June 2018  

7 / 41
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 $\rho$ is called entangled.
Partial Trace

Given \( \rho \), we want to find the state given by ignoring the last \( n \) qubit. What does 'ignoring' mean?

It means we need a \( \tau \) which describes measurements of the first \( n \) qubits of \( \rho \). I.e, we need a \( \tau \) such that for any hermitian \( O \) :

\[
\text{Tr}(\tau O) = \text{Tr}(\rho O I_{qq}) .
\]

(Recall: The expectation of measuring \( O \) on \( \phi \) is \( \text{Tr}(\phi O) \).)

If \( \rho = \lambda \sigma \) for a \( \lambda \) and \( \sigma \) then, 

\[
\text{Tr}(\rho O I_{qq}) = \text{Tr}(\lambda \sigma I_{q'}) \text{Tr}(\rho O q').
\]

So, \( \tau = \lambda \) works.

If \( \rho \) is entangled, the choice of \( \tau \) is not so obvious.
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?
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 $\rho$. 

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 $\rho$.

I.e, we need a $\tau$ such that for any hermitian $O \in L_n$,

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

I.e, we need a $\tau$ such that for any hermitian $O \in L_n$,

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

(Recall: The expectation of measuring $O$ on $\phi$ is $\text{Tr}(\phi O)$.)
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 $\rho$.
- I.e, we need a $\tau$ such that for any hermitian $O \in L_n$,

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

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

$$\text{Tr}(\rho (O \otimes I)) = \text{Tr}(\lambda O \otimes \sigma I) = \text{Tr}(\lambda O) \text{Tr}(\sigma) = \text{Tr}(\lambda O)$$

So, $\tau = \lambda$ works.
- If $\rho$ is entangled, the choice of $\tau$ is not so obvious
Denote \( L(H_n) \) by \( L_n \). Define

\[
T_1 : L_{n+1} \rightarrow L_n
\]

by \( T_1(A \otimes B) := A \ast Tr(B) \) 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 $T_1(A \otimes B) := A \ast Tr(B)$ 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 $\alpha_i, A_i \in L_n$ 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 $T_1(A \otimes B) := A \ast Tr(B)$ 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 $\alpha_i, A_i \in L_n$ and $B_i \in L_1$. (After modding out by the usual $\equiv$)

It turns out that $T_1(\rho)$ is the required $\tau$
There is an 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 $A \in L(H_n), B \in L(H_1)$,

$$A \otimes B = \begin{bmatrix} Ab_{00} & Ab_{01} \\ Ab_{10} & Ab_{11} \end{bmatrix} \text{ if } B = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix}$$
Let $\rho \in L_{n+1}$

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

be with each block in $L_n$
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

$$|\psi\rangle\langle\psi| = (|00\rangle\langle00| + |00\rangle\langle11| + |11\rangle\langle00| + |11\rangle\langle11|)/2$$
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

$$|\psi\rangle\langle\psi| = (|00\rangle\langle00| + |00\rangle\langle11| + |11\rangle\langle00| + |11\rangle\langle11|)/2$$

- 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

$$|\psi\rangle\langle\psi| = (|00\rangle\langle00| + |00\rangle\langle11| + |11\rangle\langle00| + |11\rangle\langle11|)/2$$

- 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)
1 Quantum Mechanics
   - The Density Matrix
   - Partial Trace

2 Quantum Cantor Space
   - Coherent Sequences of Density Matrices
   - Quantum $\Sigma^0_1$-Classes

3 Randomness
   - Quantum Martin-Löf Randomness
   - Computable states can be random

4 Definitions

5 Quantum Solovay Randomness is equivalent to q-MLR

6 The set of q-MLR states is convex
   - Construction
   - Verification
• Now we consider a system of countably infinitely many qubits.
Now we consider a system of countably infinitely many qubits.

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

For each $n$, let $T_n : L_n \rightarrow L_{n-1}$ 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 $T_n : L_n \rightarrow L_{n-1}$ 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 $T_n : L_n \rightarrow L_{n-1}$ 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 $T_n : L_n \rightarrow L_{n-1}$ 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.
A $\Sigma^0_1$ 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. $[A_n] \subseteq [A_{n+1}]$
A $\Sigma^0_1$ 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 $\Sigma_1^0$ class $S \subseteq 2^\omega$ can be written as

$$S = \bigcup_n \llbracket A_n \rrbracket$$

where

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

Extend this to the quantum setting.

A Hermitian projection $P \in L_n$ is said to be *special* if it’s entries are in $\mathbb{C}_{\text{alg}}$ (roots of $\mathbb{Q}$ polynomials); hence computable.
Definition: $q$-$\Sigma^0_1$ class

$S = (P_n)_n$ a sequence of special projections is a $q$-$\Sigma^0_1$ 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 $\rho = p \rho_n q$ be a state. Each $P_n$ is a measurement of the first $n$ qubits. So, $S$ is a sequence of measurements on longer and longer initial segments of a state, $\rho$. 

Definition $\rho \in S$: $\lim_{n} \text{Tr}(\rho_p P_n q) \sup_{n} \text{Tr}(\rho P_n q)$. 

Tejas Bhojraj (UW-Madison) Quantum Solovay randomness Waterloo, June 2018 16 / 41
Definition: q-$\Sigma_1^0$ class

$S = (P_n)_n$ a sequence of special projections is a q-$\Sigma_1^0$ 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.
Definition: $q$-$\Sigma^0_1$ class

$S = (P_n)_n$ a sequence of special projections is a $q$-$\Sigma^0_1$ 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: $\text{q-}\Sigma^0_1$ class

$S = (P_n)_n$ a sequence of special projections is a $\text{q-}\Sigma^0_1$ 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.
- So, $S$ is a sequence of measurements on longer and longer initial segments of a state, $\rho$.

Definition

$\rho(S) := \lim_n \text{Tr}(\rho_n P_n) = \sup_n \text{Tr}(\rho_n P_n)$
Take the classical $\Sigma^0_1$ class $S$ as before.

$$S = \bigcup_n [A_n]$$

The measure of $S$ is $\lim_n (2^{-n}|A_n|)$. 
- Take the classical $\Sigma^0_1$ class $S$ as before.

$$S = \bigcup_n \mathbb{I}[A_n]$$

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

- Analogously, we define the ‘measure’ of $G = (P_n)_n$, a $\Sigma^0_1$ to be $\lim_n 2^{-n}\text{rank}(P_n)$. 
Take the classical $\Sigma^0_1$ class $S$ as before.

$$S = \bigcup_n \llbracket A_n \rrbracket$$

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

Analogously, we define the ‘measure’ of $G = (P_n)_n$, a q-$\Sigma^0_1$ 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 $\Sigma_1^0$ 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 $q$-$\Sigma_1^0$ 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...
Definition: quantum-Martin-Löf test (q-MLT)
A uniformly computable sequence \((G_m)_m\) of \(q - \Sigma^1_0\) classes is a (q-MLT) if 
\[\tau(G_m) \leq 2^{-m}\]
for each \(m\).

Definition: Passing and Failing a q-MLT at order \(\delta\)
A state \(\rho\) fails a q-MLT \(G = (G_m)_m\) at order \(\delta\) if \(\rho(G_m) > \delta\) for each \(m\). \(\rho\) passes \(G\) at order \(\delta\) if it does not fail \(G\) at order \(\delta\). I.e, \(\exists m, \rho(G_m) \leq \delta\).

Definition: Passing a q-MLT
\(\rho\) passes a q-MLT \(G = (G_m)_m\) if it passes \(G\) at order \(\delta\) for all \(\delta > 0\). I.e, \(\inf_m \rho(G_m) = 0\). \(\rho\) is quantum-Martin-Löf Random (q-MLR) if it passes each q-MLT.
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, $\tau$ 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, $\tau$ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
The state $\tau = (2^{-n} I_{2^n})_n$ is computable.

By definition of a q-MLT, $\tau$ is q-MLR.

Work in progress: Characterize computable q-MLR states.

If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leq 2^n}$ 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, $\tau$ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leq 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of $\tau$ 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, $\tau$ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leq 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of $\tau$ 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, $\tau$ is q-MLR.
- Work in progress: Characterize computable q-MLR states.
- If $\rho_n \in L_n$ is a density matrix, its eigenvalues $(\alpha_i)_{i \leq 2^n}$ form a probability distribution. Denote the entropy of this distribution by $H(\rho_n)$.
- Each element of $\tau$ is uniform and so has maximum entropy.
- Entropy may provide a characterization?
- Partial progress: If $\rho = (\rho_n)_n$ is computable, then
  \[ \exists c \forall n[H(\rho_n) > n - c] \Rightarrow \rho \text{ is q-MLR} \Rightarrow \liminf_n[H(\rho_n)/n] = 1. \]
Q (Nies and Scholz): Is there a notion of quantum Solovay Randomness (q-SR)? If so, is it equivalent to q-MLR?

Yes. The proof uses the equivalence of q-SR and q-MLR.
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?
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.
A Quantum Solovay Test (q-ST) is a uniformly computable sequence of $\Sigma^0_1$ sets, $(S^k)_{k \in \omega}$ such that

$$\sum_{k \in \omega} \tau(S^k) < \infty$$
Failing and Passing a (q-ST) at level $\delta$

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

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

Quantum Solovay Randomness (q-SR)

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

For all states $\rho$, $\rho$ is q-SR if and only if $\rho$ is q-MLR.
Theorem (B.)

For all states $\rho$, $\rho$ is q-SR if and only if $\rho$ is q-MLR.

- $(\iff)$ A q-MLT is a q-ST.
Theorem (B.)

For all states $\rho$, $\rho$ is q-SR if and only if $\rho$ is q-MLR.

- ($\iff$) A q-MLT is a q-ST.
- ($\iff$) Let $\rho = (\rho_n)_{n \in \omega}$ fail a q-ST $(S_k^k)_{k \in \omega}$ at level $\delta$. Build a q-MLT $(G^m_m)_{m \in \omega}$, with $G^m = (G^m_n)_{n \in \omega}$, which $\rho$ fails at level $\delta^2/72$. 

WLOG, $S_k^n$ for $n \geq k$. Notation: $A \in \mathcal{C}_2$ such that $|\psi\rangle \langle \psi| S_k^n$ for $t, m \in \omega$. We may skip the proof in the interests of time and go straight to the application.
Theorem (B.)

For all states $\rho$, $\rho$ is q-SR if and only if $\rho$ is q-MLR.

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

Tejas Bhojraj (UW-Madison)  
Quantum Solovay randomness  
Waterloo, June 2018  
24 / 41
Theorem (B.)

For all states $\rho$, $\rho$ is q-SR if and only if $\rho$ is q-MLR.

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

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

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 \(\text{Tr}(\rho_n G_n^m) > \delta\) 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 \(\text{Tr}(\rho_n G^m_n) > \delta\) where \(\rho_n = \sum_{i<k} \alpha_i \rho_n^i\).
- I.e, \(\forall m \in \omega, \exists n\) such that

\[
\delta < \text{Tr}\left(\sum_{i<k} \alpha_i \rho_n^i G^m_n\right) = \sum_{i<k} \alpha_i \text{Tr}(\rho_n^i G^m_n).
\]
**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 \(\text{Tr}(\rho_n G^m_n) > \delta\) where \(\rho_n = \sum_{i<k} \alpha_i \rho^i_n\).
- I.e, \(\forall m \in \omega\), \(\exists n\) such that

\[
\delta < \text{Tr} \left( \sum_{i<k} \alpha_i \rho^i_n G^m_n \right) = \sum_{i<k} \alpha_i \text{Tr}(\rho^i_n G^m_n).
\]

- By convexity there must be an \(i\) such that \(\text{Tr}(G^m_n \rho^i_n) > \delta\)
So, \( \forall m \exists n, i \) such that \( \text{Tr} (\rho_n^i G_m^n) > \delta. \)
So, $\forall m \exists n, i$ such that $\text{Tr} \left( \rho_n^i G_m^n \right) > \delta$.

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 $\text{Tr} \left( \rho_n^i G_n^m \right) > \delta$.

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, $\exists \infty m$ with $\rho^i(G^m) > \delta$. 
So, $\forall m \exists n, i$ such that $\text{Tr} (\rho_n^i G_n^m) > \delta$.

There are only finitely many $i$ s.

By pigeonhole, there is an $i$ such that $\exists^\infty m$ with $\text{Tr} (\rho_n^i G_n^m) > \delta$, for some $n$.

So, $\exists^\infty m$ with $\rho^i (G^m) > \delta$.

So, $\rho^i$ fails the q-Solovay test $(G^m)_{m \in \omega}$ and hence is not q-MLR by our previous result.
Thank You
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Quantum Mechanics</strong></td>
</tr>
<tr>
<td></td>
<td>• The Density Matrix</td>
</tr>
<tr>
<td></td>
<td>• Partial Trace</td>
</tr>
<tr>
<td>2</td>
<td><strong>Quantum Cantor Space</strong></td>
</tr>
<tr>
<td></td>
<td>• Coherent Sequences of Density Matrices</td>
</tr>
<tr>
<td></td>
<td>• Quantum $\Sigma^0_1$-Classes</td>
</tr>
<tr>
<td>3</td>
<td><strong>Randomness</strong></td>
</tr>
<tr>
<td></td>
<td>• Quantum Martin-Löf Randomness</td>
</tr>
<tr>
<td></td>
<td>• Computable states can be random</td>
</tr>
<tr>
<td>4</td>
<td><strong>Definitions</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Quantum Solovay Randomness is equivalent to q-MLR</strong></td>
</tr>
<tr>
<td>6</td>
<td><strong>The set of q-MLR states is convex</strong></td>
</tr>
<tr>
<td></td>
<td>• Construction</td>
</tr>
<tr>
<td></td>
<td>• Verification</td>
</tr>
</tbody>
</table>
Constructing the q-MLT test

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

Easy to see that $D^m_n \subseteq A^m_n$ since $C^m_n \subseteq A^m_n$.

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 $G^m_n : \psi \mapsto \psi \in C^m_n$. 

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

Lemma

For each $m$, $G^m = (G^m_n)_{n \in \omega}$ is a quantum-$\Sigma^0_1$ 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 $Th(C_{alg})$ is.
Lemma

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

For each \( m \), \( G^m = (G^n_m)_{n \in \omega} \) is a quantum-\( \Sigma_1^0 \) set.

- Given \( C_{n-1}^m \), we built \( C_n^m \) in stages \( t \). \( C_{n,0}^m = D_n \). To compute \( C_{n,s}^m \) given \( C_{n,s-1}^m \), check if:

\[
\exists \tau \in A_n^m \text{ such that } \forall \psi \in C_{n,s-1}^m, \langle \tau | \psi \rangle = 0.
\]

This check is decidable as \( Th(C_{alg}) \) is.

- If yes, find a witness \( \tau \) and set \( C_{n,s}^m = \{ \tau \} \cup C_{n,s-1}^m \). If no, set \( C_n^m = C_{n,s-1}^m \) and stop. By finite dimensionality, at some stage we must stop.

- So, \( (G^n_m)_{n \in \omega} \) is a uniformly computable sequence.
Lemma

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

- Given \( C_{n-1}^m \), we built \( C_n^m \) in stages \( t \). \( C_{n,0}^m = D_n^m \). To compute \( C_{n,s}^m \) given \( C_{n,s-1}^m \), check if:

\[
\exists \tau \in A_n^m \text{ such that } \forall \psi \in C_{n,s-1}^m, \langle \tau | \psi \rangle = 0.
\]

This check is decidable as \( Th(C_{alg}) \) is.

- If yes, find a witness \( \tau \) and set \( C_{n,s}^m = \{\tau\} \cup C_{n,s-1}^m \). If no, set \( C_n^m = C_{n,s-1}^m \) and stop. By finite dimensionality, at some stage we must stop.

- So, \( (G_n^m)_{n \in \omega} \) is a uniformly computable sequence.

- By construction, \( \text{range}(G_{n-1}^m \otimes I_2) \subseteq \text{range}(G_n^m) \).

\( \square \)
Lemma

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

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

\[
1 \geq \sum_k \tau(S^k) \geq \sum_k 2^{-n} \text{Tr}(S^k_n),
\]

by definition
Lemma

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

\[ 1 \geq \sum_k \tau(S^k) \geq \sum_k 2^{-n} \text{Tr}(S^k_n), \]

by definition

For fixed $m, n$ we have that,

\[ 2^n \geq \sum_k \text{Tr}(S^k_n) \]

\[ \geq \sum_k \text{Tr}(\sum_{\psi \in C_n^m} |\psi\rangle\langle\psi| S^k_n) \]

\[ = \sum_{\psi \in C_n^m} \sum_k \text{Tr}(|\psi\rangle\langle\psi| S^k_n) \]

\[ > |C_n^m| \frac{2^m \delta}{6} \]

\[ = \text{Tr}(G^m_n) \frac{2^m \delta}{6}. \]
Lemma:

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

\[
\text{Tr}(\rho_n G^m_n) \geq \frac{\delta^2}{72}.
\]
Lemma:

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

$$\text{Tr}(\rho_n G^m_n) \geq \frac{\delta^2}{72}.$$ 

- Let $m$ be arbitrary.
Lemma:

\[ \rho \text{ fails } (G^m)_m \text{ at level } \delta^2/72. \text{ Or, for all } m \in \omega, \text{ there is an } n \text{ such that} \]

\[ \text{Tr}(\rho_n G^m_n) \geq \frac{\delta^2}{72}. \]

- Let \( m \) be arbitrary.
- Fix a \( n \) so that there exist \( 2^m \) many \( k \)s less than \( n \) such that \( \text{Tr}(\rho_n S^k_n) > \delta. \)
Lemma:

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

\[
\text{Tr}(\rho_n G^m_n) \geq \frac{\delta^2}{72}.
\]

- Let \( m \) be arbitrary.
- Fix a \( n \) so that there exist \( 2^m \) many \( k_s \) less than \( n \) such that \( \text{Tr}(\rho_n S^k_n) > \delta \).
- Case 1: \( \rho_n \) is algebraic:

\[
\rho_n = \sum_{i \leq 2^n} \alpha_i |\psi^i\rangle\langle\psi^i|\]

\( \sum_{i \leq 2^n} \alpha_i = 1 \) and for each \( i \), \( |\psi^i\rangle \in \mathbb{C}^{2^n}_{\text{alg}} \) and \( ||\psi^i|| \leq 1 \).
Fix $i_2$; let $\psi_i$. Write $\psi_i$ and $|\psi_i|^2$.

where $\psi_o \in \mathcal{G}$ and $\psi_p \in \mathcal{G}$ are unit vectors, $|\psi_i|^2$ and $|\psi_|^2$.

For a $k$, let $S_k$. An easy, but long, calculation shows:

$$\text{Tr}_{p\in S}|\psi_i\rangle\langle\psi_i|_{k-1} = \langle S\psi_o|S\psi_o\rangle|c_o|^2 - \langle S\psi_p|S\psi_p\rangle|c_p|^2 |\psi_i| |\psi_i|^2 |\langle S\psi_p|S\psi_o\rangle| \leq 1.$$
• Fix $i \leq 2^n$; let $\psi = \psi^i$. Write

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

where $\psi_o \in \text{range}(G^m_n)$ and $\psi_p \in \text{range}(G^m_n)^\perp$ are unit vectors, $c_o, c_p \in \mathbb{C}$ and $|c_0|^2 + |c_p|^2 = ||\psi||^2 \leq 1$. 
• Fix $i \leq 2^n$; let $\psi = \psi^i$. Write

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

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

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

$$\text{Tr}(S|\psi\rangle\langle\psi|) \leq$$

$$|c_o|^2 \langle S\psi_o | S\psi_o \rangle + |c_p|^2 \langle S\psi_p | S\psi_p \rangle + 2|c_o||c_p| |\langle S\psi_p | S\psi_o \rangle|$$
By Cauchy-Schwarz:

\[
\langle S\psi_p | S\psi_o \rangle \leq \|S\psi_o\| \|S\psi_p\| \max_t \|d\| \langle \psi_o | d | \psi_p \rangle ^2.
\]

Using this and that: \[\|c_o\| \leq 1, \text{Tr}_p S|\psi_o \rangle \langle \psi| q \|c_p\| \leq \langle S\psi_o | S\psi_o \rangle^{1/2} \langle S\psi_p | S\psi_p \rangle^{1/2} \|c_o\| \|c_p\|^{1/2} \|S\psi_o\| \|S\psi_p\|^{1/2}.\]

Tejas Bhojraj (UW-Madison)  Quantum Solovay randomness  Waterloo, June 2018  34 / 41
By Cauchy-Schwarz:

\[ |\langle S\psi_p | S\psi_o \rangle| \leq ||S\psi_o|| ||S\psi_p|| \]
\[ \leq (\max\{||S\psi_o||, ||S\psi_p||\})^2 \]
\[ \leq ||S\psi_o||^2 + ||S\psi_p||^2. \]
By Cauchy-Schwarz:

\[ |\langle S\psi_p | S\psi_o \rangle| \leq \|S\psi_o\| \|S\psi_p\| \]
\[ \leq (\max\{\|S\psi_o\|, \|S\psi_p\|\})^2 \]
\[ \leq \|S\psi_o\|^2 + \|S\psi_p\|^2. \]

Using this and that \(|c_o|, |c_p| \leq 1\),

\[
\text{Tr}(S|\psi\rangle\langle\psi|)
\leq |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)
\leq |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)
By the choice of $n$, pick $M \subseteq \{1, 2...n\}$ such that $|M| = 2^m$ and $\text{Tr}(\rho_n S_n^k) > \delta$ for each $k$ in $M$.

$$2^m \delta < \sum_{k \in M} \text{Tr}(\rho_n S_n^k)$$

$$= \sum_{k \in M} \text{Tr}\left(\sum_{i \leq 2^n} \alpha_i |\psi^i\rangle \langle \psi^i | S_n^k\right)$$

$$= \sum_{k \in M} \sum_{i \leq 2^n} \alpha_i \text{Tr}(|\psi^i\rangle \langle \psi^i | S_n^k)$$

$$= \sum_{i \leq 2^n} \alpha_i \sum_{k \in M} \text{Tr}(|\psi^i\rangle \langle \psi^i | S_n^k)$$

$$\leq \sum_{i \leq 2^n} \alpha_i \sum_{k \in M} 3(|c_i^o| \langle S_n^k \psi_o | S_n^k \psi_o \rangle + |c_p^i| \langle S_n^k \psi_p | S_n^k \psi_p \rangle).$$
So,

\[
\frac{2^m \delta}{3} < \sum_{i \leq 2^n} \alpha_i \sum_{k \in M} (|c_i^i|^2 \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + |c_p^i|^2 \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle)
\]

\[
= \sum_{i \leq 2^n} \alpha_i |c_o^i|^2 \sum_{k \in M} \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + \sum_{i \leq 2^n} \alpha_i |c_p^i|^2 \sum_{k \in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle
\]
So,

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

\[
= \sum_{i \leq 2^n} \alpha_i |c_o^i| \sum_{k \in M} \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + \sum_{i \leq 2^n} \alpha_i |c_p^i| \sum_{k \in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle
\]

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

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

\[
= \sum_{i \leq 2^n} \alpha_i |c_o^i| \sum_{k \in M} \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle + \sum_{i \leq 2^n} \alpha_i |c_p^i| \sum_{k \in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle
\]

- 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.
Hence, $\psi_i$ is perpendicular to each element of $C_mn$. If $\psi_i \in A_{mn}$, then $t \psi_i u Y C_mn$ is a orthonormal subset of $A_{mn}$ strictly containing $C_mn$, contradicting the maximality of $C_mn$. So, $\psi_i \in A_{mn}$ for each $i$.

But, $\psi_i \in C_{2n}$ and $||\psi_i|| = 1$. So the only way $\psi_i \in A_{mn}$ is if $\langle \psi_i | S_k n \rangle = 2 \delta_{i,k}$.
\[ \forall i, \psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_\text{alg}^{2^n}. \]
\( \forall i, \psi^i_p \in \text{range}(G_n^m) \perp \cap \mathbb{C}^{2^n}_{\text{alg}}. \)

Hence, \( \psi^i_p \) is perpendicular to each element of \( C_n^m \).
\begin{itemize}
  \item \( \forall i, \psi^i_p \in \text{range}(G^m_n)^\perp \cap \mathbb{C}^{2n}_{\text{alg}}. \)
  
  \item Hence, \( \psi^i_p \) is perpendicular to each element of \( C^m_n. \)
  
  \item If \( \psi^i_p \in A^m_m, \) then \( \{ \psi^i_p \} \cup C^m_n \) is a orthonormal subset of \( A^m_n \) strictly containing \( C^m_n, \) contradicting the maximality of \( C^m_n. \)
\end{itemize}
\( \forall i, \psi^i_p \in \text{range}(G^n_m)^\perp \cap \mathbb{C}^{2^n} \).

Hence, \( \psi^i_p \) is perpendicular to each element of \( C^n_m \).

If \( \psi^i_p \in A^n_m \), then \( \{ \psi^i_p \} \cup C^n_m \) is an orthonormal subset of \( A^n_m \) strictly containing \( C^n_m \), contradicting the maximality of \( C^n_m \).

So, \( \psi^i_p \notin A^n_m \) for each \( i \).
\( \forall i, \psi_p^i \in \text{range}(G_n^m) \perp \cap C_{2n}^\text{alg}. \)

Hence, \( \psi_p^i \) 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, \( \psi_p^i \in \mathbb{C}_{2n}^\text{alg} \) and \( ||\psi_p^i|| = 1 \). So the only way \( \psi_p^i \notin A_n^m \) is if
\begin{itemize}
  \item $\forall i, \psi^i_p \in \text{range}(G^m_n) \perp \cap \mathbb{C}^{2^n}_{\text{alg}}$.
  
  Hence, $\psi^i_p$ is perpendicular to each element of $C^m_n$.
  
  If $\psi^i_p \in A^m_n$, then $\{\psi^i_p\} \cup C^m_n$ is an orthonormal subset of $A^m_n$ strictly containing $C^m_n$, contradicting the maximality of $C^m_n$.
  
  So, $\psi^i_p \notin A^m_n$ for each $i$.
  
  But, $\psi^i_p \in \mathbb{C}^{2^n}_{\text{alg}}$ and $||\psi^i_p|| = 1$. So the only way $\psi^i_p \notin A^m_n$ is if
  
  \[
  \sum_{k \leq n} \text{Tr}(|\psi^i_p \rangle \langle \psi^i_p | S^n_k) \leq \frac{2^m \delta}{6}.
  \]
\end{itemize}
Recall

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

\[
\frac{2^m \delta}{3} < \sum_{i \leq 2^n} \alpha_i |c^i| \sum_{k \in M} \langle S^k_n \psi^i_o | S^k_n \psi^i_o \rangle + \sum_{i \leq 2^n} \alpha_i |c^i| \sum_{k \in M} \langle S^k_n \psi^i_p | S^k_n \psi^i_p \rangle
\]
So, bound the sum as follows:

\[ \sum_{i=2}^{n} \alpha_i |c_i p| \sum_{k=\Psi}^{\Psi} \langle S_k n \psi | S_k n \psi \rangle \]

This means:

\[ \sum_{i=2}^{n} \alpha_i |c_i o| \sum_{k=\Psi}^{\Psi} \langle S_k n \psi | S_k n \psi \rangle \]
So, bound the sum as follows:

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

$$\leq \sum_{i \leq 2^n} \alpha_i |c_p^i| \frac{2^m \delta}{6} < \sum_{i \leq 2^n} \alpha_i \frac{2^m \delta}{6} \leq \frac{2^m \delta}{6}$$
So, bound the sum as follows:

\[
\sum_{i \leq 2^n} \alpha_i |c_p^i| \sum_{k \in M} \langle S_n^k \psi_p^i | S_n^k \psi_p^i \rangle 
\]

\[
\leq \sum_{i \leq 2^n} \alpha_i |c_p^i| \frac{2^m \delta}{6} < \sum_{i \leq 2^n} \alpha_i \frac{2^m \delta}{6} \leq \frac{2^m \delta}{6}
\]

This means:

\[
\sum_{i \leq 2^n} \alpha_i |c_o^i| \sum_{k \in M} \langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle > \frac{2^m \delta}{6}
\]
\[ |\langle S_n^k \psi_i | S_n^k \psi_i^i \rangle| \leq 1 \text{ and } |M| = 2^m \]
\[ |\langle S_n^k \psi_o | S_n^k \psi_o \rangle| \leq 1 \text{ and } |M| = 2^m \]

So, cancel the \(2^m\)s to get:

\[
\frac{\delta}{6} < \sum_{i \leq 2^n} \alpha_i |c_i^o|.
\]
$|\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle| \leq 1$ and $|M| = 2^m$

So, cancel the $2^m$s to get:

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

As $\sum_{i \leq 2^n} \alpha_i = 1$, by Jensen’s inequality:

$$\frac{\delta^2}{36} < \left( \sum_{i \leq 2^n} \alpha_i |c_o^i| \right)^2 \leq \sum_{i \leq 2^n} \alpha_i |c_o^i|^2$$
\[
\langle S_n^k \psi_o^i | S_n^k \psi_o^i \rangle | \leq 1 \text{ and } |M| = 2^m
\]

So, cancel the \(2^m\)s to get:

\[
\frac{\delta}{6} < \sum_{i \leq 2^n} \alpha_i |c_o^i|.
\]

As \(\sum_{i \leq 2^n} \alpha_i = 1\), by Jensen’s inequality:

\[
\frac{\delta^2}{36} < \left( \sum_{i \leq 2^n} \alpha_i |c_o^i| \right)^2 \leq \sum_{i \leq 2^n} \alpha_i |c_o^i|^2
\]

Finally, it is easy to see that

\[
Tr(\rho_n G_n^m) = \sum_{i \leq 2^n} \alpha_i Tr(|c_o^i \psi_o^i \rangle \langle c_o^i \psi_o^i|)
\]

\[
= \sum_{i \leq 2^n} \alpha_i |c_o^i|^2 > \frac{\delta^2}{36}
\]
Case 2: $\rho_n$ is not expressible as a convex sum of algebraic projections.

Since $\{\psi \in \mathbb{C}^{2^n}_{\text{alg}} : \|\psi\| \leq 1\}$ is dense in the closed unit ball in $\mathbb{C}^{2^n}$, using case 1, we see that $Tr(\rho_n G^m_n) > \frac{\delta^2}{72}$