Randomness for infinite sequences of quantum bits

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

CCR 2017, Mysore

Joint work with Volkher Scholz, ETH Zürich

Plan

I.
- Quantum bits
- Finite sequences of quantum bits, density operators
- Infinite coherent sequences of density operators.
  They are states on a certain computable C^*-algebra

II.
- Extend Martin-Löf randomness to this setting.
- Universal quantum Martin-Löf test
- For classical bit sequences,

$$\text{ML-random} \iff \text{quantum ML-random}$$

- A version of Levin-Schnorr theorem in this setting.

Quantum bits

- A classical bit can be in states $0, 1$. Write them as $|0\rangle$, $|1\rangle$.
- A qubit is a physical system with two classical states:
  - polarisation of photon horizontal/vertical,
  - hydrogen atom with electron in basic/excited state
  - Schrödinger's cat dead / alive.
- A qubit can be in a superposition of the two classical states:
  $$\alpha \mid 0\rangle + \beta \mid 1\rangle,$$
  $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. E.g. $\alpha = 2/\sqrt{5}, \beta = -i/\sqrt{5}$.
- Visualise as surface points on "Bloch sphere", where $|0\rangle$, $|1\rangle$ are South and North pole, respectively.
- Measurement of a qubit w.r.t. standard basis $|0\rangle, |1\rangle$ yields 0 with probability $|\alpha|^2$, and 1 with probability $|\beta|^2$.
- Measurement forces the system to settle on a classical state.

Hilbert spaces and their tensor products

- The state of a physical system is represented by a vector in a finite dimensional Hilbert space.
- $\langle a|b\rangle$ denotes the inner product of vectors a, b, linear in the second component.
- For systems A, B, the tensor product $A \otimes B$ is a Hilbert space that represents the combined system.
- $A \otimes B$ is the quotient of the vector space generated by the set $A \times B$ as a basis, by the relations saying things like $(\gamma a, b) = \gamma(a, b)$ for $\gamma \in \mathbb{C}$, and $(a + a', b) = (a, b) + (a', b)$. Write $a \otimes b$ for the equivalence class of (a, b).
- Define inner product on $A \otimes B$ by

$$\langle a \otimes b|c \otimes d\rangle = \langle a|c\rangle\langle b|d\rangle.$$

Finite sequences of quantum bits

- Mathematically, a qubit is simply a unit vector in $\mathbb{C}^2$. The state of a system of n qubits is a unit vector in the tensor power
$$(\mathbb{C}^2)^{\otimes n} := \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n}.$$
- We denote the standard basis of $\mathbb{C}^2$ by $|0\rangle, |1\rangle$. The standard basis of $(\mathbb{C}^2)^{\otimes n}$ is given by n-bit strings: it consists of vectors
$$|a_1 \ldots a_n\rangle := |a_1\rangle \otimes \ldots \otimes |a_n\rangle.$$
- The state of the system of n qubits is a linear superposition of them. Example: Bell (or "maximally entangled") state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Mixed states, or density operators

- So far we had "pure" states $|\psi\rangle$ viewed as unit vectors in $(\mathbb{C}^2)^{\otimes n}$.
- $|\psi\rangle\langle\psi|$ is orth. projection on the subspace spanned by $|\psi\rangle$ fixing $|\psi\rangle$.
- A mixed state is a convex linear combination $\sum_{i=1}^{2^n} p_i|\psi_i\rangle\langle\psi_i|$ for pairwise orthogonal pure states ψ_i.
- E.g. for $n = 1$, a mixed state is $\frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|$.
- Recall that for an operator S on A, the trace is

$$\mathsf{tr}(S) = \text{sum of eigenvalues of } S.$$

- A mixed state is the same as a positive Hermitean operator S on $(\mathbb{C}^2)^{\otimes n}$ with $\mathsf{tr}(S) = 1$. One can see this via the spectral decomposition.

Partial trace $T_B \colon L(A \otimes B) \to L(A)$

Recall: Given systems (finite dimensional Hilbert spaces) A, B, the tensor product $A \otimes B$ is a Hilbert space that represents the combined system. $L(A)$ denotes the space of the linear operators on A.

We want to surject $L(A \otimes B)$ onto $L(A)$. The partial trace T_B is the unique linear operator $L(A \otimes B) \to L(A)$ such that for $R \in L(A), S \in L(B)$, we have $T_B(R \otimes S) = R \cdot \mathsf{tr}(S)$.

- Example: Let $A = B = \mathbb{C}^2$. The partial trace T_B corresponds to deleting the last qubit. E.g. $T_B(|10\rangle\langle 10|) = |1\rangle\langle 1|$.
- Let's consider again the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, now viewed as projection β in $L(A \otimes B)$. We have $T_B(\beta) = \frac{1}{2}(|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|)$ which is a mixed state!

Infinite coherent sequences of density operators

M_n denotes the set of $2^n \times 2^n$ matrices over $\mathbb{C}$. We have a partial trace operation $T_n \colon M_{n+1} \to M_n$ ("erase the last qubit").

"Quantum Cantor space" $S(M_\infty)$ consists of the sequences $(\rho_n)_{n\in\mathbb{N}}$ of density operators in M_n such that $T_n(\rho_{n+1}) = \rho_n$ for each n.

- This is the set of states (linear functionals of norm 1) on the computable C^* algebra $M_\infty = \lim_n M_n$, known as the CAR algebra (for "canonical anticommutation relations").
- $S(M_\infty)$ is compact in a natural topology (weak-$*$), and has a convex structure.

Embed Cantor space into quantum Cantor space

Recall: $(\mathbb{C}^2)^{\otimes n}$ has as a base the vectors $|\sigma\rangle$, for σ a string of n classical bits.

We describe the partial trace operation $T_n \colon M_{n+1} \to M_n$ ("erase last qubit") given by the isomorphism $M_{n+1} \cong M_n \otimes \mathbb{C}^2$.

For a $2^{n+1} \times 2^{n+1}$ matrix $A = (a_{\sigma r, \tau s})$ where $|\sigma|, |\tau| = n$, r, s are bits, $B = T_n(A)$ is given by the $2^n \times 2^n$ matrix

$$b_{\sigma,\tau} = a_{\sigma 0, \tau 0} + a_{\sigma 1, \tau 1}.$$

- Classical bit sequence Z becomes $(\rho_n)_{n \in \mathbb{N}}$ where the bit matrix $B = \rho_n \in M_n$ satisfies $b_{\sigma,\tau} = 1 \iff \sigma = \tau = Z \upharpoonright_n$.
- If all the ρ_n are diagonal matrices, we describe a measure on Cantor space. Classical bit sequences are Dirac measures.

Part 2: Randomness for coherent sequences of density operators

- Main objects of study: states $Z \in S(M_\infty)$.
- Z is a coherent sequence $(\rho_n)_{n\in\mathbb{N}}$, where $\rho_n \in M_n$ is a density matrix, $T_n(\rho_{n+1}) = \rho_n$.

Special projections

- $\mathbb{C}_{\texttt{alg}}$ denotes the field of algebraic complex numbers.
- A projection in M_n is a hermitean matrix p such that $p^2 = p$.
- A special projection in M_n is a projection with matrix entries in $\mathbb{C}_{\texttt{alg}}$.
- We have a natural embedding $M_n \to M_{n+1}$ via $A \to A \otimes I_2$, i.e. replace every element t by $\begin{matrix} t & 0 \\ 0 & t \end{matrix}$.
- $p \leq q$, for projections $p \in M_n, q \in M_k$, means that range of p is contained in range of q.

Σ^0_1 probabilistic sets on quantum Cantor space

A Σ^0_1 set in Cantor space can be described by an ascending effective union $\bigcup_n C_n$ where C_n is a clopen set given by strings of length n.

We want to give a quantum version of this.

A quantum Σ^0_1 set G is given by a computable ascending sequence of special projections (p_n) where $p_n \in M_n$. Corresponding to measure, we have

$$\tau(G) := \sup_n 2^{-n}\mathsf{tr}(p_n).$$

For Z in quantum Cantor space let $G(Z) = \sup_n Z(p_n)$.

Measurements

Recall: A quantum Σ_1^0 set G is given by a computable ascending sequence of special projections (p_n) where $p_n \in M_n$. For Z in quantum Cantor space let $G(Z) = \sup_n Z(p_n)$.

In classic setting, p_n is a clopen set given by strings of length n. If Z is a bit sequence, we have $Z(p_n) = 1 \iff Z\restriction_n \in p_n$, so $G(Z)$ is as usual.

In the language of quantum mechanics we can view $Z(p_n)$ as a measurement of Z with the observable p_n. $Z(p_n)$ is the probability that Z is "in" p_n. In the classical case this is simply 1 (in) or 0 (out).

We have $Z(p_n) = \mathsf{tr}(Z\restriction_n p_n)$, recalling that tr is the trace, and $Z\restriction_n \in M_n$ is a density operator. This means the measurement only depends on the first n qubits of Z.

Quantum ML test

- A quantum Martin-Löf test is an effective sequence $\langle G_r \rangle_{r\in\mathbb{N}}$ of quantum Σ^0_1 sets such that $\tau(G_r) \leq 2^{-r}$ for each r.
- Z passes the test if $\inf_r G_r(Z) = 0$. Z is quantum ML random if it passes each quantum ML test.

Adapting the usual construction, we have:

Prop. There is a universal quantum ML-test $\langle L_n \rangle$. In fact for each qML test $\langle G_k \rangle$ and each state Z we have $\inf_n L_n(Z) \geq \inf_k G_k(Z)$.

However, because of the "$\inf(...) = 0$" in the passing condition, quantum ML-randomness is merely a Π^0_3 property of states (while the usual ML-randomness of bit sequences is Σ^0_2).

No difference for bit sequences

Thm. Suppose $Z \in \{0,1\}^{\mathbb{N}}$. Then Z is ML-random $\iff$ Z viewed as an element of $\mathcal{S}(M_{2^\infty})$ is qML-random.

$\Leftarrow$: Every classical ML-test is also a quantum ML-test.
$\Rightarrow$: Given a quantum ML test (G_r) with $\inf_r G_r(Z) > 0$, we have to find a classical ML-test that succeeds on Z.

- For the projection p_n, compute unitary $u_n \in M_n$ such that $q_n := u_n^* p_n u_n$ is a (projection onto the subspace spanned by a) clopen set.
- Make the u_n cohere with the q_n in sense that $u_{n+1} q_n = u_n q_n$ (u_{n+1} doesn't do new things on the range of p_n).
- $Z(p_n) = \sum_{|\sigma|=n, q_n(\underline{\sigma})=\underline{\sigma}} |\langle u(\underline{\sigma}) | Z\restriction_n \rangle|^2$ where $\underline{\sigma}$ is short for $|\sigma\rangle$.
- Use this to build a classical ML-test for Z.

Value of quantum ML test at state

Recall: A quantum Martin-Löf test is an effective sequence $\langle G_r \rangle_{r \in \mathbb{N}}$ of quantum Σ^0_1 sets such that $\tau(G_r) \leq 2^{-r}$ for each r.

Think of $\langle G_r \rangle_{r \in \mathbb{N}}$ as a sequence of measurements. The overall measured value at Z is $\inf_r G_r(Z)$.

It is possible Z is not random, but the measured value is < 1 for the universal quantum ML-test:
Take a ML-random bit sequence Y. Let Z be the state $\frac{1}{2}Y + \frac{1}{2}0^\infty$.
This is not random, but for the universal qML-test (L_r) we have

$$\inf_r L_r(Z) \leq \inf_r L_r(Y) + \frac{1}{2} = \frac{1}{2}.$$

ML-random measures on $\{0,1\}^{\mathbb{N}}$

Recall that measures on $\{0,1\}^{\mathbb{N}}$ correspond to states Z on M_∞ with all the $Z\upharpoonright_n$ diagonal matrices. Mauldin and Monticino (Israel J. Math., 1995) and then Culver's thesis (Notre Dame, 2015) describe the uniform computable probability measure $\mathbb{P}$ on the set of measures on Cantor space. So for measures there is an established notion of ML-randomness.

Question. If a probability measure μ is ML-random wrt to $\mathbb{P}$, is μ quantum ML-random?

All we can show: if μ is $\mathbb{P}$-random and (G^r) a (classical) ML-test, then μ passes the test in the sense above that $\inf \mu(G^r) = 0$. This uses that $\int_{\mathcal{M}(\{0,1\}^{\mathbb{N}})} \mu(G) d\mathbb{P}(\mu) = \lambda(G)$ for open $G \subseteq \{0,1\}^{\mathbb{N}}$.

Quantum Turing machines

- Bernstein and Vazirani (SIAM, 1997) introduced quantum TM.
- Single steps are unitary operations. Computation is reversible.
- QTM input and output are qubit strings.
- They showed that there is a universal QTM $\mathbb{U}$.
- I/O behaviour is linear, so we can use as inputs density operators in some M_n.

Quantum Kolmogorov complexity

Berthiaume, van Dam, LaPlante JCSS 2001 defined quantum Kolmogorov complexity.

- For an operator ρ, the trace norm is $||\rho||_{\mathsf{tr}} = |\mathsf{tr}(\rho)|$.
  (Generalises L_1 norm of vectors.)
- For $\epsilon > 0$ let

  $$QC^{\epsilon}(X) = \min\{\ell(P) \colon \ ||X - \mathbb{U}(P)||_{\mathsf{tr}} \leq \epsilon\}.$$

  This says we take the least length of a qubit string P such that $\mathbb{U}(P)$ and X are within ϵ in the trace distance.
- conditional version $QC^{\epsilon}(X)|r$, where r is a number (in binary)

No convincing prefix free version of quantum Kolg. complexity (an attempt is in Markus Mueller's 2007 thesis, U. Berlin).

Version of Miller/Yu theorem (in progress)

Let Z be a state on M_∞. Then we have the following:

- If Z is qML-random, then for each computable function f with $\sum_n 2^{-f(n)} < \infty$, $\quad \forall \epsilon > 0 \ \exists r \ \forall n$

$$QC^\epsilon(Z\restriction_n | \, n) \geq n - f(n) - r.$$

- There exists a computable function f with $\sum_n 2^{-f(n)} < \infty$ such that: Z not quantum ML-random $\Rightarrow \exists \epsilon > 0 \ \forall r \ \exists n$

$$QC^\epsilon(Z\restriction_n | \, n) < n - f(n) - r.$$

  In fact if Z fails the uniform qML test at order $\delta < 1$, we can choose $\epsilon = 2(\sqrt{1-\delta}$.

We plan to adapt the short proof in the Bienvenu/Merkle/Shen 2007 paper to the quantum setting. Many new complications.

Questions

- Closure properties of quantum ML-randomness. E.g., is a computable convex combination of qML-random states again qML-random?
- Base invariance (how about sequences of "qutrits"- are they equivalent in some way to qML-random sequences?)
- One can introduce quantum Solovay tests. Are they equivalent in strength to quantum ML-tests? (No direction is obvious. However, a classic ML-random bit sequence is also quantum Solovay random.)
- Is each ML-random measure quantum ML-random?

Reference: upcoming paper with Volkher Scholz.