# Computability theory and quantum information theory

QuSoft, Amsterdam
June 21, 2022

André Nies
School of Computer Science

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

# Computability theory

- a subfield of mathematical logic
- founded by Gödel, Turing, Church, Kleene in the 1930s
- studies (relative) computability in principle, without considering resource bounds.

## Fundamental notions of computability theory

- Computable set, computable function on the natural numbers
- recursively enumerable (r.e.) set
- reduction procedures such as $\leq_m$ and $\leq_T$
- The halting problem $K$ is undecidable.
- In fact it is $\leq_m$-complete for the class of r.e. sets.

# The spectral gap problem undecidable

Cubitt et al. 2015; Bausch et al. 2020

Cubitt, Perez-Garcia and Wolf (Undecidability of the Spectral Gap, Nature 528, 2015, 6 pages) showed that whether there is a spectral gap is undecidable for spin square lattices.

The full proof has last been updated on arXiv in 2020 (1502.04573v4), and now stands at 126 pages.

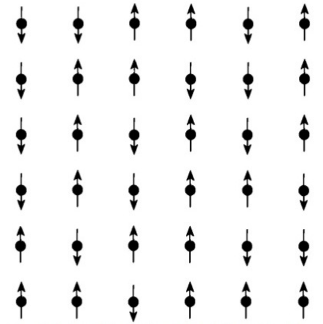
Later on, Bausch, Cubitt, Lucia and Perez-Garcia (Phys. Review X.10, 2020, 20 pages) showed that the existence of a spectral gap is undecidable for abstract spin chains.

# Spin chains and spin lattices

Spin chains were introduced to understand magnetism. A classical spin chain consists of $N$ dipoles arranged linearly:

$$\underbrace{\uparrow\downarrow\downarrow\uparrow \;\ldots\; \uparrow}_{N}$$

Higher-dimensional arrangements of dipoles have are also studied, in particular square lattices.



# Ising model in 1D: Hamiltonian

The 1D Ising model is due to Lenz (1920), and was “solved” by his student Ising in his thesis (1925).
The positions $i = 1, \dots, N$ in a spin chain are called sites.
The energy of a state of the system is given by a Hamiltonian.

For the 1D Ising model with $N$ sites, the Hamiltonian is

$$H_N = -J \sum_{i=1}^{N-1} \sigma_i \sigma_{i+1} - h \sum_{j=1}^{N} \sigma_j$$

- $J$ is the interaction strength between neighbours,
- $h$ is the strength of the external magnetic field,
- $\sigma_i = 1$ for spin $\uparrow$ at site $i$, and $\sigma_i = -1$ for spin $\downarrow$ at site $i$.

# Quantum setting: Heisenberg (1928) model

- $n$-chain, each site contains a spin $1/2$ particle (e.g., electron).
- state is unit vector in $(\mathbb{C}^2)^{\otimes n}$
- Spins in $x, y, z$ directions, corresponding to observables given by the Pauli matrices $\sigma^x, \sigma^y, \sigma^z$.
- Write $\vec{\sigma} = (\sigma^x, \sigma^y, \sigma^z)$ and $\vec{\sigma}_k = \mathbb{I}_2 \otimes \ldots \otimes \mathbb{I}_2 \otimes \vec{\sigma} \otimes \mathbb{I}_2 \otimes \ldots \otimes \mathbb{I}_2$, where the $\vec{\sigma}$ is in position $k$.

The Hamiltonian is now a Hermitian operator on $(\mathbb{C}^2)^{\otimes n}$:

$$H = \sum_{i=1}^{n-1} h_{i,i+1}^{(2)} \text{ where } h_{i,i+1}^{(2)} = \tfrac{J}{4}(\vec{\sigma}_i \cdot \vec{\sigma}_{i+1} - \mathbb{I}^{\otimes n});$$

$J \in \mathbb{R}$ is a coupling constant, and the local Hamiltonians $h_{i,i+1}^{(2)}$ describe the interaction of neighbouring sites.

# Abstract spin chains

For $d \geq 2$ (sometimes suppressed), a qudit is a unit vector in $d$-dimensional Hilbert space $\mathbb{C}^d$.

- An abstract spin chain is a system of $n$ qudits, arranged linearly. The positions are referred to as sites.
- The state of such a system is given by a vector in the $d^n$-dimensional Hilbert space $(\mathbb{C}^d)^{\otimes n}$.

One also considers higher dimensional arrangements of qudits, e.g. square lattices.

# Local Hamiltonians

Let $M_n(\mathbb{C})$ denote the algebra of $n \times n$ complex matrices.

As in the case of the Ising and Heisenberg chains, the behaviour of an abstract spin chain is described by local Hamiltonians.

Let $h^{(1)} \in M_d(\mathbb{C})$ and $h^{(2)} \in M_{d^2}(\mathbb{C})$ be Hermitian matrices, where

- $h^{(1)}$ describes the one-site "interactions", and
- $h^{(2)}$ describes the nearest-neighbour interactions.

The global Hamiltonian of a spin chain of $n$ qudits is given by shifting and adding up these interactions as the indices vary:

$$H_n = \sum_{i=1}^{n} h_i^{(1)} + \sum_{i=1}^{n-1} h_{i,i+1}^{(2)}.$$

# Asymptotic spectral gap

The spectral gap of a nontrivial Hamiltonian $H$ acting on a finite-dimensional Hilbert space is $\Delta(H) = \gamma_1(H) - \gamma_0(H)$, the difference between its least two eigenvalues.

When writing a sequence $\langle H_n \rangle_{n\in\mathbb{N}}$ we will assume that $H_n$ is a Hamiltonian on the $d^n$-dimensional Hilbert space.

The asymptotic spectral gap of such a sequence can be defined as

$$\Delta\langle H_n \rangle = \liminf_n \Delta(H_n).$$

(Note that the ground energy $\gamma_0(H_n)$ might increase with $n$.)

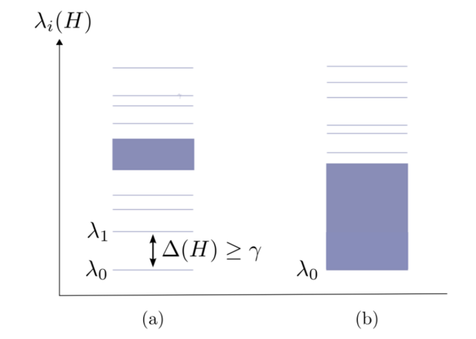
# Gapped and gapless sequences of Hamiltonians

Intuitively, the system is gapped if $\Delta\langle H_n\rangle$ is positive, and gapless otherwise. Cubitt et al. (2015) and then Bausch et al. (2020) use definitions making both the gapped and the gapless case more restricted, so that some sequences have neither property.

$\langle H_n\rangle$ is gapped if $\Delta\langle H_n\rangle = \liminf_n \Delta(H_n)$ is positive; moreover, for sufficiently large $n$, the least eigenvalue $\lambda_0(H_n)$ is non-degenerate. Physically the additional condition means that there is a unique ground state of the system (up to phase).

$\langle H_n\rangle$ is gapless if there is some $c > 0$ such that for each $\varepsilon > 0$, for all sufficiently large $n$, each point in the interval $[\lambda_0(H_n), \lambda_0(H_n) + c]$ is $\varepsilon$-close to some eigenvalue of $H_n$.

(a) $\langle H_n \rangle$ is gapped if $\Delta\langle H_n \rangle = \liminf_n \Delta(H_n)$ is positive and for sufficiently large $n$, the least eigenvalue $\lambda_0(H_n)$ is non-degenerate.
(b) $\langle H_n \rangle$ is gapless if there is some $c > 0$ such that for each $\varepsilon > 0$, for all sufficiently large $n$, each point in the interval $[\lambda_0(H_n), \lambda_0(H_n) + c]$ is $\varepsilon$-close to some eigenvalue of $H_n$.




From Cubitt et al., Nature 2015

# 1D case due to Bausch et al.

Even in the 1-dimensional case, whether there is a spectral gap was shown to be undecidable (Bausch et al., 2020). Given a Turing machine $M$, they determine a (fairly large) dimension $d$. Then, given an input $\eta \in \mathbb{N}$ to $M$ they compute local Hamiltonians $h^{(1)} \in M_d(\mathbb{C})$ and $h^{(2)} \in M_{d^2}(\mathbb{C})$ as above such that

- if $M(\eta)$ halts then the sequence $\langle H_n(\eta) \rangle$ (defined as above by shifting the local interactions) is gapless,
- otherwise the sequence $\langle H_n(\eta) \rangle$ is gapped.

They rely on the methods of Cubitt et al. (2015) who showed that the spectral gap problem is undecidable in the 2D case, using square lattices of qudits. The definitions there are similar, except that there are two types of nearest-neighbour interactions, for rows and for columns.

# Remarks

1. In the 2D case, the relationship between machines and Hamiltonians is the other way round: if $M(\eta)$ halts then the sequence is gapped, else gapless.

2. The entries of the Hamiltonians are easy "complex" numbers:
   - Let $R$ be the subring of $\mathbb{C}$ generated by
   $$\mathbb{Q} \cup \{\sqrt{2}\} \cup \{\exp(2\pi i\theta) \colon \theta \in \mathbb{Q}\}.$$
   - The entries of the local Hamiltonians, and hence of the $H_n(\eta)$, are all in $R$.
   - So the undecidability of the spectral gap is not an artefact of the well-known fact that equality of two computable reals is undecidable.

# Elements of the proofs in 2D and 1D

In 2 dimensions:

- quantum Turing machines (Bernstein and Vazirani)
- history state Hamiltonian $T^{-1/2} \sum_{t=0}^{T-1} |t\rangle|\psi_t\rangle$ due to Feynman
- Gottesman and Irani (FOCS 2013): The ground state encodes the whole computation of a QTM up to stage $T$.
- The quantum TM is not related to $M$; rather, it is related to the phase estimation algorithm (e.g. Nielsen/Chuang)
- Quasi-periodic Wang tiling due to Robinson 1971.

In 1 dimension:

the Wang tiling, for which the second spatial dimension in the lattice was needed, is replaced by a "marker Hamiltonian".

# Defining quantum Martin-Löf randomness

for infinite "sequences" of qubits

- Nies and Scholz, Martin-Löf random quantum states, JMP 2019, https://arxiv.org/abs/1709.08422
- Tejas Bhojraj 2021 thesis at UW Madison under Joe Miller's and my supervision, arxiv 2106.14280

# Some terminology and notation

- The state $|\psi\rangle$ of a system of $n$ qubits is a linear superposition of vectors $|a_1 \ldots a_n\rangle$ where $a_i \in \{0,1\}$. E.g., the EPR state is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
- A mixed state has the form $\sum_{i=1}^{2^n} \alpha_i |\psi_i\rangle\langle\psi_i|$ where $0 \leq \alpha_i \leq 1$ and $\sum_i \alpha_i = 1$. It corresponds to a density matrix.
- $M_d$ denotes the $C^*$-algebra of $d \times d$ matrices over $\mathbb{C}$.
- The trace of $A \in M_{2^d}$ is $\mathsf{tr}(A) = \sum_i A_{ii}$. Also $\tau(A) = \mathsf{tr}(A)/d$.
- Partial trace operation $T_n \colon M_{2^{n+1}} \to M_{2^n}$. For $A$ a density matrix, think of $T_n(A)$ as $A$ with the last qubit erased.
- There is a natural embedding $M_{2^n} \to M_{2^{n+1}}$ via

$$A \to A \otimes I_2 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}.$$

- The $C^*$-algebra $M_\infty$ is the operator norm completion of $\bigcup_n M_{2^n}$.

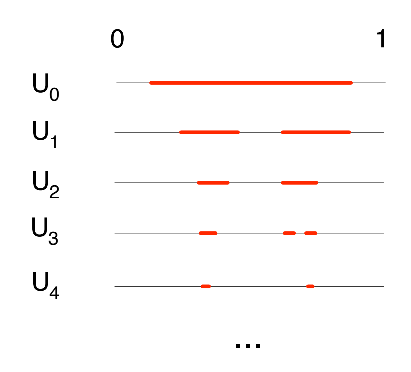
# States on $M_\infty$ are sequences of density operators

$S(M_\infty)$ denotes the space of sequences $(\rho_n)_{n\in\mathbb{N}}$ of density matrices in $M_{2^n}$ that are coherent in that $T_n(\rho_{n+1}) = \rho_n$ for each $n$.

- This is the set of states $\rho$ (i.e., positive linear functionals of norm $1$) on the $C^*$-algebra $M_\infty$, via
$$\rho(A) = \mathsf{tr}(\rho_n A) \text{ for } A \in M_{2^n}.$$
- A classical bit sequence $Z$ turns into $(\rho_n)_{n\in\mathbb{N}}$ where the bit matrix $B = \rho_n \in M_{2^n}$ satisfies $b_{\sigma,\tau} = 1 \iff \sigma = \tau = Z \upharpoonright n$.
- If all the $\rho_n$ are diagonal matrices, we describe a measure on Cantor space $\{0,1\}^{\mathbb{N}}$.

# Martin-Löf's test notion for bit sequences = reals

- A Martin-Löf test is an effective sequence $(U_m)_{m \in \mathbb{N}}$ of open sets in $[0,1]$ such that the Lebesgue measure of $U_m$ is at most $2^{-m}$.
- Intuitively, $U_m$ is an attempt to approximate a bit sequence (or real) $Z$ with accuracy $2^{-m}$.
- $Z$ passes the test if $Z$ is not in all $U_m$.
- $Z$ is called Martin-Löf random if it passes all ML-tests.



# Projections and measurements of states

- A projection in $M_{2^n}$ is a Hermitian matrix $p$ such that $p^2 = p$.
- A special projection in $M_{2^n}$ is a projection with matrix entries in $\mathbb{C}_{\mathtt{alg}}$, the field of algebraic complex numbers.

The expression $\mathsf{tr}(\eta\, p)$, where $\eta$ is a density matrix in $M_{2^n}$ and $p$ a projection in $M_{2^n}$, is the expected squared length of projecting $\eta$ onto the range of $p$.

We can view $\rho(p_n)$ as a measurement of state $\rho \in \mathcal{S}(M_\infty)$ with the observable $p_n$. So $\rho(p_n) = \mathsf{tr}(\rho_n p_n)$ is the probability that $\rho$ is "in" $p_n$. In the classical case this is simply $1$ (in) or $0$ (out).

# Quantum ML randomness (N. and Scholz, 2019)

- A test component $G$ is given by a computable ascending sequence of special projections $\langle p_n \rangle_{n\in\mathbb{N}}$ where $p_n \in M_{2^n}$.
- For $\rho \in \mathcal{S}(M_\infty)$ let $\rho(G) = \sup_n \rho(p_n)$.
- In particular, $\tau(G) = \sup_n 2^{-n}\mathsf{tr}(p_n)$.

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

Think of the $\langle G_r \rangle_{r\in\mathbb{N}}$ as forming a sequence of measurements, with asymptotic value $\inf_r \rho(G_r)$ at $\rho$. If all the pieces are classical we re-obtain the usual definition of Martin-Löf tests.

# Tracial state is random according to this definition

- A probability measure on Cantor space can be seen as a state of the form $\rho = (\rho_n)_{n\in\mathbb{N}}$ where all the $\rho_n$ are diagonal matrices.
- The tracial state $\tau$ corresponds to the usual Lebesgue measure. This is the case where each diagonal entry of $\tau_n$ is $2^{-n}$.
- This state is random according to our definition, because $\tau(G_m) \to 0$ for each qML test $(G_m)$.
- This is compatible with our intuition because each $\tau_n$ is a fully mixed state, so has no structure.

# Facts about quantum Martin-Löf randomness

One of Martin-Löf's results was the construction of a universal test for bit sequences.

**Proposition**

There is a universal quantum ML-test.

If one wants to test classical bit sequences, the additional power of quantum ML-tests doesn't help.

**Theorem**

*Suppose* $Z \in \{0,1\}^{\mathbb{N}}$. *Then* $Z$ *is ML-random* $\Longleftrightarrow$

$Z$ *viewed as an element of* $\mathcal{S}(M_{2^\infty})$ *is qML-random.*

# Quantum Solovay test

**Definition (Quantum Solovay randomness)**

- A quantum Solovay test is an effective sequence $\langle G_r \rangle_{r \in \mathbb{N}}$ of quantum $\Sigma^0_1$ sets such that $\sum_r \tau(G_r) < \infty$.
- We say that the test is restricted if the $G_r$ are given as projections; that is, from $r$ we can compute $n_r$ and a matrix of algebraic numbers in $M_{2^{n_r}}$ describing $G_r$.
- We say that $\rho$ is [weakly] quantum Solovay-random if $\lim_r \rho(G_r) = 0$ for each [restricted] quantum Solovay test $\langle G_r \rangle_{r \in \mathbb{N}}$.

**Theorem (Bhojraj, 2021)**

Quantum Martin-Löf random $\Longleftrightarrow$ quantum Solovay random.

The Solovay definition implies that the set of qML states is convex.

# Descriptive QK complexity and weak Solovay rd.

Levin-Schnorr theorem: an infinite bit sequence is ML-random iff each of its initial segment is incompressible in the sense of prefix free Kolmogorov complexity $K$. We seek analogs for infinite qubit sequences. The first was in Nies/Scholz 2019. This one is new:

**Definition (Bhojraj, 2021)**

Let $\alpha$ be a density matrix in $M_{2^n}$. For $\epsilon > 0$, define

$$QK^\epsilon(\alpha) = \min\{K(p) + \log|p| : \\ p \in M_{2^n} \text{ is special projection} \wedge \mathsf{tr}(\alpha\, p) > \epsilon\}.$$

Here $|p|$ is the dimension of the range of $p$.

**Theorem (Bhojraj, 2021)**

A state $\rho = \langle \rho_n \rangle$ passes all restricted Solovay tests $\iff$ for each $\epsilon$, $\lim_n QK^\epsilon(\rho_n) - n = \infty$.

# Initial segment characterizations

Bhojraj showed quantum Schnorr randomness is equivalent to incompressibility w.r.t. a restricted version of $QK$ where the decompression is carried out by computable measure machines.

Diagram of some of the results in his JMP and TCS papers:

$$
\begin{tikzcd}
\text{q-ML rd.} \arrow[rr, Leftrightarrow, "\text{JMP}"'] \arrow[dd, Rightarrow] & & \text{q-Sol. rd.} \arrow[d, Rightarrow] \\
& \text{QK-incompr.} \arrow[r, Leftrightarrow, "\text{TCS}"'] \arrow[d, Rightarrow] & \text{q-weak Sol. rd.} \\
\text{q-Schnorr rd.} \arrow[r, Leftrightarrow, "\text{TCS}"'] & \text{QK}_C\text{-incompr.} &
\end{tikzcd}
$$

# An initial segment condition for randomness, based on entropy

- The von Neumann entropy of a density matrix $S \in M_n$ is $H(S) = -\mathsf{tr}(S \log_2 S)$.
- This is the usual entropy of the distribution that $S$ induces on its eigenvectors.
- Its maximum value is $n$, when the distribution is uniform.

**Theorem (Bhojraj, Thesis, UW Madison 2021, Thm. 5.4)**

Let $\rho$ be a state on $M_\infty$. Suppose there is a constant $b \in \mathbb{N}$ such that $H(\rho_n) \geq n - b$ for infinitely many $n$.

Then $\rho$ is quantum ML-random.

For instance, this applies to the tracial state $\tau$; but Bhojraj constructs further examples. The converse fails.

# Effective SMB theorem

- A 1950s theorem due to Shannon, McMillan and Breiman says that the (global) entropy of an ergodic measure $\mu$ on $\{0,1\}^{\mathbb{N}}$ equals the empirical entropy $-\lim_n \frac{1}{n} \log_2 \mu[Z \upharpoonright n]$ for $\mu$-almost every bit sequence $Z$.
- If $\mu$ is computable, and $Z$ is ML-random w.r.t. $\mu$, then its empirical entropy determines the entropy of $\mu$ (Hochman, 2009).
- Bjelakovic, Krueger, Siegmund and Szkola (2004) proved a version of the Shannon-McMillan theorem for ergodic quantum lattice systems. Since there is no notion of null set of states, they use an ad hoc, finitary definition of "for almost".
- We present a conjecture that attempts to remedy this, using that quantum ML-tests are a quantum analog of effective null sets of bit sequences.

# Effective quantum SMB theorem?

- A state $\mu$ on $M_\infty$ is called ergodic if it is an extreme point on the convex set of shift invariant states.
- $h(\mu) = \lim_n \frac{1}{n} H(\mu_n)$ is the von Neumann entropy of $\mu$.
- Define qML-randomness relative $\mu$ as before, but with the condition $\mu(G_r) \leq 2^{-r}$ when defining tests.

**Conjecture (with Marco Tomamichel, Nies Logic Blogs 2017, 2020)**

Suppose that for some $D > 0$, for each $n$, the diagonal entries of $\mu_n$ are bounded below by $2^{-nD}$. Let $\rho$ be a state that is quantum ML-random with respect to $\mu$. Then

$$h(\mu) = -\lim \frac{1}{n} \mathsf{tr}(\rho_n \log_2 \mu_n).$$

This is known when $\mu$ is a diagonal state. See Logic Blog 2020 Prop 9.3 (arxiv.org/abs/2101.09508).

# Conclusions

- We have seen that notions from computability theory and algorithmic randomness interact meaningfully with the study of finite and infinite abstract spin chains.
- We've discussed two papers showing that the existence of a spectral gap is undecidable.
- We have defined infinite qubit sequences, and extended Martin-Löf randomness for classical bit sequences to the quantum setting.
- To find connections between the two approaches to spin chains, one would have to first formulate a version of the Cubitt et al. results for infinite qudit chains.
- Hamiltonians have been studied in this case, but they are usually not bounded, and only defined on a dense Hilbert subspace. See papers and books by Nachtergaele, Naaijkens, Sims, also Bjelakovic

J. Bausch, T. Cubitt, AngeA. Lucia, D. Perez-Garcia, and M. Wolf.
Size-driven quantum phase transitions.
*arXiv preprint arXiv:1512.05687*, 2015.

I. Bjelaković, T. Krüger, R. Siegmund-Schultze, and A. Szkoła.
The Shannon-McMillan theorem for ergodic quantum lattice systems.
*Inventiones mathematicae*, 155(1):203–222, 2004.

T. Bjojraj.
Algorithmic Randomness and Kolmogorov Complexity for Qubits.
Thesis, 2021
Arxiv 2106.14280.

A. Nies.
*Computability and Randomness*, volume 51 of *Oxford Logic Guides*.
Oxford University Press, Oxford, 2009.
444 pages. Paperback version 2011.

A. Nies and V. Scholz.
Martin-Löf random quantum states.
*Journal of Mathematical Physics*, 60(9):092201, 2019.

available at doi.org/10.1063/1.5094660.