Lecture 14

Nov 12, 2024

Notion of non-deterministic q. computation.

Also of interest as it relates to major questions of interest in q. mechanics.

Does QMA have the same error-amplification properties of BQP?

<u>Yes</u>. But it is not as easy as repeat multiple times.

B.c. measurement is perturbative. After running $C(|\psi\rangle, |0^m\rangle)$ the state $|\psi\rangle$ may be destroyed.

Easiest to switch to Prover & Verifier interaction perspective

Prover

$$\Big\downarrow |\psi\rangle$$

Verifier runs $C(|\psi\rangle|0^m\rangle)$

and measures.

Goal. Come up with a better verifier which accepts with near certainty if $\exists$ an accepting witness and rejects with near certainty if $\nexists$ an accepting witness.

Idea: Have the (honest) prover send $|\psi\rangle^{\otimes T} \in (\mathbb{C}^2)^{\otimes nT}$

Issue: Prover may cheat and send a different entangled state $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes nT}$.

Resolution: One can show that best strategy for the prover is to send an unentangled state

But in fact, $\exists$ a verification algorithm with better acceptance and rejection probabilities that only needs 1 copy.

Requires Jordan's lemma.

The story of a QMA verification circuit C is a tale of two projectors.

$$\Pi_0 = \mathbb{1}_{2^n} \otimes |0\rangle\langle 0|^m$$

$$\Pi_1 = C^\dagger \left(|1\rangle\langle 1| \otimes \mathbb{1}_{2^{n+m-1}} \right) C.$$

$\Pi_0 |\bar{\psi}\rangle = |\bar{\psi}\rangle$ where $|\bar{\psi}\rangle = |\psi\rangle \otimes |0^m\rangle$.

Π_0 checks input has correct ancilla.

Π_1 checks computation + measurement accepts.

<u>Jordan's lemma</u> Given two projectors $A, B \in \mathbb{C}^{D \times D}$, $\exists$ a change of basis s.t. A, B are block-diagonal with 1- or 2-dim blocks.

<u>Pf</u>. Let $|v\rangle$ be λ- eigenvector $(\lambda \neq 0)$ of $A+B$. Then,

$$A|v\rangle + B|v\rangle = \lambda |v\rangle.$$

if $A|v\rangle \in \mathrm{span}(|v\rangle)$, then $B|v\rangle \in \mathrm{span}(|v\rangle)$ and so A and B preserve the block spanned by $|v\rangle$.

if $A|v\rangle \notin \mathrm{span}(|v\rangle)$, then

$$B|v\rangle \in \mathrm{span}\big(A|v\rangle, |v\rangle\big) =: S$$

Then, $A\big(\alpha A|v\rangle + \beta|v\rangle\big) = \alpha A|v\rangle + \beta A|v\rangle \in S.$

& $B\big(\alpha A|v\rangle + \beta|v\rangle\big) = B\Big(\alpha\big(\lambda|v\rangle - B|v\rangle\big) + \beta|v\rangle\Big)$

$$\propto B|v\rangle \in S.$$

So, S is preserved by both A and B. Recursion finishes decomposition.

Applying Jordan's lemma to QMA verifiers.

Decompose Π_0, Π_1 using Jordan's lemma.

<u>Claim</u> Acceptance prob. $= \max_{|\bar{\Psi}\rangle} \| \Pi_1 \Pi_0 |\bar{\Psi}\rangle \|^2$

Pf. when $|\bar{\Psi}\rangle = |\psi\rangle \otimes |0^m\rangle$ for optimal $|\psi\rangle$, then LHS $\leq$ RHS.

To show LHS $\geq$ RHS, use witness $|\psi\rangle = \Pi_0 |\bar{\Psi}\rangle$. ∎

Equiv. acceptance prob $= \lambda_{max}\left(\Pi_0 \Pi_1 \Pi_0\right)$

needed for Hermiticity.

$\Pi_0 \Pi_1 \Pi_0$ is also block-diagonal

so λ_{max} is max eigenvalue over blocks.

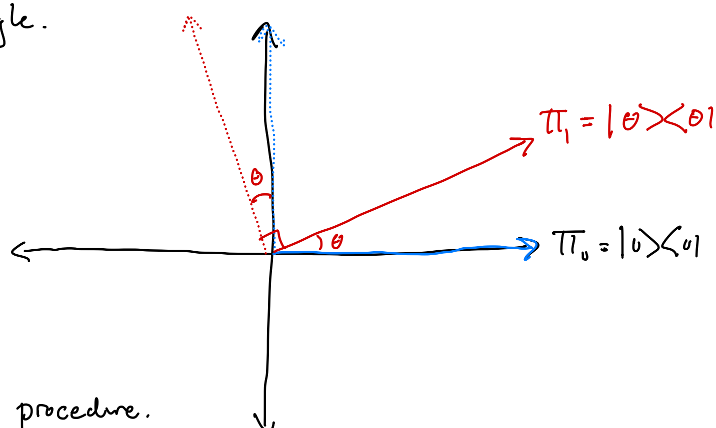
Consider the block of max eigenvalue.

If either Π_0 or $\Pi_1 = \mathbb{1}$, then easy as max eigenvalue $= 1$.

So, $\exists$ a $|\tilde{\Psi}\rangle$ s.t. $\Pi_0 \Pi_1 \Pi_0 |\tilde{\Psi}\rangle = |\tilde{\Psi}\rangle$.

Otherwise, let θ = angle.

$\lambda_{max} = \cos^2 \theta$.



Consider the following procedure.

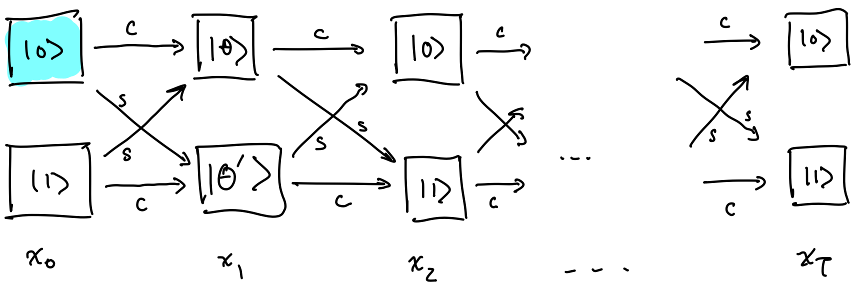
- Start with $|0\rangle$. Set $x_0 = 0$.
- Measure in $\{|\theta\rangle, |\theta + \frac{\pi}{2}\rangle\}$ basis. Set $x_1 = 0$ or 1, respectively.
- Measure in $\{|0\rangle, |1\rangle\}$ basis. Set $x_2 = 0$ or 1, respectively.

— Measure in $\{|\theta\rangle, |\theta + \frac{\pi}{2}\rangle\}$ basis. Set $x_3 = 0$ or 1, respectively.

$\vdots$

— Measure in $\{|0\rangle, |1\rangle\}$ basis. Set $x_T = 0$ or 1, respectively.

$c = \cos^2\theta$, $s = \sin^2\theta$ $\quad c + s = 1$.



Let $y_t = x_t \oplus x_{t-1}$. Change in t-th step.

$\mathbb{E}\, y_t = s$.

Use Chernoff bound argument on y_t to estimate s. And therefore c.

Lifted to original problem.

Algorithm($|\psi\rangle$):

(0) Start with $|\bar{\psi}\rangle = |\psi\rangle \otimes |0^m\rangle$. Set $x_0 = 0$.

(1) Apply C. Measure output and record as x_1. Appl $C^\dagger$.

② Measure POVM $\{\Pi_0, \mathbb{1} - \Pi_0\}$. Record as x_2.

(Not the same as measuring all ancilla, similar to Grover reflection operator)

1 Y

③ Apply C. Measure output and record as x_3. Apply $C^\dagger$.

⋮

Ⓣ Measure POVM $\{\Pi_0, \mathbb{1} - \Pi_0\}$. Record as x_T.

(T+1) Compute $y_t = x_t \oplus x_{t-1}$ for $t = 1, \dots T$.

Accept if $\sum y_t \le \frac{1}{3} T$.

By Chernoff analysis + Jordan's lemma,

if $\langle C \rangle \in L_{yes}$ and prover gave valid $|\psi\rangle$, then

we accept with prob. $1 - \exp\left(-\Omega(T)\right)$.

if $\langle C \rangle \in L_{no}$, $\forall\, |\psi\rangle$, we accept with prob. $\le \exp\left(-\Omega(T)\right)$.

The local Hamiltonian problem

Why study QMA?

- Quantum generalization of NP
- Has a complete problem that is very interesting for physics.

LH problem:

A k-local Hamiltonian term is a matrix $h_i = h_i^\dagger \in \mathbb{C}^{2^k}$ (wlog $1 \geq h_i \geq 0$) and a site $S_i \subseteq [n]$ with $|S_i| = k$.

The Ham. term can also be seen as $(h_i)_{S_i} \otimes \mathbb{1}_{[n]\setminus S_i}$ as an operator on $(\mathbb{C}^2)^{\otimes n}$.

A k-local Hamiltonian (system) is a collection of k-local Hamiltonian terms and we define

$$H = \sum_{i=1}^{m} h_i \in \mathbb{C}^{2^n \times 2^n}.$$

$\lambda_{min}(H)$ = ground energy.

Problem $(\langle H \rangle, a, b)$:

Decide if $\underbrace{\lambda_{min}(H) \le a}_{\text{yes}}$ or $\underbrace{\lambda_{min}(H) \ge b}_{\text{No}}$.

Note: $\langle H \rangle$ is the succinct $O\left(m\left(2^k + k \log n\right)\right)$ size description given by describing each h_i.

① LH is a generalization of CSPs.

3-SAT clause $x_1 \vee x_2 \vee \neg x_3 \implies$

$$h_i = \text{diag}(0, 0, 0, 0, 0, 0, \underset{\substack{\uparrow \\ (0,0,1) \\ \text{site.}}}{1}, 0)$$

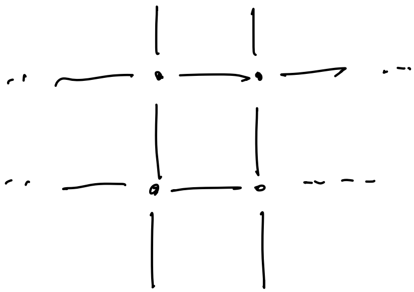
Each term checks a local energy term.

When h_i are <u>all</u> diagonal, $\lambda_{min}(H)$ occurs at a basis vector.

Corresponds to the classical optimal solution to the CSP.

LHs are the Hermitian generalizations of CSPs.

(2) LHs capture Physical systems of interest:



$$H = -J\left(\sum_{i \sim j} Z_i Z_j + g \sum_j X_j \right)$$

transverse field Ising model.

Describes particle interactions in many-body q. mechanics.

Calculating groundstates of LHs is of critical interest in physics.

Calculating groundenergy is the decision version of the search problem.

<u>Claim</u> $LH \in QMA$.

Say prover sends you witness $|\psi\rangle \in \mathbb{C}^{2^n}$.

<u>Algorithm</u> $(|\psi\rangle)$:

Pick a random Ham term h_i, acting on S_i.

Write $h_i = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ ← spectral decomposition

Measure $|\psi\rangle$ with POVM P_i

$$\{|\psi_j\rangle\langle\psi_j|\}_{S_i} \otimes \mathbb{1}_{-S_i}.$$

For measurement outcome j, accept if $\lambda_j < \frac{b}{m}$.

Proof.

Let's compute the expectation over λ_j output:

By construction, measuring the POVM P_i gives us expected outcome

$$\sum_j \lambda_j \langle\psi|\left(|\psi_j\rangle\langle\psi_j| \otimes \mathbb{1}\right)|\psi\rangle$$

$$= \langle\psi| h_i |\psi\rangle.$$

Expectation over i gives output $\langle\psi| \mathbb{E} h_i |\psi\rangle = \frac{1}{m}\underbrace{\langle\psi|H|\psi\rangle}_{E}.$

Let $X \in [0,1]$ be the outcome of λ_j.

$$\mathbb{E}X = \frac{E}{m}$$

If yes instance: $E \leq a$ so $\mathbb{E}X \leq \frac{a}{m}$.

If no instance: $E \geq b$ so $\mathbb{E}X \geq \frac{b}{m}$.

Using $X \in [0,1]$, we can show (exercise) that

$$\Pr[\text{accept} \mid \text{yes}] \geq 1 - \frac{a}{m} \quad \text{and} \quad \Pr[\text{accept} \mid \text{no}] \leq 1 - \frac{b}{m}.$$

gap between completeness and soundness $= \dfrac{b-a}{m}$.

Since $m \leq n^k$, as long as $b - a \geq 1/\text{poly}(n)$,

$LH_{a,b}$ is in QMA.

Proving local Hamiltonian is QMA-hard:

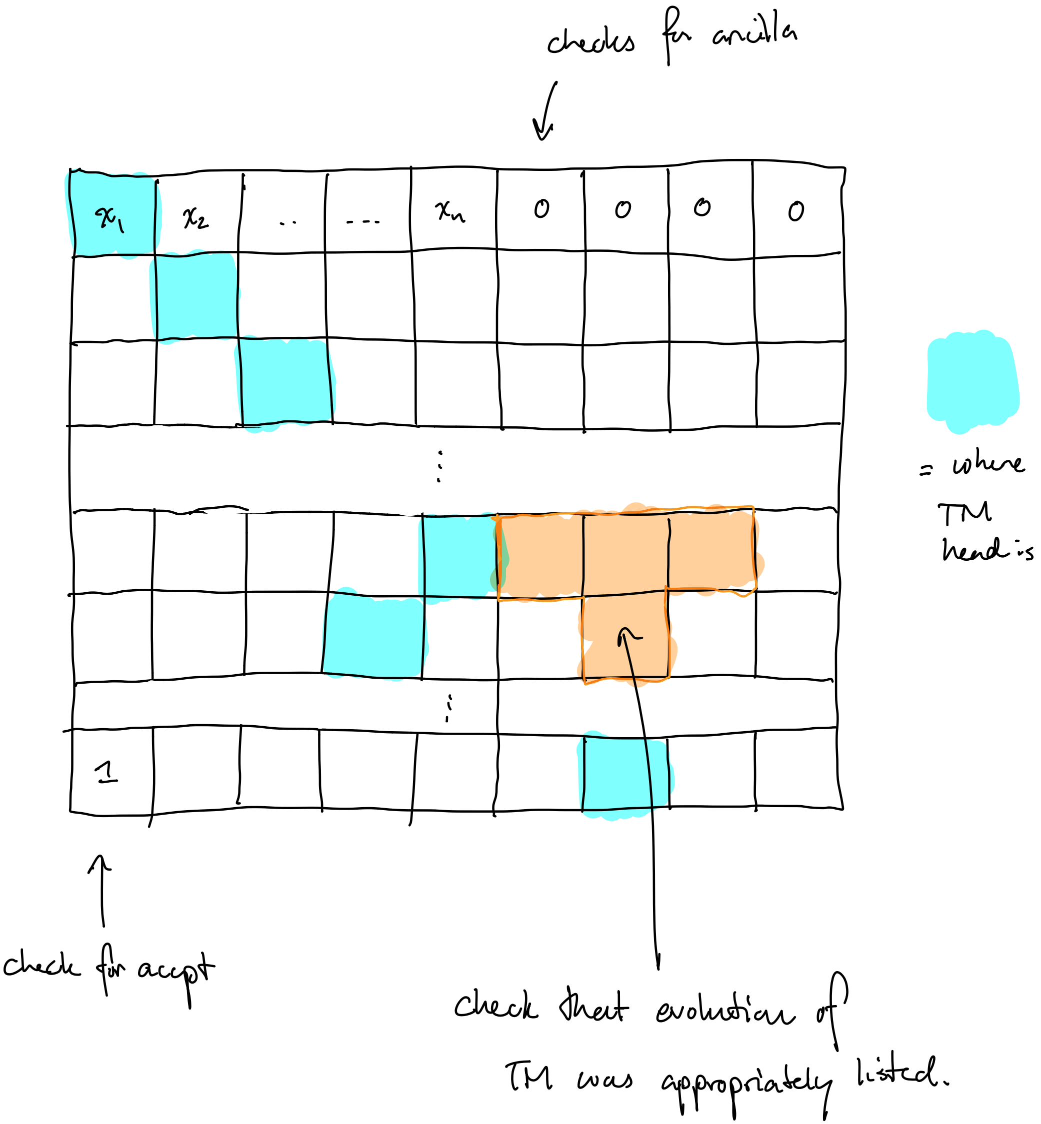
In class, we will only prove that $\underbrace{O(\log n)}_{\leq k}$-LH is QMA-hard.

HW will include problem for proving 5-local hardness.

Quantum analog of the Cook-Levin theorem proving that 3-SAT is NP-complete.

Cook-Levin Tableau Review:

given classical computation of T time steps using total space S, write a $T \cdot S$ tableau with the state of the machine at time t in row t.



Can we construct the same for quantum comp?

Consider a circuit $C = g_T \cdots g_1$. Can we create a table with rows

$$|\psi_0\rangle = |\psi_{witness}\rangle \otimes |0^m\rangle$$

$$|\psi_1\rangle = g_1|\psi_0\rangle$$

$$|\psi_2\rangle = g_2 g_1|\psi_0\rangle = g_2|\psi_1\rangle$$

$$\vdots$$

$$|\psi_T\rangle = C|\psi_0\rangle.$$

Why does this not work? Local checks cannot verify the evolutions.

Ex. $|\psi_t\rangle = \dfrac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ and $g_{t+1} = Z_1$.

Then $|\psi_{t+1}\rangle = \dfrac{|0^n\rangle - |1^n\rangle}{\sqrt{2}}$.

Whereas if $g_{t+1} = \mathbb{1}$, then $|\psi_{t+1}\rangle = \dfrac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$.

Claim Any $k \le (n-1)$ reduced density matrix of $\dfrac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$ is

$$\frac{1}{2}\left(|0^k\rangle\langle 0^k| + |1^k\rangle\langle 1^k|\right).$$

So a check differentiating if $g_{t+1} = Z_1$ vs. $\mathbb{1}$ must be non-local if it can distinguish

$$|\psi_t\rangle \otimes |\psi_{t+1}\rangle \text{ from } |\psi_t\rangle \otimes |\psi_t\rangle$$

$$g_t = Z_1. \qquad\qquad g_t = \mathbb{1}$$

We need a better solution that can detect global changes that occur from local gates.

Let's create a $O(\log n)$-local Hamiltonian whose ground states are of the form

$$\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_t\rangle$$

t expressed in $\lceil \log(T+1) \rceil$ bits

and $|\psi_t\rangle = g_t \cdots g_1 |\psi_0\rangle$ (all related).

In order to write out the Ham. let's first understand

$$h = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes \mathcal{U} - |0\rangle\langle 1| \otimes \mathcal{U}^{\dagger} + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$h = \frac{1}{2}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^\dagger \\ -\mathcal{U} & \mathbb{1} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -\mathcal{U}^\dagger \\ \mathbb{1} \end{pmatrix}\begin{pmatrix} -\mathcal{U} & \mathbb{1} \end{pmatrix}$$

Then $\langle\psi|h|\psi\rangle$ for $h = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$ ← unnormalized eqns.

$$\frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^\dagger \\ -\mathcal{U} & \mathbb{1} \end{pmatrix}\begin{pmatrix} |\psi_0\rangle \\ |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} |\psi_0\rangle - \mathcal{U}^\dagger|\psi_1\rangle \\ -\mathcal{U}|\psi_0\rangle + |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\left(\langle\psi_0|\psi_0\rangle - \langle\psi_0|\mathcal{U}^\dagger|\psi_1\rangle - \langle\psi_1|\mathcal{U}^\dagger|\psi_0\rangle + \langle\psi_1|\psi_1\rangle\right)$$

$$= \frac{1}{2}\left\| |\psi_0\rangle - \mathcal{U}^\dagger|\psi_1\rangle \right\|^2.$$

h measures distance from states of the form

$$\frac{1}{\sqrt{2}}|0\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle\mathcal{U}|\psi_1\rangle.$$

Alternate proof of fact:

Let $V = |1\rangle\langle 1| \otimes U + |0\rangle\langle 0| \otimes \mathbb{1}$

$V^\dagger = |1\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}$

$$V^\dagger h V = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes \mathbb{1} - |0\rangle\langle 1| \otimes \mathbb{1} + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$= |-\rangle\langle -| \otimes \mathbb{1}.$$

So groundstates of $V^\dagger h V$ are states of the form

$|+\rangle \otimes |\psi_0\rangle$.

and $V^\dagger h V$ is a projector. So groundstates of h

are states of the form $V|+\rangle \otimes |\psi_0\rangle$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle U|\psi_0\rangle\right).$$

Apply this intuition to general Hamiltonian circuit

$$h_t = \frac{1}{2}\Big(|t\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes g_t - |t-1\rangle\langle t| \otimes g_t^\dagger + |t-1\rangle\langle t-1| \otimes \mathbb{1} \Big)$$

Same calculation will tell us that for $|\psi\rangle = \sum_t \alpha_t |t\rangle|\psi_t\rangle$

that

$$\langle\psi|h_t|\psi\rangle = \Big\| \alpha_{t-1}|\psi_{t-1}\rangle - \alpha_t\, g_t^\dagger\, |\psi_t\rangle \Big\|^2 .$$

But how do all the pieces act together? Analyze a rotation.

$$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1$$

$$V^\dagger = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_1^\dagger \cdots g_t^\dagger .$$

$$V^\dagger h_t V = \frac{1}{2}\Big(|t\rangle\langle t| \otimes \mathbb{1} - |t-1\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes \mathbb{1} + |t-1\rangle\langle t-1| \otimes \mathbb{1} \Big)$$

$$= \frac{1}{\sqrt{2}}\big(|t\rangle - |t-1\rangle \big) \frac{1}{\sqrt{2}}\big(\langle t| - \langle t-1| \big) \otimes \mathbb{1} .$$

So, $V^\dagger\Big(\sum_{t=1}^{T} h_t\Big)V =$

$$\frac{1}{2}\begin{pmatrix} 1 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix} \otimes \mathbb{1} .$$

This is a special matrix. It is the Laplacian of a line graph and also a circulant matrix. (also tri-diagonal)

$\lambda_0 = 0$, eigenvector $|\Psi_0\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle$.

$\lambda_1 \geq \frac{c}{T^2}$ $\leftarrow$ exercise / intuition from graph mixing time.

So, removing rotation by V:

$$H_{prop} = \sum_{t=0}^{T} h_t$$ is a Hamiltonian with

ground-energy $= 0$, groundstates of the form $\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi_0\rangle$

for any state $|\psi_0\rangle$ $\leftarrow$ highly degenerate groundspace.

and first non-zero energy of $\geq c/T^2$.

Next: Adding checks for ancilla and output and computing overall eigenvalues to make sure cheating provers are detected.