Making the leap to quantum PCPs

Chinmay Nirkhe
IBM Quantum

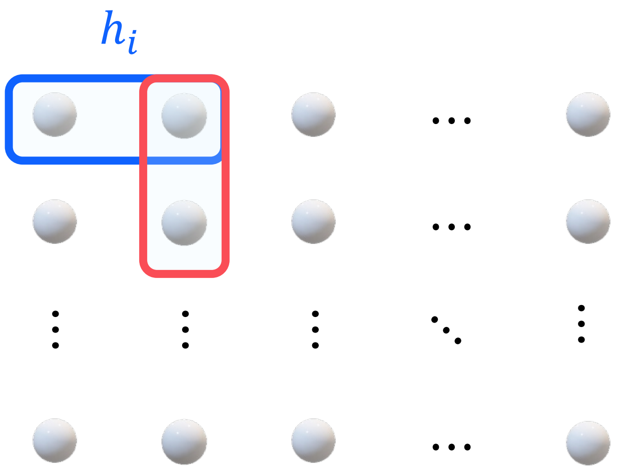
My goals today

A brief recap of NLTS result and it's scope

Possible next steps towards QPCPs

Chinmay Nirkhe
IBM Quantum

Calculating ground-energy is a hard problem



defined by local interactions

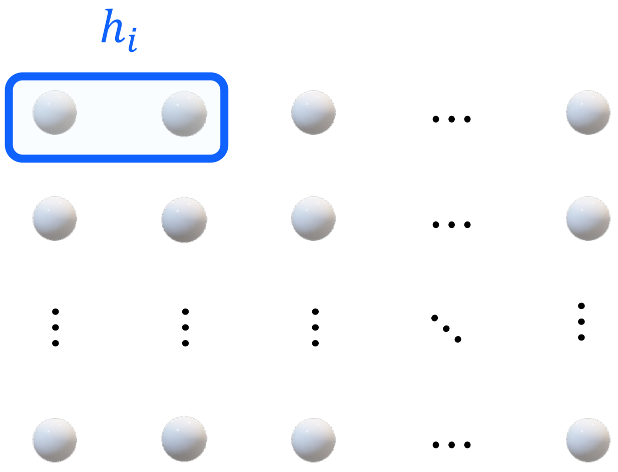
each k-local interaction is described by

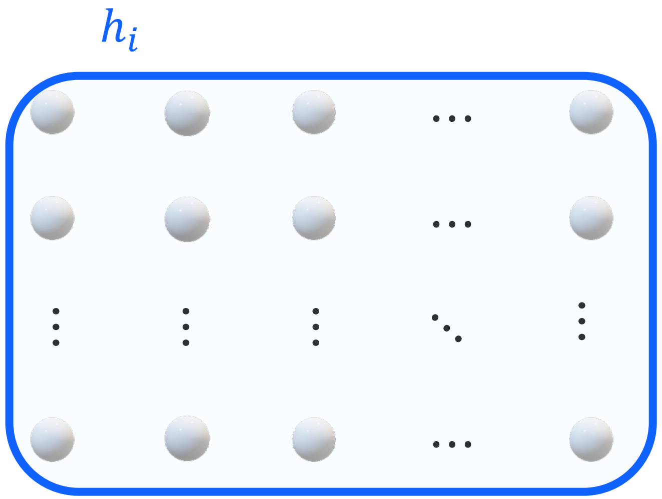
$$\text{Hamiltonian } h_i = \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix} \updownarrow 2^k$$

$$\longleftrightarrow 2^k$$

Calculating ground-energy is a hard problem

local Hamiltonian term

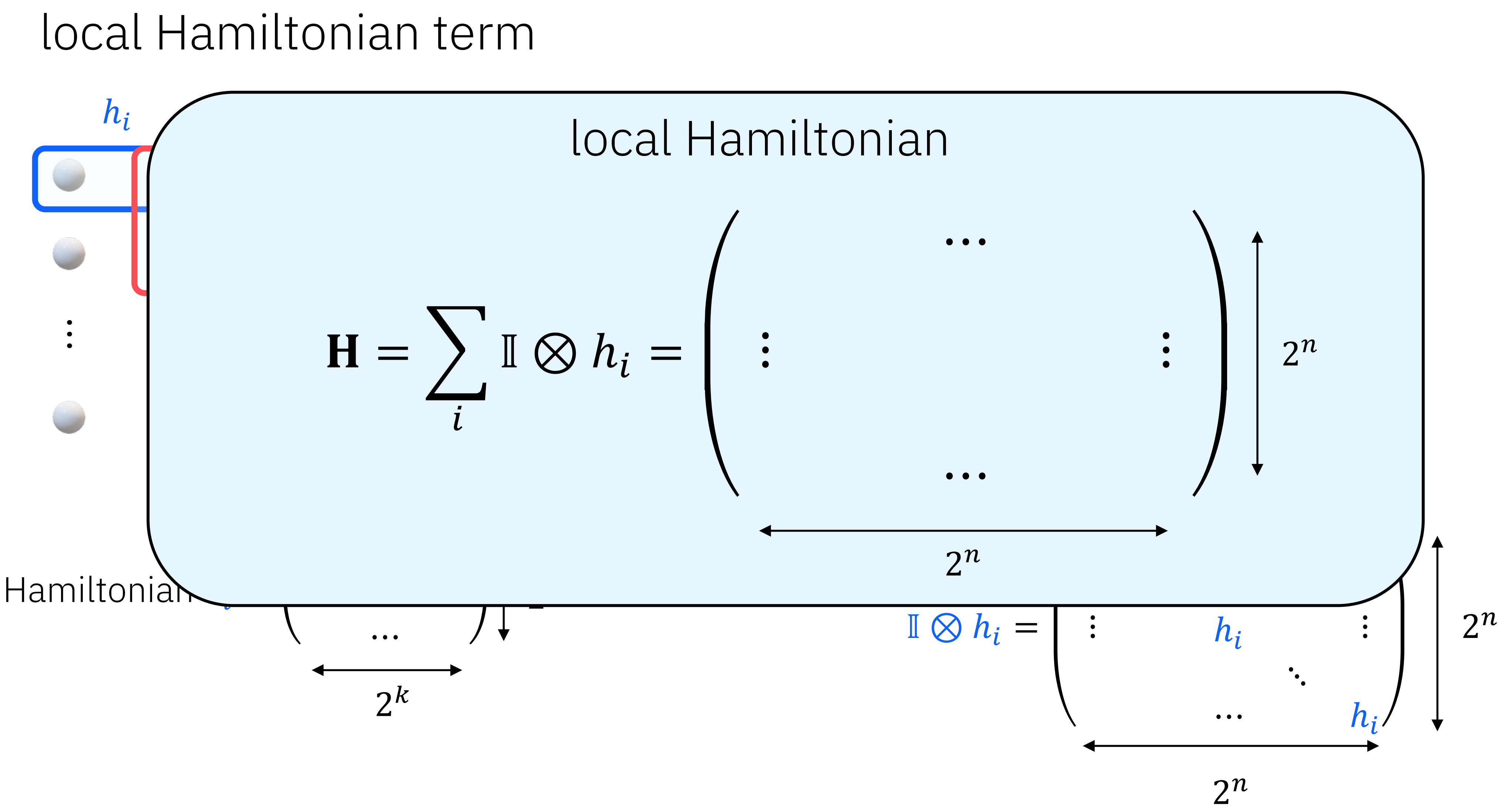




$$\text{Hamiltonian } h_i = \underbrace{\begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}}_{2^k} \updownarrow 2^k$$

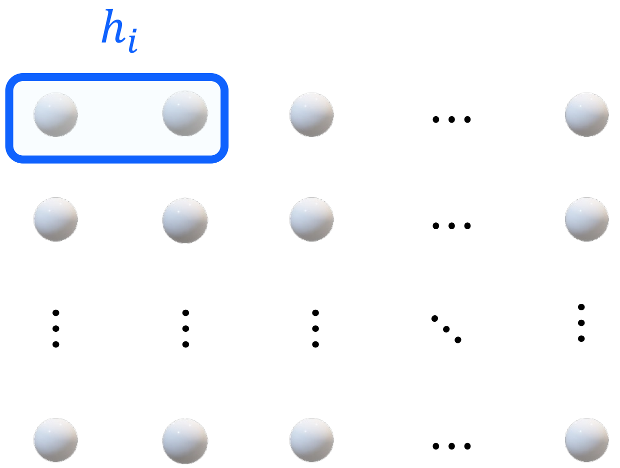
$$\mathbb{I} \otimes h_i = \underbrace{\begin{pmatrix} h_i & & \cdots & & \\ & h_i & & & \\ \vdots & & h_i & & \vdots \\ & & & \ddots & \\ & & \cdots & & h_i \end{pmatrix}}_{2^n} \updownarrow 2^n$$

Calculating ground-energy is a hard problem



Calculating ground-energy is a hard problem

$$\mathbf{H} = \sum_i \mathbb{I} \otimes h_i = \begin{pmatrix} & \cdots & \\ \vdots & & \vdots \\ & \cdots & \end{pmatrix}$$



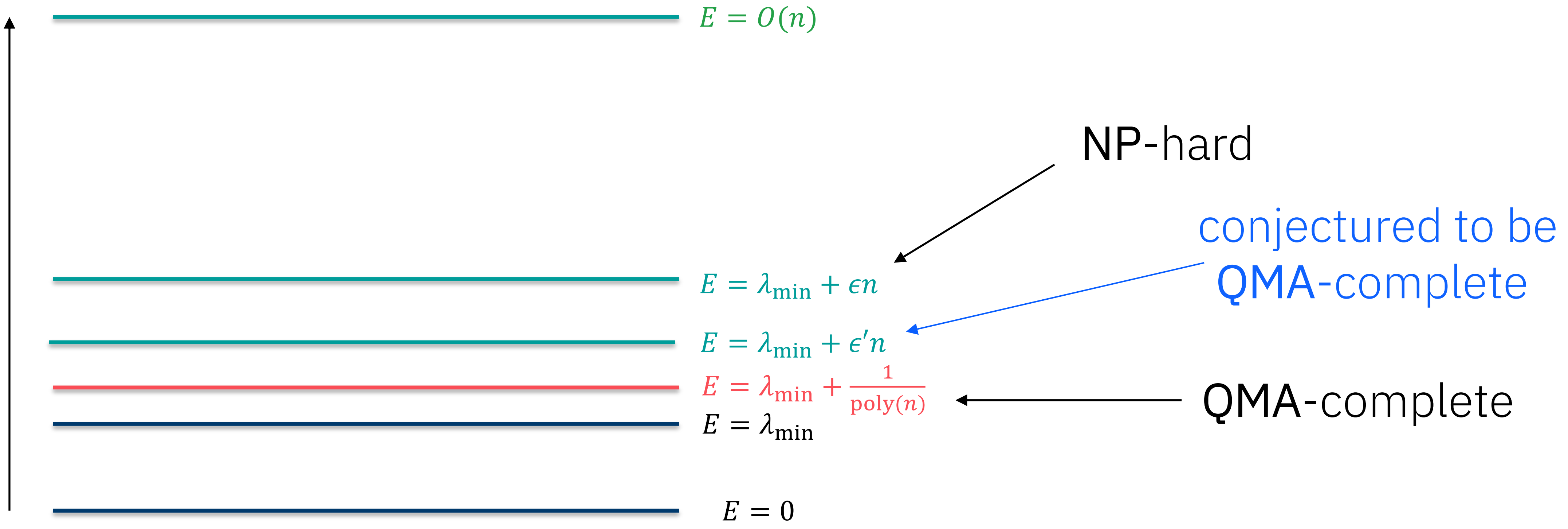
the relevant states in physics are the "low-energy" states of $\mathbf{H}$

energy of $|\psi\rangle := \langle\psi|\mathbf{H}|\psi\rangle$ (eigenvalue)

[Kitaev'99]: It is **QMA**-hard to calculate any value

$$\min_{|\psi\rangle} \langle\psi|\mathbf{H}|\psi\rangle \pm \frac{1}{\mathrm{poly}(n)}$$

How hard is ground-energy approximation?



Why are quantum PCPs harder to prove than PCPs?

No cloning theorem.

Dinur's 2007 proof of PCP theorem:

- Preprocessing
  - Convert interaction graph into expander
  - Replace high-locality variables with a cloud connected by consistency checks
- Gap amplification
  - Have each vertex describe not only it's assignment, but it's neighborhood
  - Check consistency between neighborhoods
- Alphabet reduction
  - Apply error-correction to reduce alphabet
  - Replace high-locality variables with a cloud connected by consistency checks
- Repeat $O(\log n)$ times

Many of these steps violate no-cloning theorem) although some can be avoided).

Why are quantum PCPs harder to prove than PCPs?

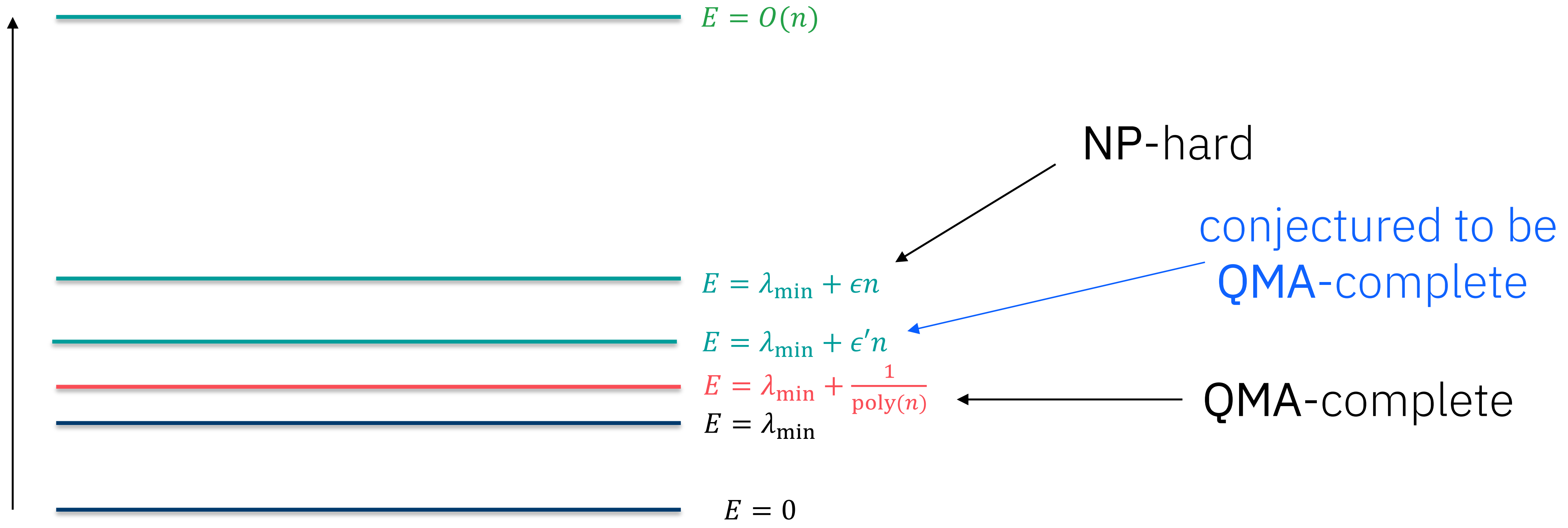
No cloning theorem.

Dinur's 2007 proof of PCP theorem:

- Preprocessing
  - Convert interaction graph into expander
  - Replace high-locality variables with a cloud connected by consistency checks
- Gap amplification
  - Have each vertex describe not only it's assignment, but it's neighborhood
  - Check consistency between neighborhoods
- Alphabet reduction
  - Apply error-correction to reduce alphabet
  - Replace high-locality variables with a cloud connected by consistency checks
- Repeat $O(\log n)$ times

Many of these steps violate no-cloning theorem) although some can be avoided).

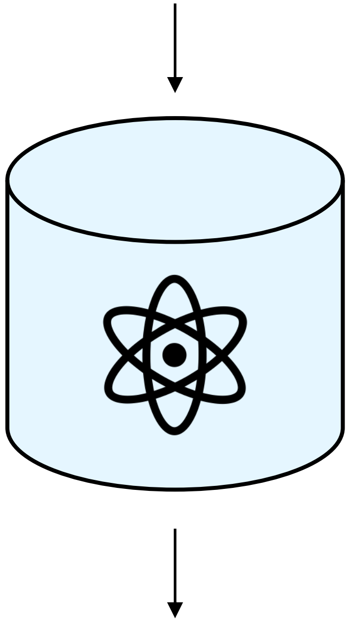
How hard is ground-energy approximation?



State complexity classes

Decision Complexity Class

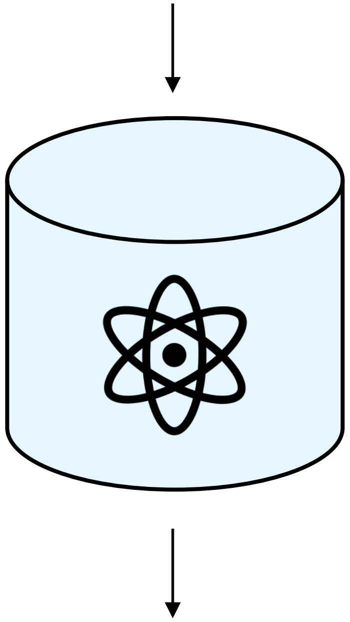
description of a decision problem
ex. Does C accept any quantum state?



yes/no (binary) answer

State Complexity Class

description of a quantum state
ex. the accepting quantum state of C



a quantum state ψ matching the description

The QPCP conjecture and state complexity

Def. (stateNP)
A set of strings $(x_n)_{n\in\mathbb{N}}$ is a **stateNP** representation of states $(\psi_n)_{n\in\mathbb{N}}$ if x_n can be used to calculate $\mathrm{tr}\,(O\psi_n)$ for any local observable O.

Examples
- x_n = description of a constant-depth quantum circuit
- x_n = description of matrix-product state
- x_n = listing of stabilizers for a stabilizer state

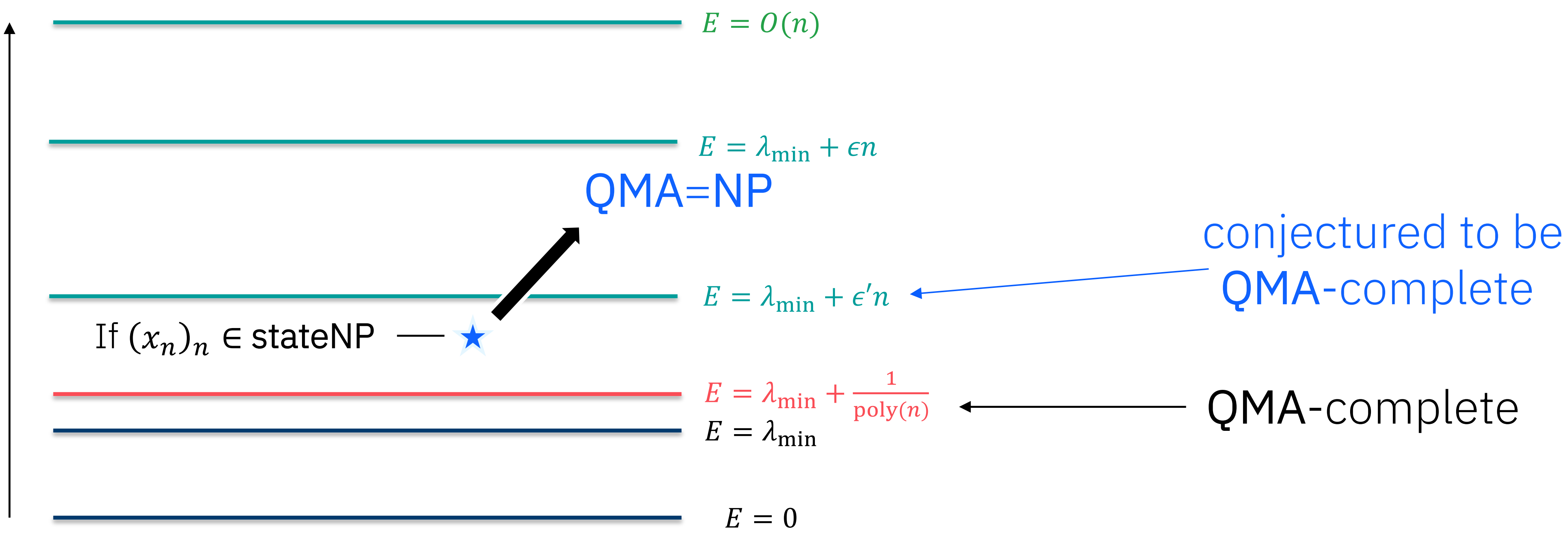
Non-Examples
- x_n = a list claiming to describing a map
$$O \mapsto \mathrm{tr}(O\psi_n)$$
- x_n = a purported classical shadow a quantum state ψ_n

The QPCP conjecture and state complexity

Def. (stateNP)
A set of strings $(x_n)_{n\in\mathbb{N}}$ is a stateNP representation of states $(\psi_n)_{n\in\mathbb{N}}$ if x_n can be used to calculate $\mathrm{tr}\,(O\psi_n)$ for any local observable O.

The QPCP conjecture and state complexity

<u>Def. (stateNP)</u>
A set of strings $(x_n)_{n\in\mathbb{N}}$ is a **stateNP** representation of states $(\psi_n)_{n\in\mathbb{N}}$ if x_n can be used to calculate $\mathbf{tr}\,(O\psi_n)$ for any local observable O.



The QPCP conjecture and state complexity

The QPCP conjecture implies State Complexity Lower Bounds!

QPCP conj. + $\mathcal{C} \neq$ **QMA** implies **state**$\mathcal{C}$ lower-bounds for ϵ-low energy states of local Hamiltonians.

Extracts the state complexity hardness statements underlying the QPCP conjecture.

When $\mathcal{C} =$ **NP**, **QPCP** conj. implies many **stateNP** lower bounds including

NLTS [FH'14]:
There exist local Ham. systems with every $\leq \epsilon n$-energy state requiring at least $\Omega(\log \log n)$ circuit depth

The NLTS problem

No Low-energy Trivial States (NLTS) Theorem
Anshu, Breuckmann, and ***Nirkhe*** *'22.*

For any $n > 0$, there exists an n-qubit local Hamiltonian system such that <u>every</u> $\leq \epsilon n$-energy state requires at least $\Omega(\log n)$ circuit depth.

Seq. of partial results: [EH'17,**N**VY'18,Eld'21,BKKT'19,A**N**'20,AB'22]

Robust entanglement can (theoretically) exist at room temperature!

Our proof of NLTS is based on *quantum error-correction*; specifically, high-rate and high-distance quantum error correcting codes

(more on this soon)

What should we try to solve next?

<u>Stronger state complexity bounds</u>

Construct local Hams. with state complexity lower bounds for all low-energy states

- NLSS conjecture [G-LG'22,CCNN'23]
- Trivially-rotated stabilizer states lower bounds

<u>Reintroduce computational hardness</u>

- Prove that QPCPs are MA-hard (or even just BQP-hard)
- Construct local Hams. which are simultaneous NLTS and NP-hard

The NLTS problem

No Low-energy Trivial States (NLTS) Theorem
Anshu, Breuckmann, and ***Nirkhe*** *'22.*

For any $n > 0$, there exists an n-qubit local Hamiltonian system such that <u>every</u> $\leq \epsilon n$-energy state requires at least $\Omega(\log n)$ circuit depth.

Seq. of partial results: [EH'17,**N**VY'18,Eld'21,BKKT'19,A**N**'20,AB'22]

Robust entanglement can (theoretically) exist at room temperature!

Our proof of NLTS is based on *quantum error-correction*; specifically,
high-rate and high-distance quantum error correcting codes

(more on this soon)

Proof sketch of the NLTS result

First, we need a method for proving circuit-depth lower bounds

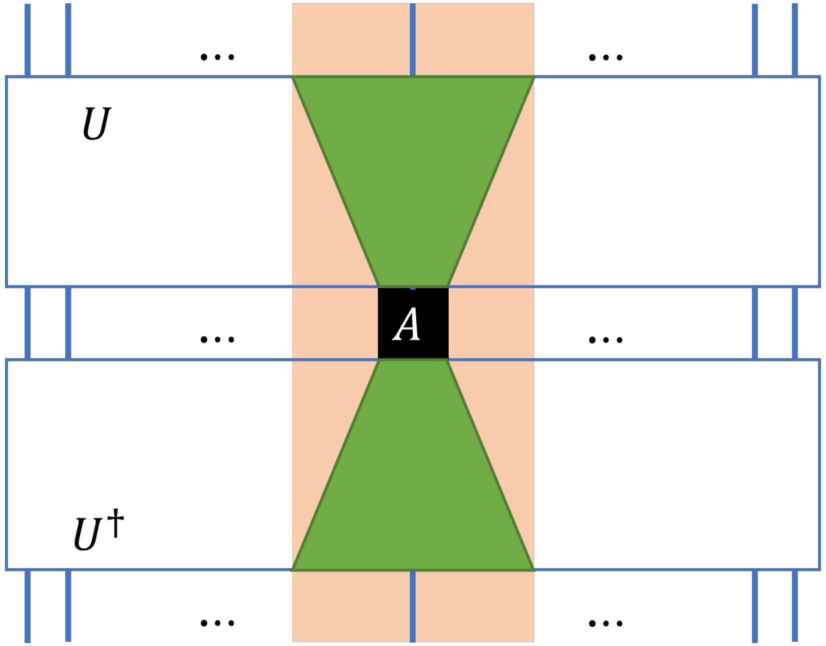
Fact 1

For every t-depth circuit C, the local Ham.

$$\mathbf{H} = \sum_{i=1}^{n} h_i = \sum_{i=1}^{n} C|1\rangle\langle 1|_i C^\dagger$$

is 2^t-local and has a *unique* ground-state of $C|0\rangle$ with spectral gap 1.

Proof: by induction on the depth of C.



Proof sketch of the NLTS result

Fact 2

Let $x_1, x_2, \ldots, x_m \in \{0,1\}^n$ be points such that $\left|x_i \oplus x_j\right| > L$. Then,

$$|\psi\rangle = \sum_{j=1}^{m} \alpha_j |x_j\rangle$$

cannot be the unique ground-state of a L-local Hamiltonian $\mathbf{H} = \sum h_i$.

Proof: Define

$$|\psi'\rangle = -\alpha_1 |x_1\rangle + \sum_{j=2}^{m} \alpha_j |x_j\rangle.$$

For any L $-$local term h,

$$\begin{aligned} \langle\psi|h|\psi\rangle &= \sum_{j,j'=1}^{m} \alpha_j \alpha_{j'}^{\dagger} \langle x_{j'}|h|x_j\rangle \\ &= \sum_{j=1}^{m} \left|\alpha_j\right|^2 \langle x_j|h|x_j\rangle \\ &= \langle\psi'|h|\psi'\rangle. \end{aligned}$$

Therefore, $\langle\psi|\mathbf{H}|\psi\rangle = \langle\psi'|\mathbf{H}|\psi'\rangle$ proving *non-uniqueness.*

Proof sketch of the NLTS result

Corollary

Let $x_1, x_2, \dots, x_m \in \{0,1\}^n$ be points such that $\left|x_i \oplus x_j\right| > L$. Then,

$$|\psi\rangle = \sum_{j=1}^{m} \alpha_j |x_j\rangle$$

is not the output of a $\mathbf{O(\log} \, L)$ depth quantum circuit.

Proof: Define

$$|\psi'\rangle = -\alpha_1|x_1\rangle + \sum_{j=2}^{m} \alpha_j|x_j\rangle.$$

For any L −local term h,

$$\begin{aligned}
\langle\psi|h|\psi\rangle &= \sum_{j,j'=1}^{m} \alpha_j \alpha_{j'}^{\dagger} \langle x_{j'}|h|x_j\rangle \\
&= \sum_{j=1}^{m} \left|\alpha_j\right|^2 \langle x_j|h|x_j\rangle \\
&= \langle\psi'|h|\psi'\rangle.
\end{aligned}$$

Therefore, $\langle\psi|\mathbf{H}|\psi\rangle = \langle\psi'|\mathbf{H}|\psi'\rangle$ proving *non-uniqueness.*

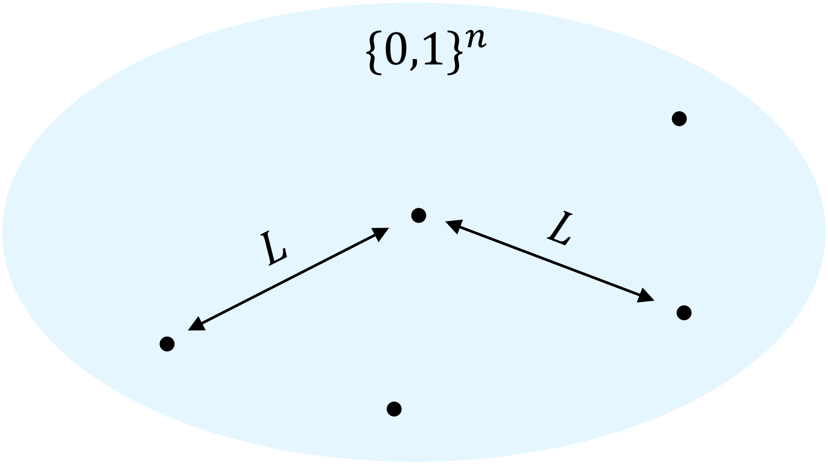
Proof sketch of the NLTS result

Corollary

Let $x_1, x_2, \ldots, x_m \in \{0,1\}^n$ be points such that $|x_i \oplus x_j| > L$. Then,

$$|\psi\rangle = \sum_{j=1}^{m} \alpha_j |x_j\rangle$$

is not the output of a $\mathrm{O}(\log L)$ depth quantum circuit.



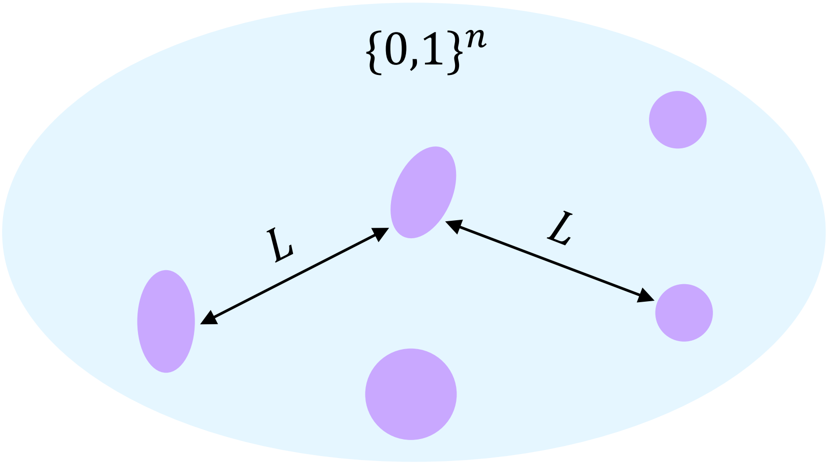
Proof sketch of the NLTS result

<u>Corollary</u>

Let $S_1, S_2, \dots, S_m \subset \{0,1\}^n$ be subsets such that $\mathrm{dist}(S_j, S_{j'}) > L$. Then

$$|\psi\rangle = \sum_{j=1}^{m} \alpha_j |v_j\rangle$$

for $\Pi_{S_j}|v_j\rangle = |v_j\rangle$ is not the output of a $\mathrm{O}(\log L)$ depth quantum circuit.



"well-spread dist."

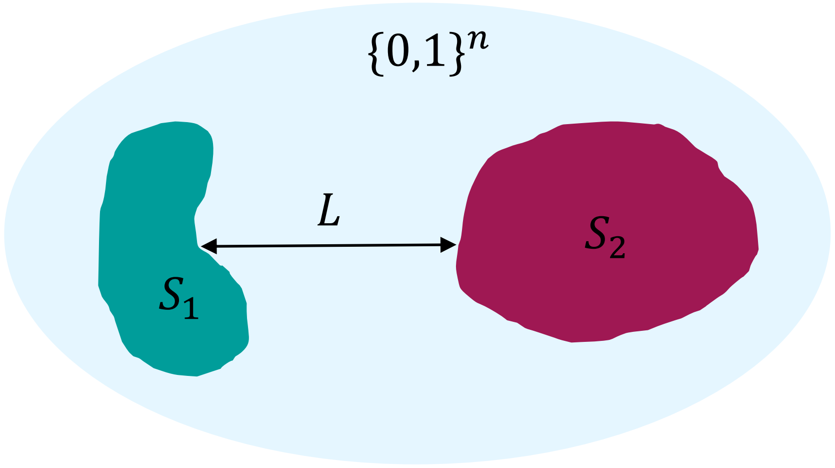
Robust well-spread lower bounds

Theorem

Let $S_1, S_2 \subset \{0,1\}^n$ be subsets such that $\mathrm{dist}(S_1, S_2) > L$. Any distribution D with mass $D(S_1), D(S_2) \geq \mu$

has circuit-depth lower bounds of

$$\Omega\left(\log\left(\frac{L^2\,\mu}{n}\right)\right).$$

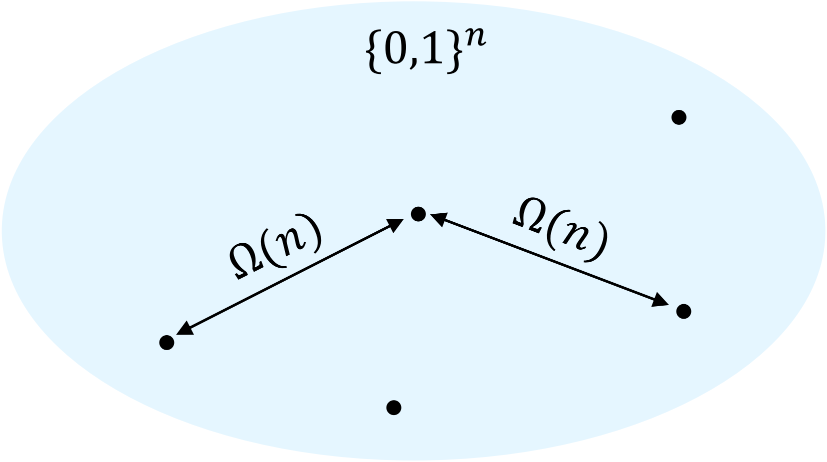


"well-spread dist."

Finding well-spread distributions

There is a really nice visual associated with classical error-correcting codes

What does the low-energy space look like? For classical codes, it includes any vector supported on $\{x : |Hx| \leq \epsilon n\}$



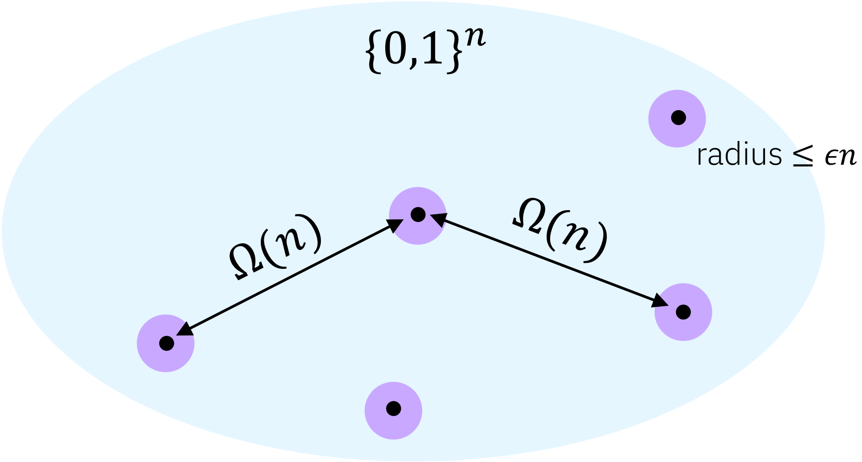
This is the view of the exact solutions to a linear-distance error-correcting code $\{x : |Hx| = 0\}$

If the matrix H represents a small-set expanding graph, then it looks like this

Finding well-spread distributions

There is a really nice visual associated with error-correcting codes

What does the low-energy space look like? For classical codes, it includes any vector supported on $\{x : |Hx| \leq \epsilon n\}$



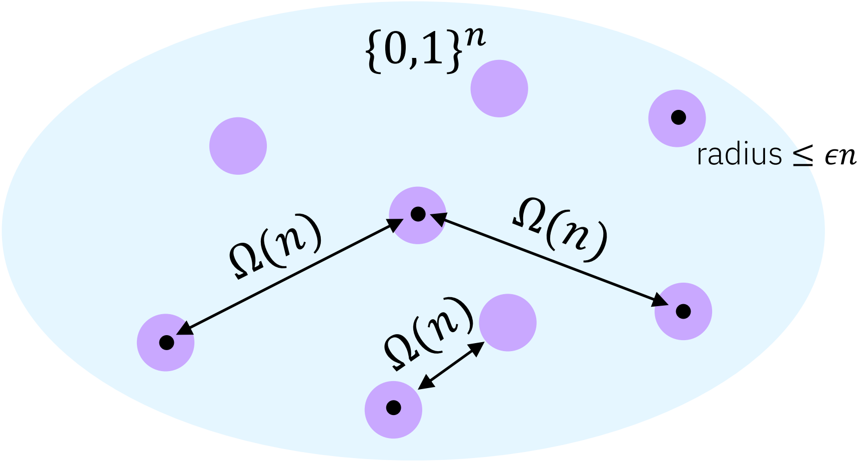
This is the view of the exact solutions to a linear-distance error-correcting code $\{x : |Hx| = 0\}$

If the matrix H represents a small-set expanding graph, then it looks like this

Finding well-spread distributions

There is a really nice visual associated with error-correcting codes

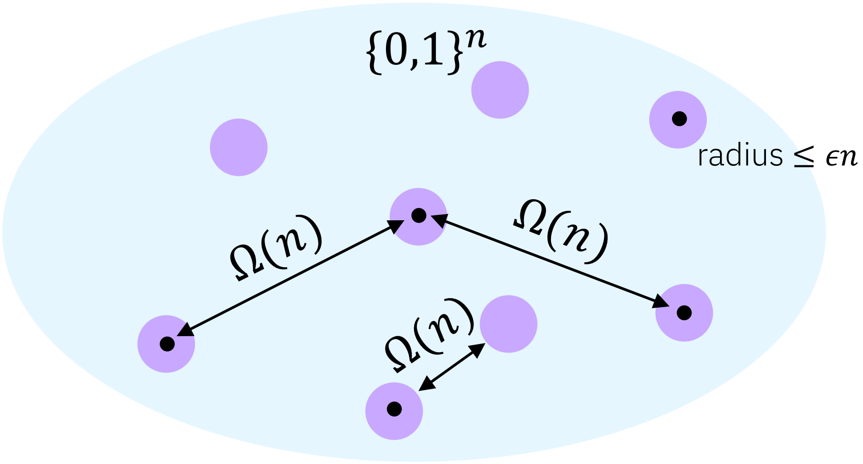
What does the low-energy space look like? For classical codes, it includes any vector supported on $\{x : |Hx| \leq \epsilon n\}$



This is the view of the exact solutions to a linear-distance error-correcting code $\{x : |Hx| = 0\}$

If the matrix H represents a small-set expanding graph, then it looks like this

Finding well-spread distributions



If there exists a low-energy state $|\psi\rangle$ supported only on these purple regions, then there exists a state $|\phi\rangle$ of the same energy but only supported on *one* purple region.

Proof: Let $|\psi\rangle = \sum_{j=1}^{m} \alpha |v_j\rangle$ with each $|\mathrm{v_j}\rangle$ supported on a different region.

Define

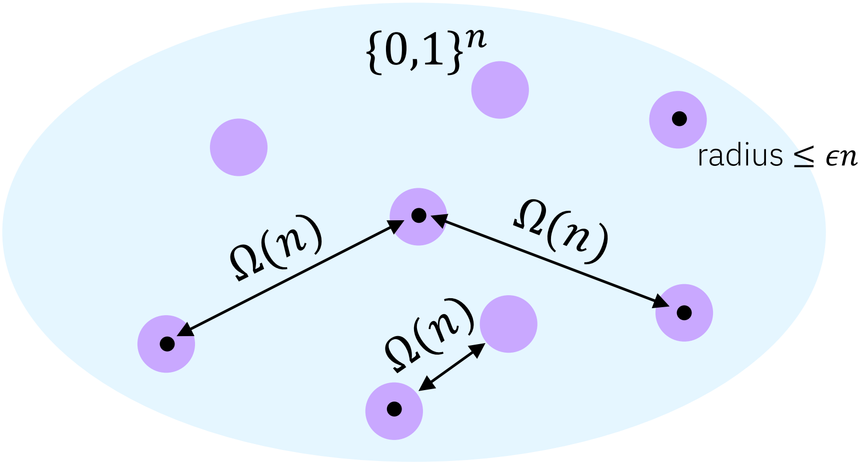
$$|\psi'\rangle = -\alpha_1|v_1\rangle + \sum_{j=2}^{m} \alpha_j|v_j\rangle.$$

For any L —local term h,

$$\begin{aligned}\langle\psi|h|\psi\rangle &= \sum_{j,j'=1}^{m} \alpha_j\alpha_{j'}^{\dagger}\langle v_{j'}|h|v_j\rangle \\ &= \sum_{j=1}^{m} |\alpha_j|^2 \langle v_j|h|v_j\rangle \\ &= \langle\psi'|h|\psi'\rangle.\end{aligned}$$

Then, $|v_j\rangle \propto |\psi\rangle - |\psi'\rangle$ and of equal energy to $|\psi\rangle$ and $|\psi'\rangle$.

Finding well-spread distributions



If there exists a low-energy state $|\psi\rangle$ supported only on these purple regions, then there exists a state $|\phi\rangle$ of the same energy but only supported on *one* purple region.

An apparent contradiction:

1. Find a state $|\psi\rangle$ that is well-spread
2. Find a local Hamiltonian $\mathbf{H}$ with $|\psi\rangle$ as a ground-state
3. States $|\phi\rangle$ supported on one region are also ground-states of $\mathbf{H}$
4. Can't prove that $|\phi\rangle$ is well-spread

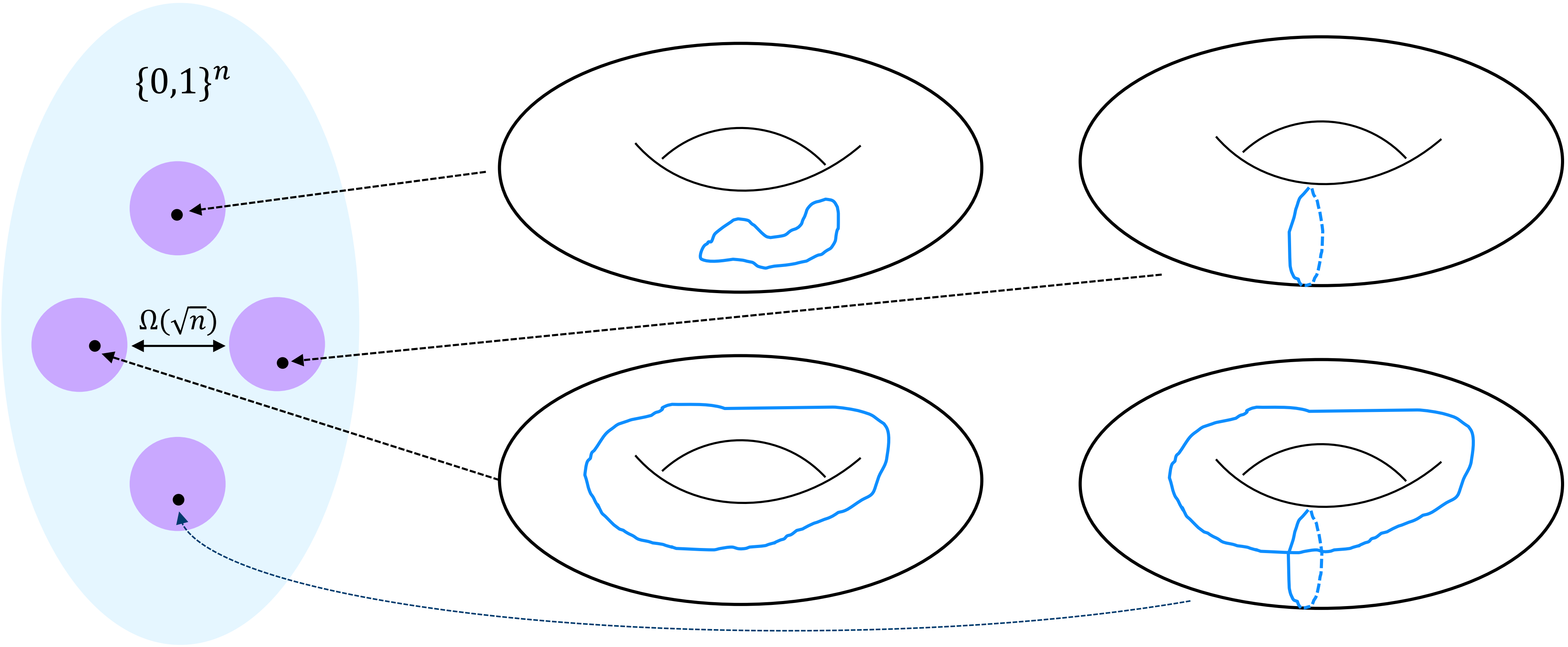
Multiple bases to the rescue

<u>Uncertainty lemma intuition:</u>
If a state's measurement in the Z-basis is rather *certain* then the measurement in the X-basis is rather *uncertain*.

$$\forall\, S,T \subset \{0,1\}^n, \qquad D_X(T) \leq 2\sqrt{1 - D_Z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Multiple bases to the rescue

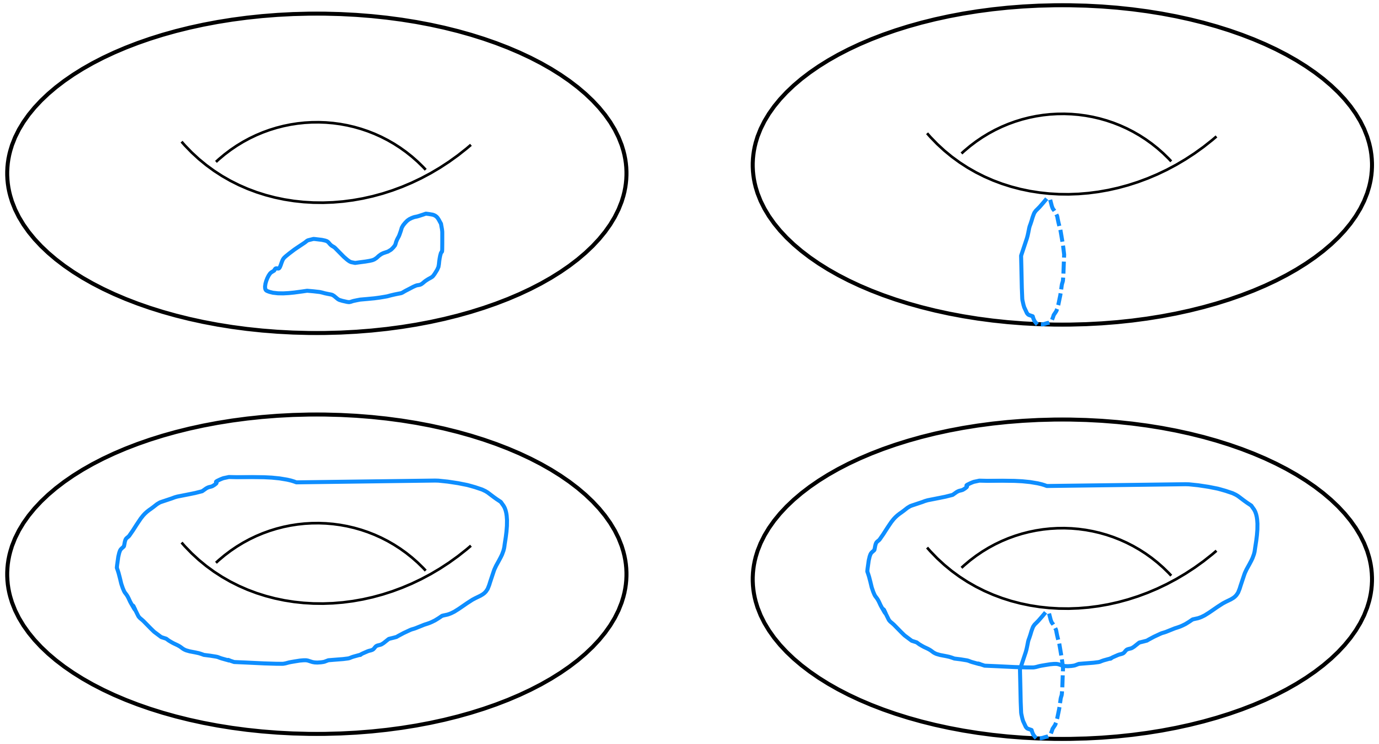
<u>The (current) NLTS intuition:</u>
Show that every low-energy state's measurement in the Z-basis *or* in the X-basis is *well-spread*.



Multiple bases to the rescue

<u>The (current) NLTS intuition:</u>
Show that every low-energy state's measurement in the Z-basis *or* in the X-basis is *well-spread*.

<u>Example</u>
If you measure the ground-state of the toric code in the Z-basis, you get one of 4 measurement classes corresponding to loops.

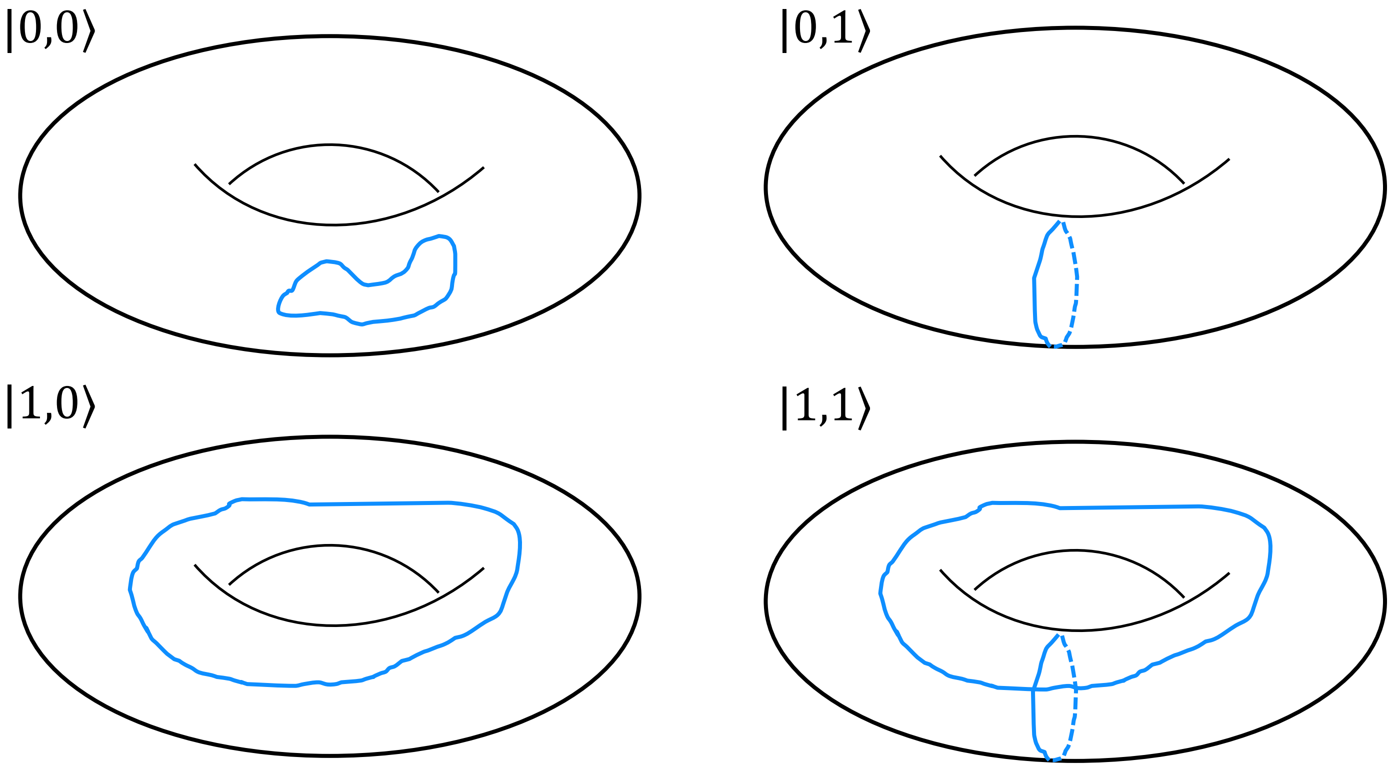


Multiple bases to the rescue

The (current) NLTS intuition:
Show that every low-energy state's measurement in the Z-basis *or* in the X-basis is *well-spread*.

Example
If you measure the ground-state of the toric code in the Z-basis, you get one of 4 measurement classes corresponding to loops.

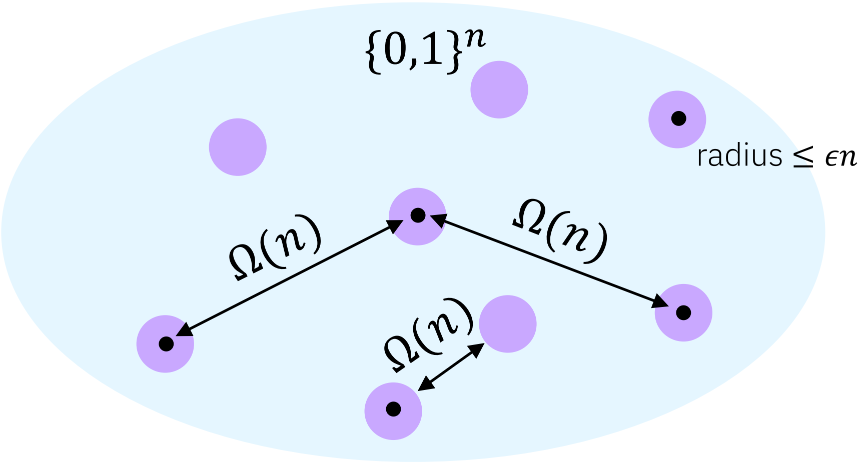
If the measurement is concentrated in the Z-basis, then it won't be concentrated in the X-basis.



Proving NLTS via “well-spreadness” and codes

<u>The (current) NLTS intuition:</u>
Show that every low-energy state’s measurement in the Z-basis *or* in the X-basis is *well-spread*.

<u>Good rate:</u>
- Degeneracy is necessary for proving well-spreadness
- How much degeneracy matters! A high-rate helps prove well-spreadness in some basis



<u>Good distance:</u>
- Distance is needed for proving robust well-spread lower bounds

<u>Good expansion</u>
- Needed for “shape” of low-energy distributions

What should we try to solve next?

Stronger state complexity bounds

Construct local Hams. with state complexity lower bounds for all low-energy states

- **NLSS** conjecture [G-LG[22],CCNN[23]]
- Trivially-rotated stabilizer states lower bounds

Reintroduce computational hardness

- Prove that **QPCP**s are **MA**-hard (or even just **BQP**-hard)
- Construct local Hams. which are simultaneous **NLTS** and **NP**-hard

What should we try to solve next?

Stronger state complexity bounds

Construct local Hams. with state complexity lower bounds for all low-energy states

- NLSS conjecture [G-LG[22],CCNN[23]]
- Trivially-rotated stabilizer states lower bounds

Reintroduce computational hardness

- Prove that QPCPs are MA-hard (or even just BQP-hard)
- Construct local Hams. which are simultaneous NLTS and NP-hard

Superpositions over NP solutions

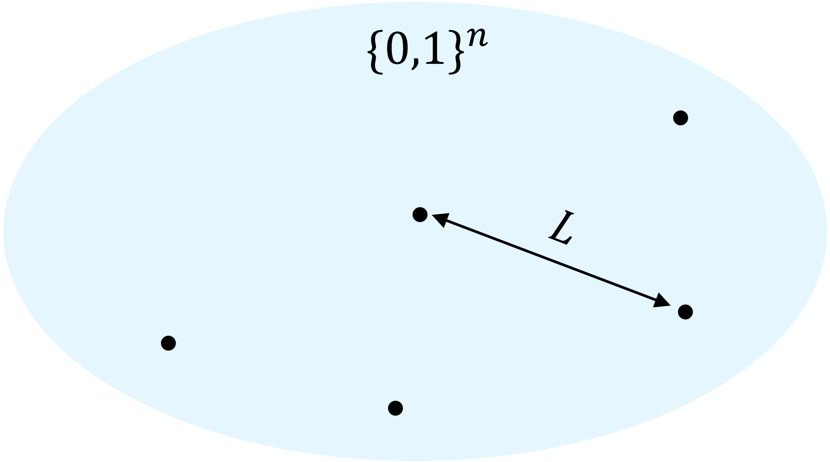
The [ABN[22]] NLTS construction is a stabilizer Hamiltonian and all stabilizer terms commute so, $\lambda_{\min}(\mathbf{H}_{ABN}) = \mathbf{0}$.

In general, any stabilizer Hamiltonian is easy to analyze.

<u>Simultaneously NP-hard and NLTS Hamiltonians:</u>
Can we construct a family of Hamiltonians such that

1. every $\leq \lambda_{\min}(\mathbf{H}) + \epsilon n$ –energy state cannot be generated by a low-depth circuit
2. It is NP-hard to decide if $\lambda_{\min}(\mathbf{H}) \leq an$ or $\geq bn$

Superpositions over NP solutions



<u>Simultaneously NP-hard and NLTS Hamiltonians:</u>
Can we construct a family of Hamiltonians such that

1. every $\leq \lambda_{\min}(\mathbf{H}) + \epsilon n$ –energy state cannot be generated by a low-depth circuit
2. It is NP-hard to decide if $\lambda_{\min}(\mathbf{H}) \leq an$ or $\geq bn$

<u>Idea 1:</u>
Let C be a YES-instance CSP. Find a Hamiltonian $\mathbf{H}_C$ with ground-state

$$|\psi\rangle \propto \sum_{C(x)=0} |x\rangle$$

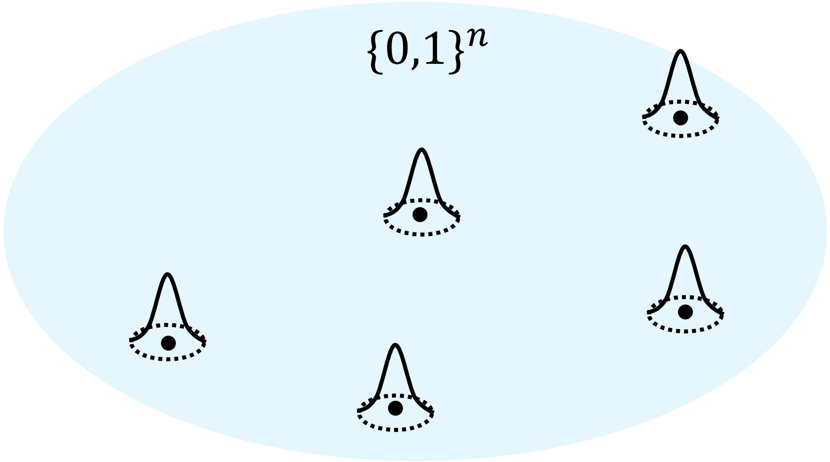
<u>Issue:</u>
Unless $\mathbf{H}_C$ is L-local, then every $|x\rangle$ is a ground-state for $C(x) = \mathbf{0}$.

Then $\mathbf{H}_C = C$. (And isn't NLTS).

Superpositions over NP solutions

<u>Simultaneously **NP**-hard and **NLTS** Hamiltonians:</u>
Can we construct a family of Hamiltonians such that

1. every $\leq \lambda_{\min}(\mathbf{H}) + \epsilon n$ –energy state cannot be generated by a low-depth circuit
2. It is **NP**-hard to decide if $\lambda_{\min}(\mathbf{H}) \leq an$ or $\geq bn$



<u>Idea 2 [AN[22],AGK[23]]:</u>
Let C be a YES-instance PCP-CSP. There exists a Hamiltonian $\mathbf{H}_C$ with ground-state

$$|\psi\rangle \propto \sum_{x \in \{0,1\}^n} \delta^{|C(x)|} |x\rangle$$

$$h_v = \left(\prod_{e:e\ni v} Q_e\right)^{-1} |+\rangle\langle+|_v \left(\prod_{e:e\ni v} Q_e\right)^{-1}$$

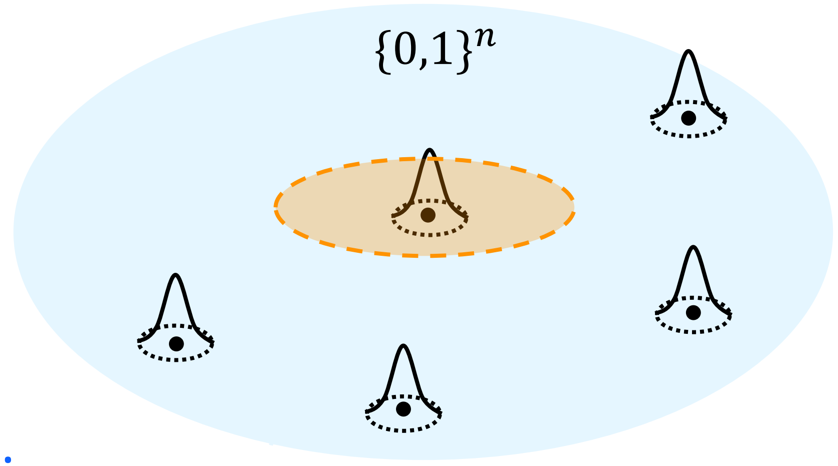
where the constraints are P_e and

$$Q_e = P_e + \delta \mathbb{I}$$

Superpositions over NP solutions

<u>Lemma (morally speaking) [AN22,AGK23]:</u>
The Hamiltonian $\mathbf{H}_C$ is combinatorial NLTS.

<u>Observation:</u> $\mathbf{H}_C$ is not NLTS necessarily.
Pf. When $C(x) = \mathbf{0}$ corresponds to a *collapsing* hash fn, there exists a non-well spread low-energy state.
Fundamental issue: $\mathbf{H}_C$ is defined too much in one basis.



Idea 2 [AN22,AGK23]:

<u>Collapsing hash fn:</u>

(roughly speaking), it is hard to distinguish $\sum_{x:h(x)=s} |x\rangle$ from $|x'\rangle$ for any $h(x') = s$.

e

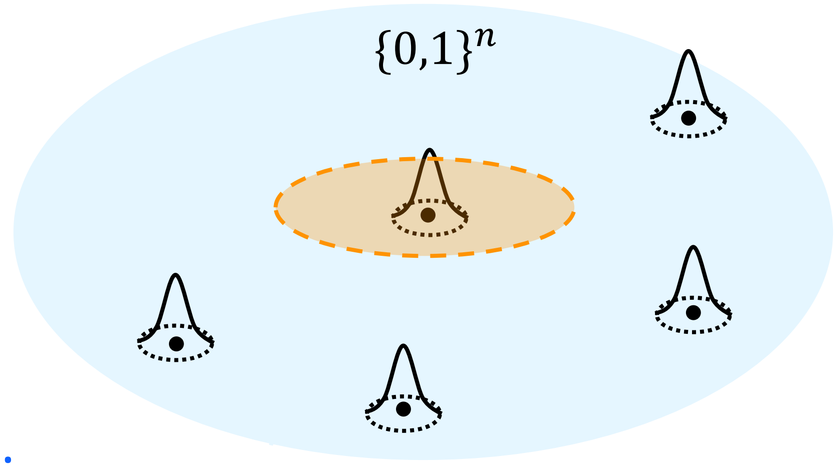
$$h_v = \left(\prod_{e:e\ni v} Q_e\right)^{-1} |+\rangle\langle+|_v \left(\prod_{e:e\ni v} Q_e\right)^{-1}$$

where the constraints are P_e and

$$Q_e = P_e + \delta\mathbb{I}$$

Superpositions over NP solutions

Lemma (morally speaking) [AN22,AGK23]:
The Hamiltonian $\mathbf{H}_C$ is combinatorial **NLTS**.



Observation: $\mathbf{H}_C$ is not **NLTS** necessarily.
Pf. When $C(x) = 0$ corresponds to a *collapsing* hash fn, there exists a non-well spread low-energy state.
Fundamental issue: $\mathbf{H}_C$ is defined too much in one basis.

Idea 2 [AN22,AGK23]:
Let C be a YES-instance PCP-CSP. There exists a Hamiltonian $\mathbf{H}_C$ with ground-state

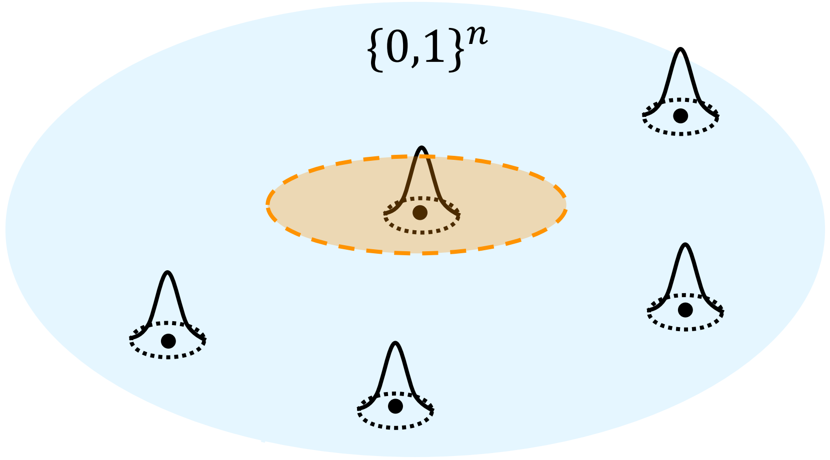
$$|\psi\rangle \propto \sum_{x\in\{0,1\}^n} \delta^{|C(x)|} |x\rangle$$

$$h_v = \left(\prod_{e:e\ni v} Q_e\right)^{-1} |+\rangle\langle+|_v \left(\prod_{e:e\ni v} Q_e\right)^{-1}$$

where the constraints are P_e and

$$Q_e = P_e + \delta\mathbb{I}$$

A surprising connection to quantum money/lightning



Quantum Money Proposal [Zhandry17]:
For a hash function h, the money state is

$$|\$_s\rangle \propto \sum_{y:h(y)=s} |y\rangle$$

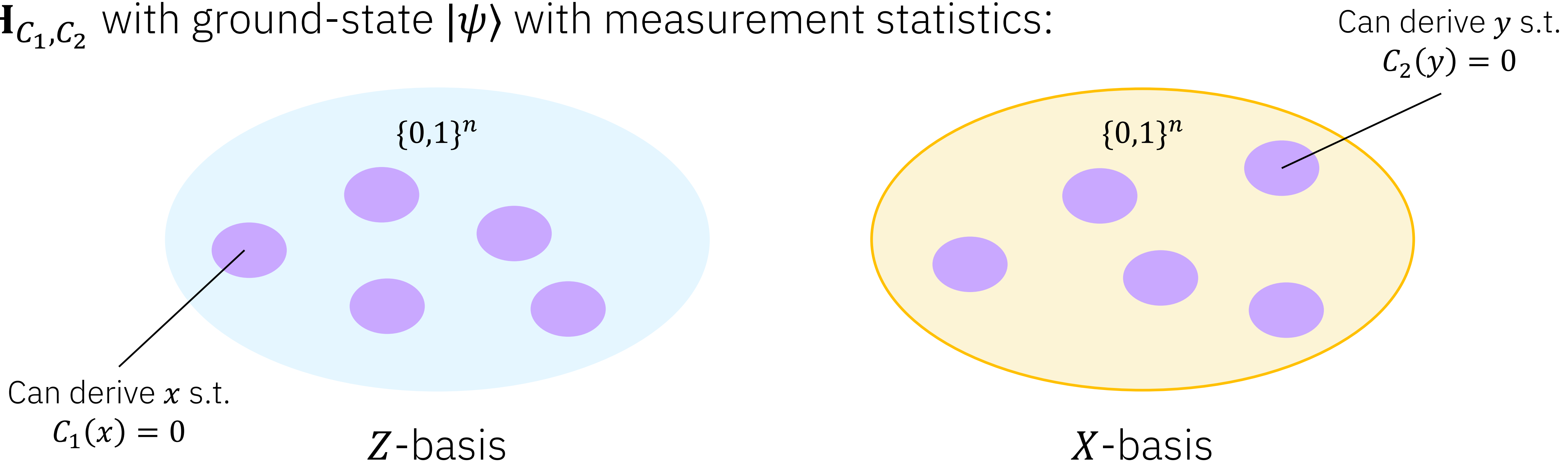
Thm [Zhandry17]: If h is collision-resistant and non-collapsing, then this is a quantum lightning scheme.

Issue:
If solutions of $h^{-1}(s)$ are $\leq L$ close to each other, then there is a brute-force n^L-time algorithm for breaking collision-resistance.

Else, h is collapsing by any algorithm that looks like Hamiltonian energy estimation.

An intermediate problem for both q. lightning and QPCP

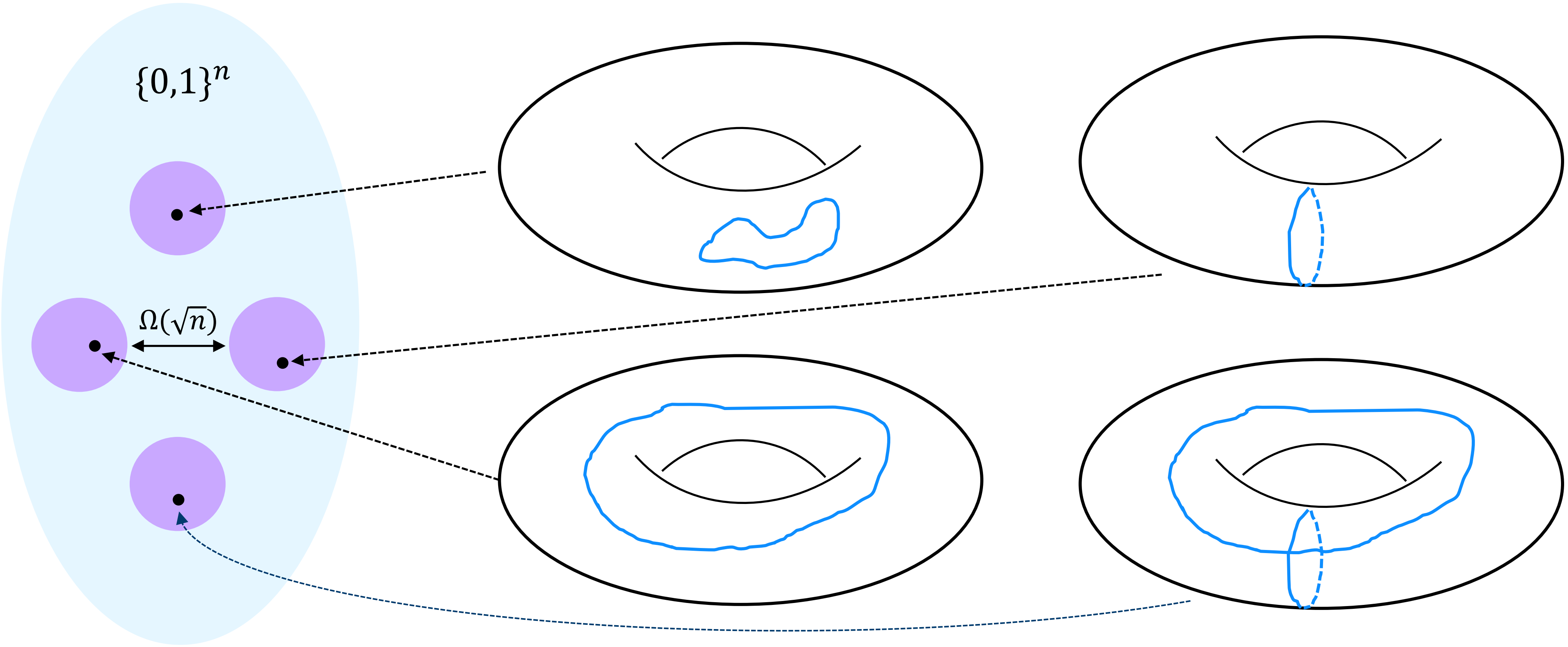
For an **NP** problems given by a CSP C_1, C_2, construct a Hamiltonian $\mathbf{H}_{C_1,C_2}$ with ground-state $|\psi\rangle$ with measurement statistics:



<u>Key desired property:</u> Measuring a ground-state of $\mathbf{H}_{C_1,C_2}$ will give us some entropy over solutions to *either* C_1 or C_2.

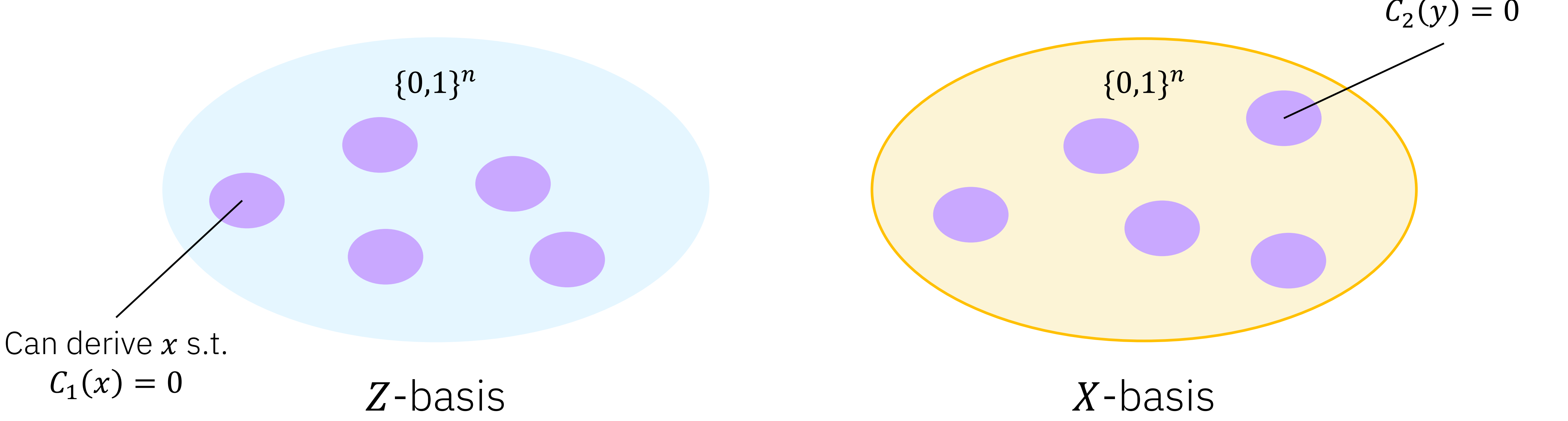
Multiple bases to the rescue

The (current) NLTS intuition:
Show that every low-energy state's measurement in the Z-basis *or* in the X-basis is *well-spread*.



An intermediate problem for both q. lightning and QPCP

For an **NP** problems given by a CSP C_1, C_2, construct a Hamiltonian $\mathbf{H}_{C_1,C_2}$ with ground-state $|\psi\rangle$ with measurement statistics:



Key desired property: Measuring a ground-state of $\mathbf{H}_{C_1,C_2}$ will give us some entropy over solutions to *either* C_1 or C_2.

An intermediate problem for both q. lightning and QPCP

For an **NP** problems given by a CSP C_1, C_2, construct a Hamiltonian $\mathbf{H}_{C_1,C_2}$ with ground-state $|\psi\rangle$ with measurement statistics:

<u>Key desired property:</u> Measuring a ground-state of $\mathbf{H}_{C_1,C_2}$ will give us some entropy over solutions to *either* C_1 or C_2.

What should we try to solve next?

<u>Stronger state complexity bounds</u>

Construct local Hams. with state complexity lower bounds for all low-energy states

- **NLSS** conjecture [G-LG[22],CCNN[23]]
- Trivially-rotated stabilizer states lower bounds

<u>Reintroduce computational hardness</u>

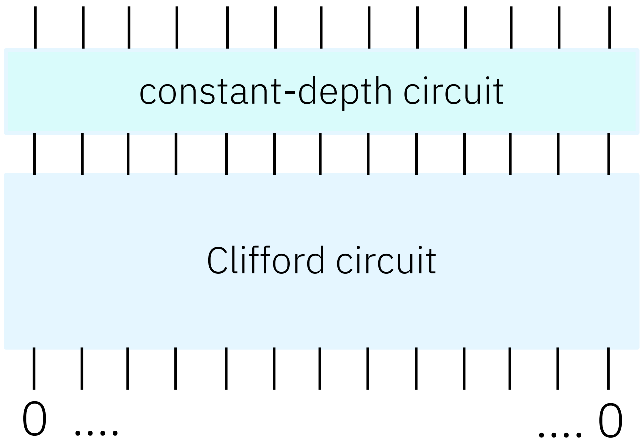
- Prove that **QPCPs** are **MA**-hard (or even just **BQP**-hard)
- Construct local Hams. which are simultaneous **NLTS** and **NP**-hard

Proving stronger lower bounds than **NLTS**

Constant-depth quantum circuits are just one of *many* classical witness that can be provided for an **NP** proof.

QPCP Conj. + NP≠QMA $\Longrightarrow$
lower-bounds for all families of **NP** witnesses

Open question: Can we prove lower-bounds for some other families of **NP** witnesses? Is there is a family of local Hamiltonians for which all known **NP** witnesses are insufficient?



Any state of this form is also a **NP** witness. These are called “trivially-rotated stabilizer states”.

NLTS+ conjecture: There exists local Hamiltonian such that all such states have energy $\geq \epsilon n$.

Our proof of **NLTS** does not satisfy this!

What should we try to solve next?

<u>Stronger state complexity bounds</u>

Construct local Hams. with state complexity lower bounds for all low-energy states

- NLSS conjecture [G-LG[22],CCNN[23]]
- Trivially-rotated stabilizer states lower bounds

<u>Reintroduce computational hardness</u>

- Prove that **QPCP**s are **MA**-hard (or even just **BQP**-hard)
- Construct local Hams. which are simultaneous **NLTS** and **NP**-hard

special class of **stateMA** lower bounds

What should we try to solve next?

Stronger state complexity bounds

Construct local Hams. with state complexity lower bounds for all low-energy states

- NLSS conjecture [G-LG[22],CCNN[23]]
- Trivially-rotated stabilizer states lower bounds

Reintroduce computational hardness

- Prove that **QPCPs** are **MA**-hard (or even just **BQP**-hard)
- Construct local Hams. which are simultaneous **NLTS** and **NP**-hard

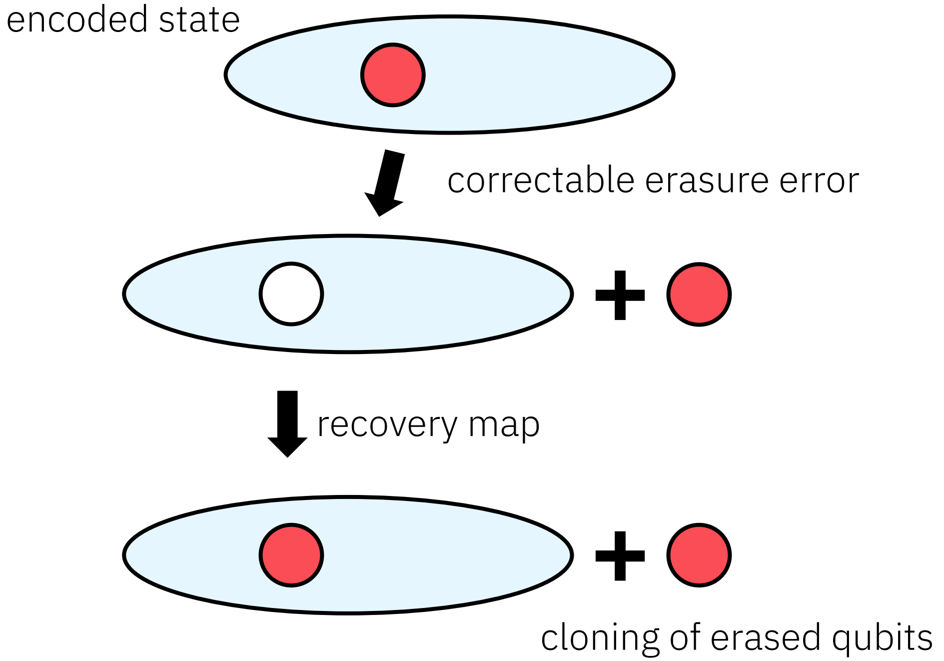
special class of **stateMA** lower bounds

The trouble with quantum codes

<u>Thm (folklore)</u>
The $< d$-sized reduced density matrices of code-states are an invariant of the encoded state.

No Cloning Theorem **+** Quantum Error-Correction **⇒** Local Indistinguishability

$$|\Psi\rangle|0\rangle \not\mapsto |\Psi\rangle|\Psi\rangle$$



Resolution: qubits are completely determined by the error-correcting code

qubit state does not depend on which state is encoded

The trouble with quantum codes

At the highest level of generality, one could summarize the classical PCP theorem as an elegant locally testable code wrapped around the satisfying assignment for the formula.

Could we do the same for quantum PCPs?

Thm (folklore)
The $< d$-sized reduced density matrices of code-states are an invariant of the encoded state.

If we use a q. code with dist. d, then the local Ham. must have locality $\ell > d$ due to *local indistinguishability*.

IBM