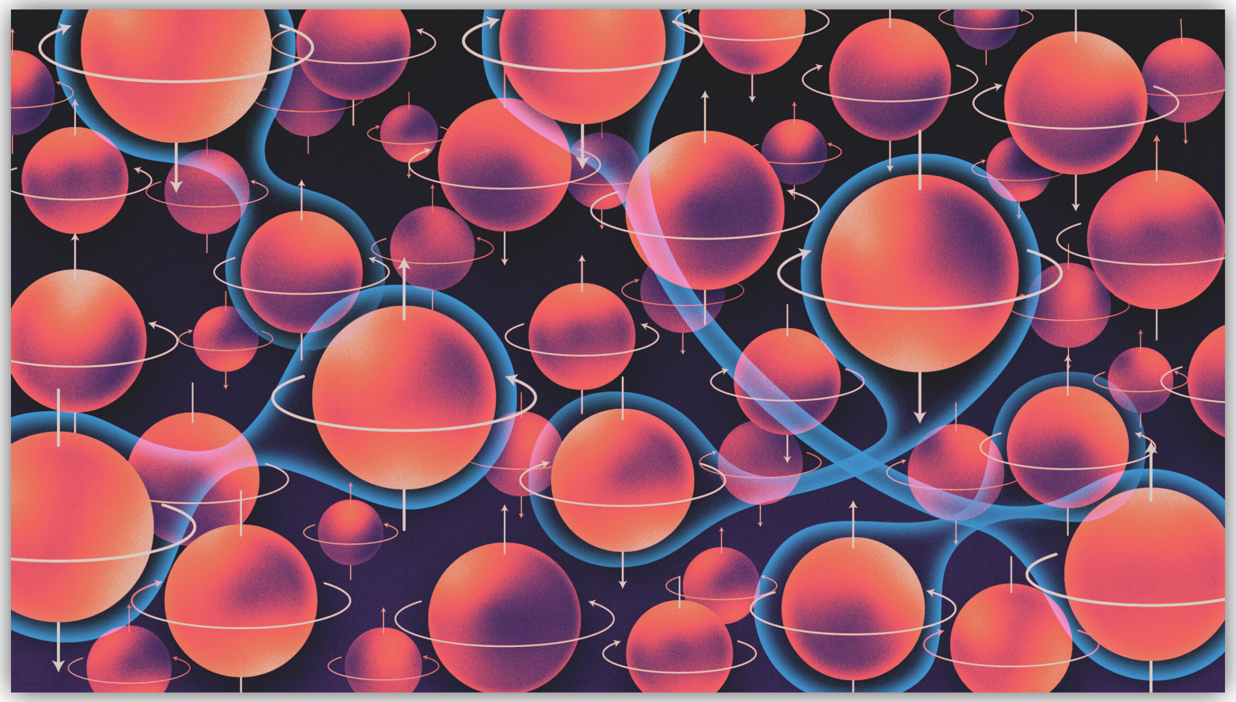
Why can't we classically describe quantum systems?

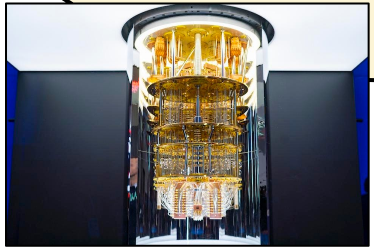


Kristina Armitage for *Quanta Magazine*

Chinmay Nirkhe
Research Staff Scientist, IBM Quantum

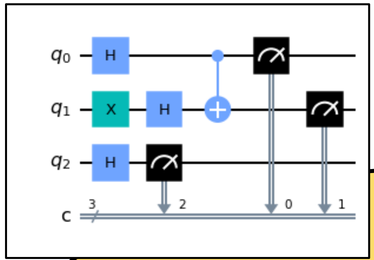
IBM

quantum computation



Local Hamiltonian systems

classically descriptions of quantum states

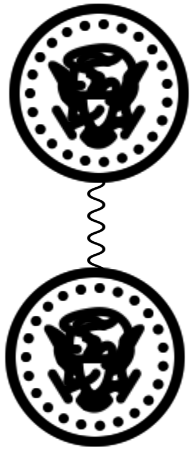


circuit lower bounds

entanglement at warm temperatures

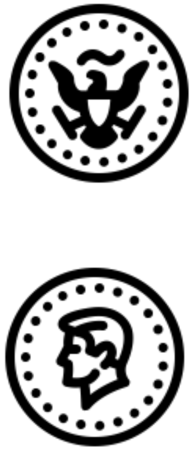
Quantum states are exponentially complex

a quantum system



$$\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$$

a classical system



$$|0\rangle|1\rangle$$

quantum entanglement

doesn't suffice to describe each individual particle

Quantum states are exponentially complex

n particles 

$$\text{quantum state} = \sum_x \alpha_x |x\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \vdots \\ \vdots \\ \alpha_{111} \end{pmatrix} \updownarrow 2^n$$

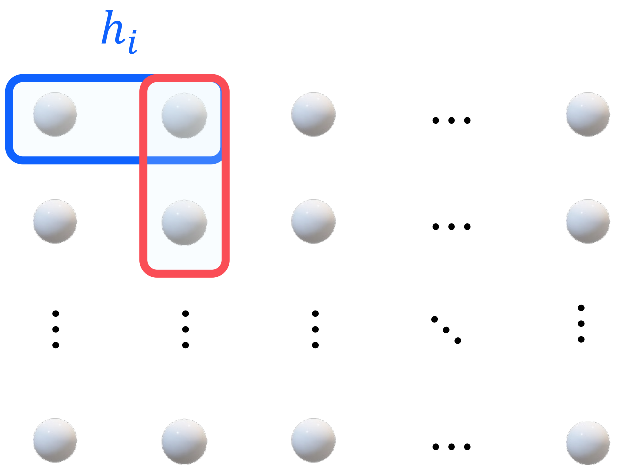
sum over all n-bit strings

Space of n particle states = $\mathbb{C}^{2^n}$

physically relevant corner

How is it possible to represent quantum states without exponential complexity?

The physically relevant corner

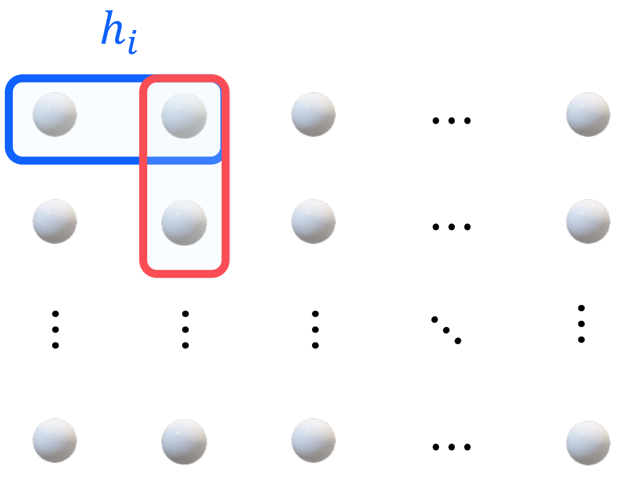


defined by local interactions

each k-local interaction is described by

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

The physically relevant corner



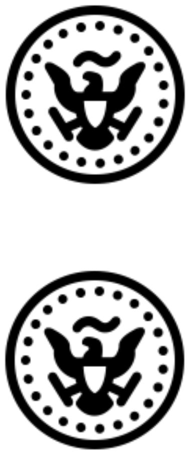
defined by local interactions

each k-local interaction is described by

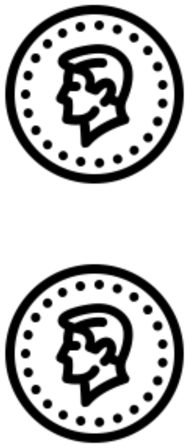
Hamiltonian $h_i = \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}$ (size $2^k \times 2^k$)

---

example: h_i prefers

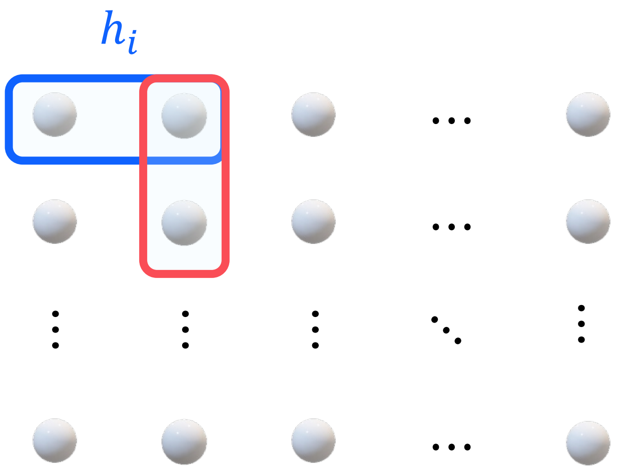


OR



$$h_i = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 1 & \\ & & & 0 \end{pmatrix}$$

The physically relevant corner



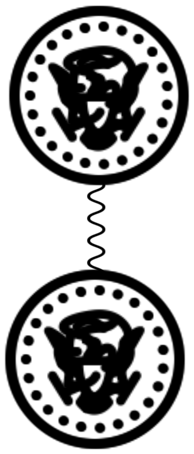
defined by local interactions

each k-local interaction is described by

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

---

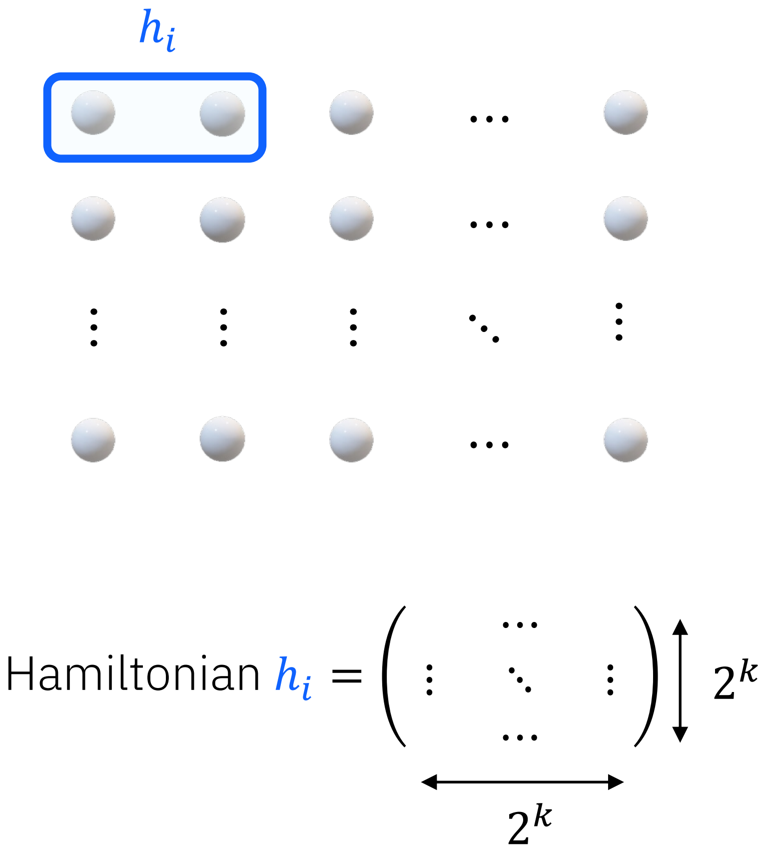
example: h_i prefers

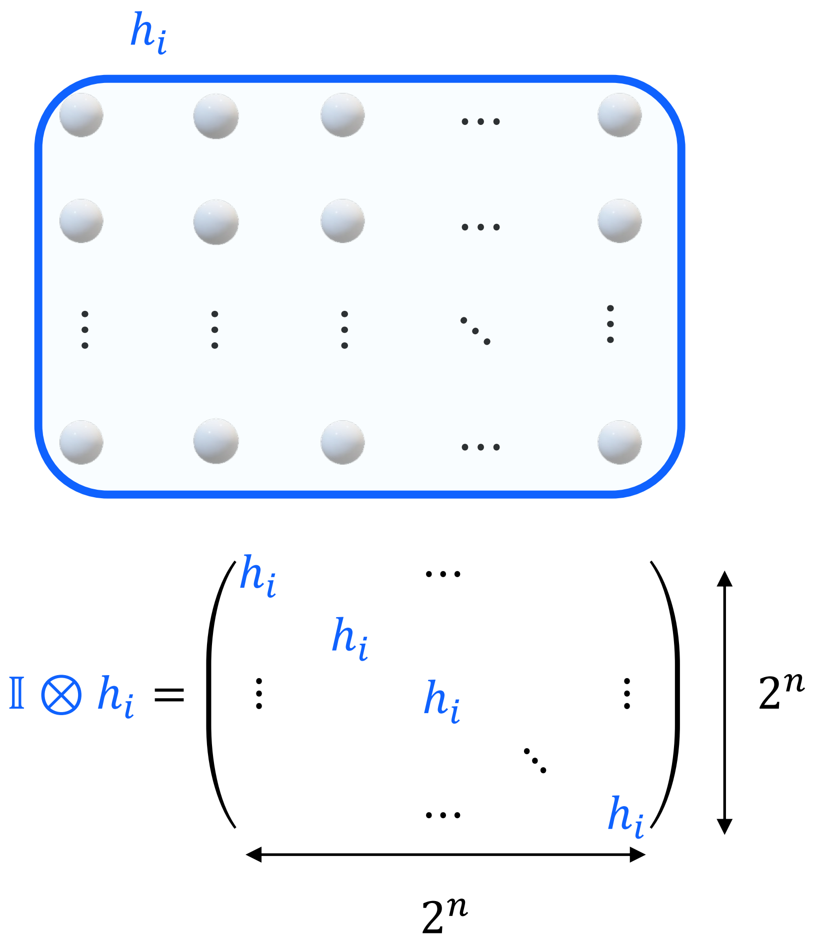


$$h_i = \frac{1}{2}\begin{pmatrix} -1 & & & -1 \\ & 2 & & \\ & & 2 & \\ -1 & & & -1 \end{pmatrix}$$

A global view on the interactions

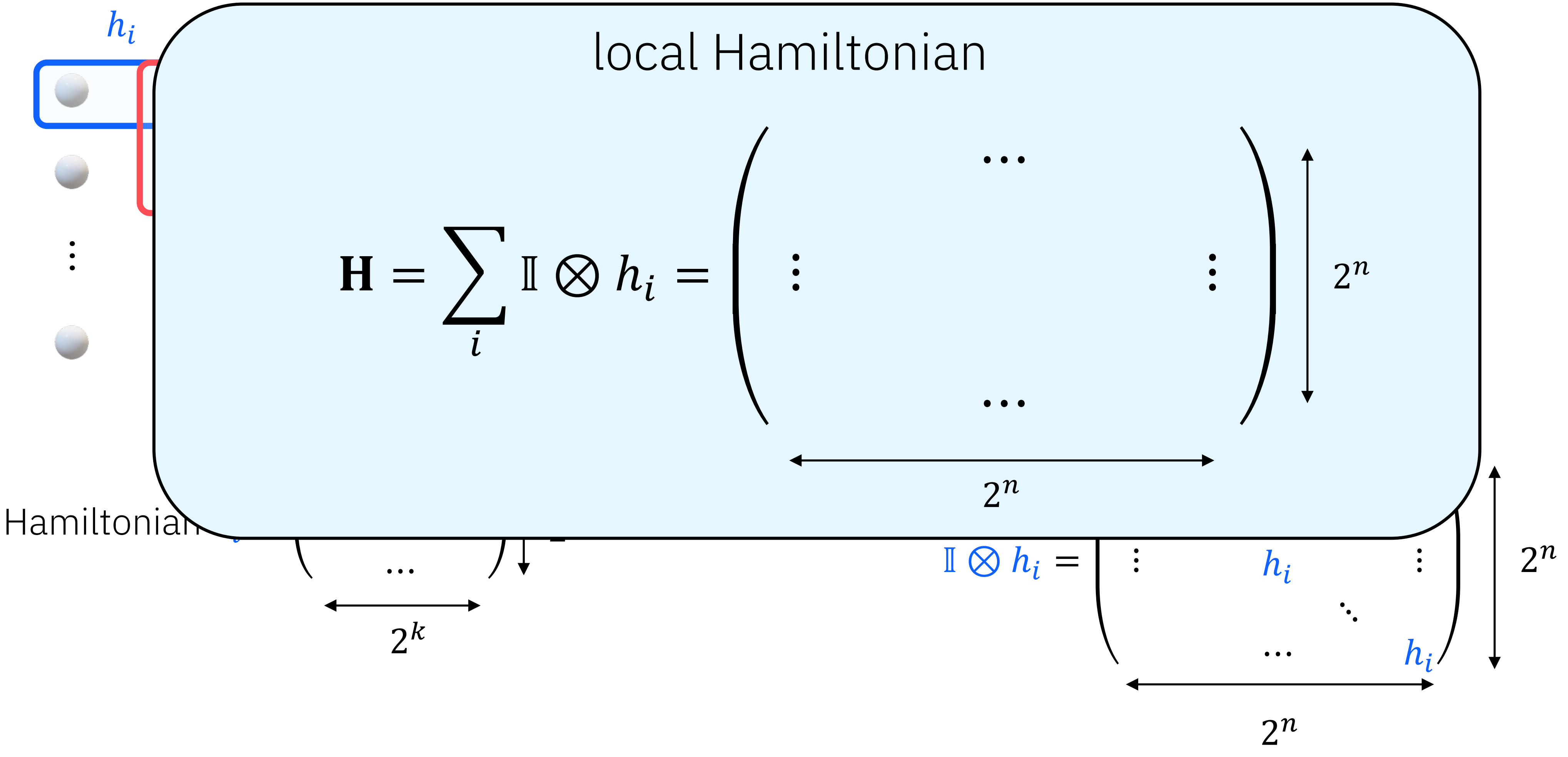
local Hamiltonian term





A global view on the interactions

local Hamiltonian term

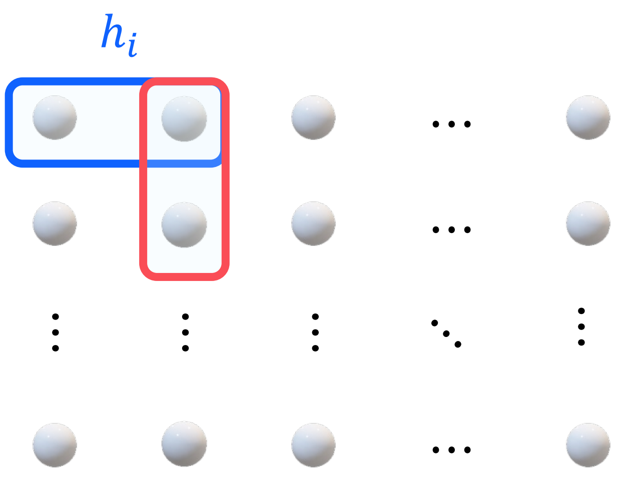


local Hamiltonian

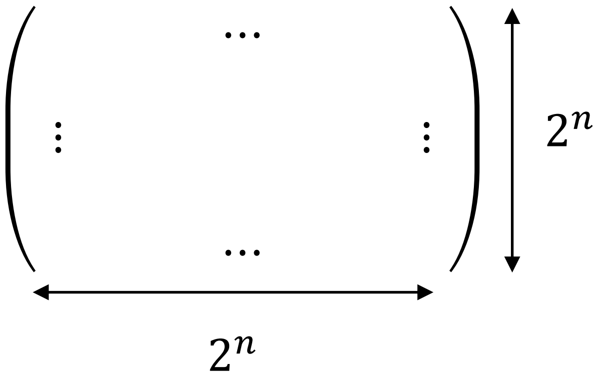
$$\mathbf{H} = \sum_i \mathbb{I} \otimes h_i = \begin{pmatrix} & \cdots & \\ \vdots & & \vdots \\ & \cdots & \end{pmatrix}$$

A short description of the interactions

local Hamiltonian



$$\mathbf{H} = \sum_i \mathbb{I} \otimes h_i =$$



$\mathbf{H}$ has a short ($\mathbf{poly}(n)$) length description

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

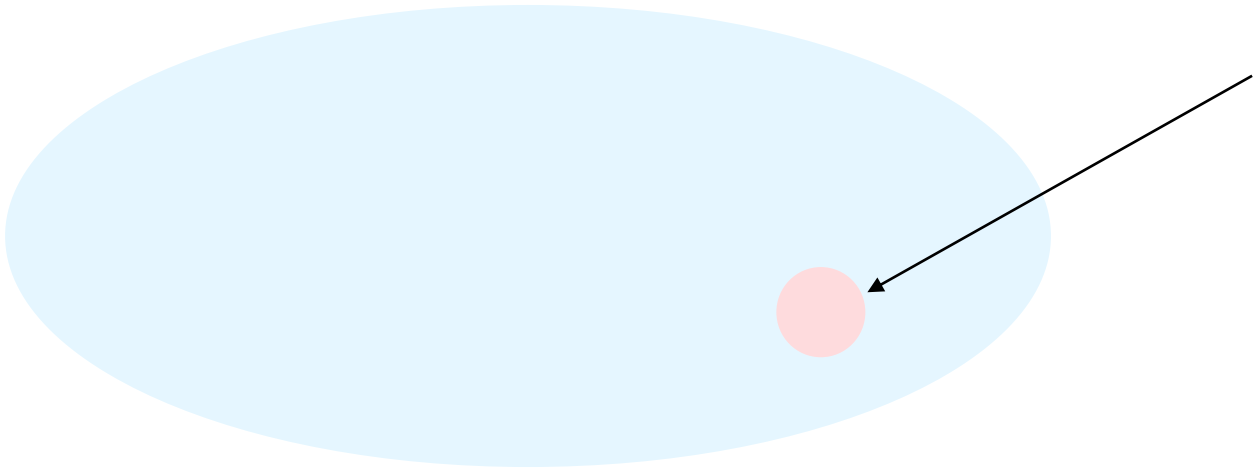
energy of a state $|v\rangle$:= eigenvalue of $|v\rangle$

low-energy means small-eigenvalue

calculating the low-energy states of $\mathbf{H}$ involves piecing together the solutions of each of the local terms $\{h_i\}$

Describing low-energy states

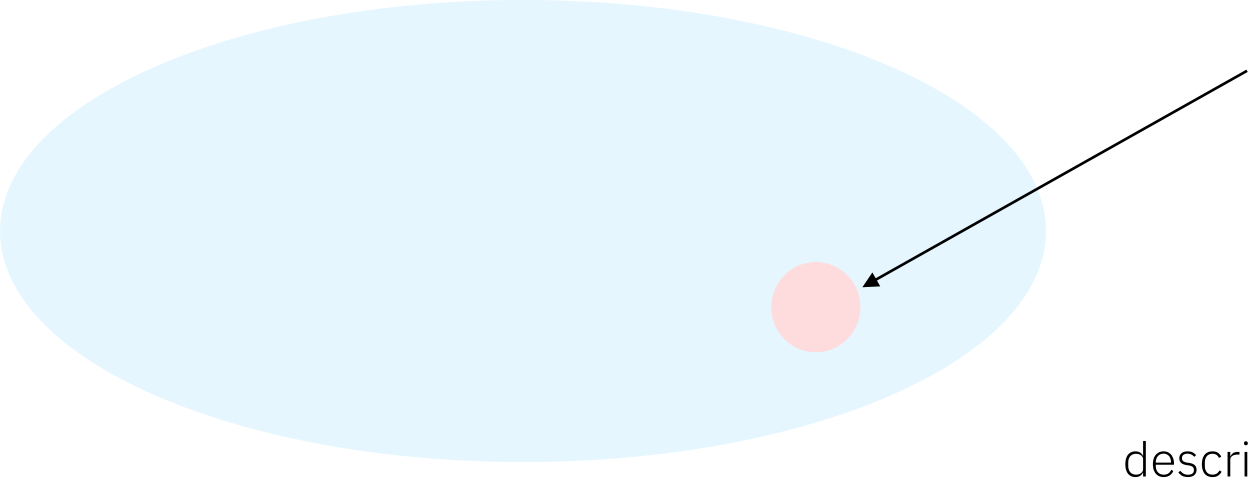
Space of n particle states = $\mathbb{C}^{2^n}$



physically relevant corner

Describing low-energy states

Space of n particle states = $\mathbb{C}^{2^n}$



low-energy states of local Hamiltonians

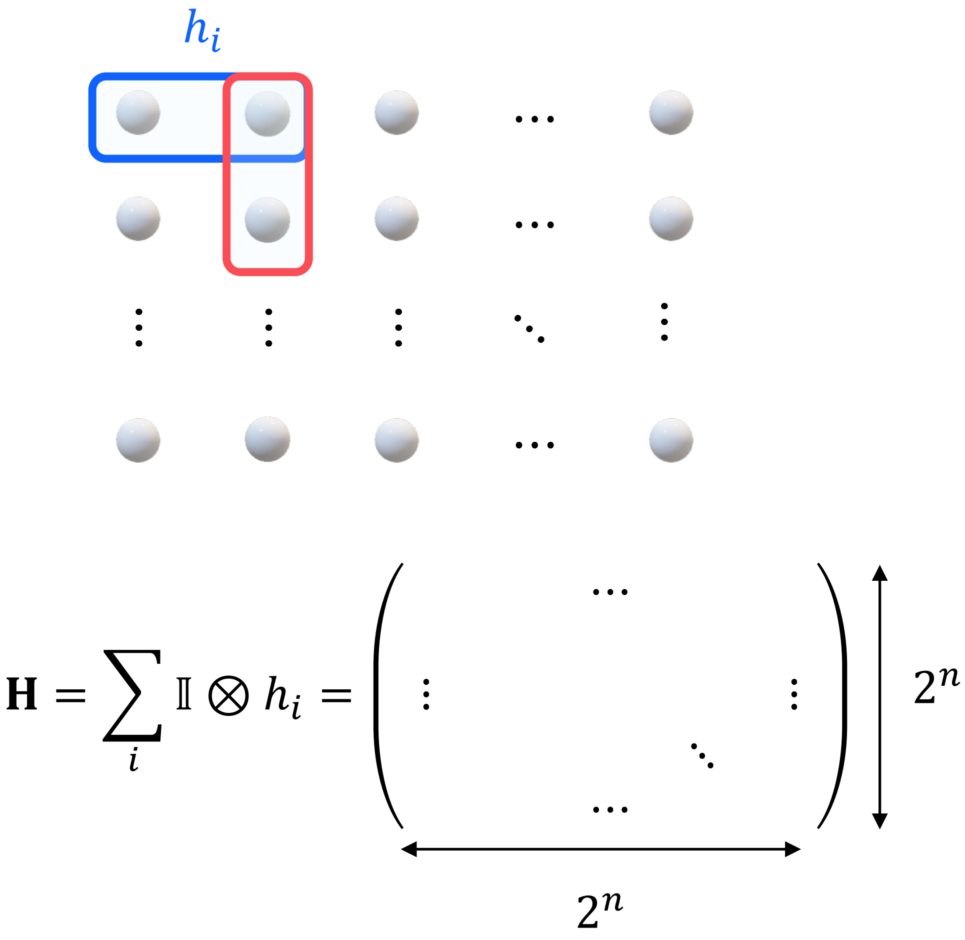
describes the states at constant temperature

What does "low" mean?

ground-state = eigenvector of minimal e-value	up to energy $\leq \epsilon n$ any vector $\lvert v\rangle$ such that $\langle v\rvert \mathbf{H} \lvert v\rangle \leq \epsilon n$

Describing low-energy states

local Hamiltonian



$\mathbf{H}$ has a short ($\mathbf{poly}(n)$) length description

Are there short descriptions for the ground-states of $\mathbf{H}$?

[Kitaev'99]: It is **QMA**-hard (Quantum **NP**) to describe the ground-states

What about the low-energy states? Could any of them be easy to describe?

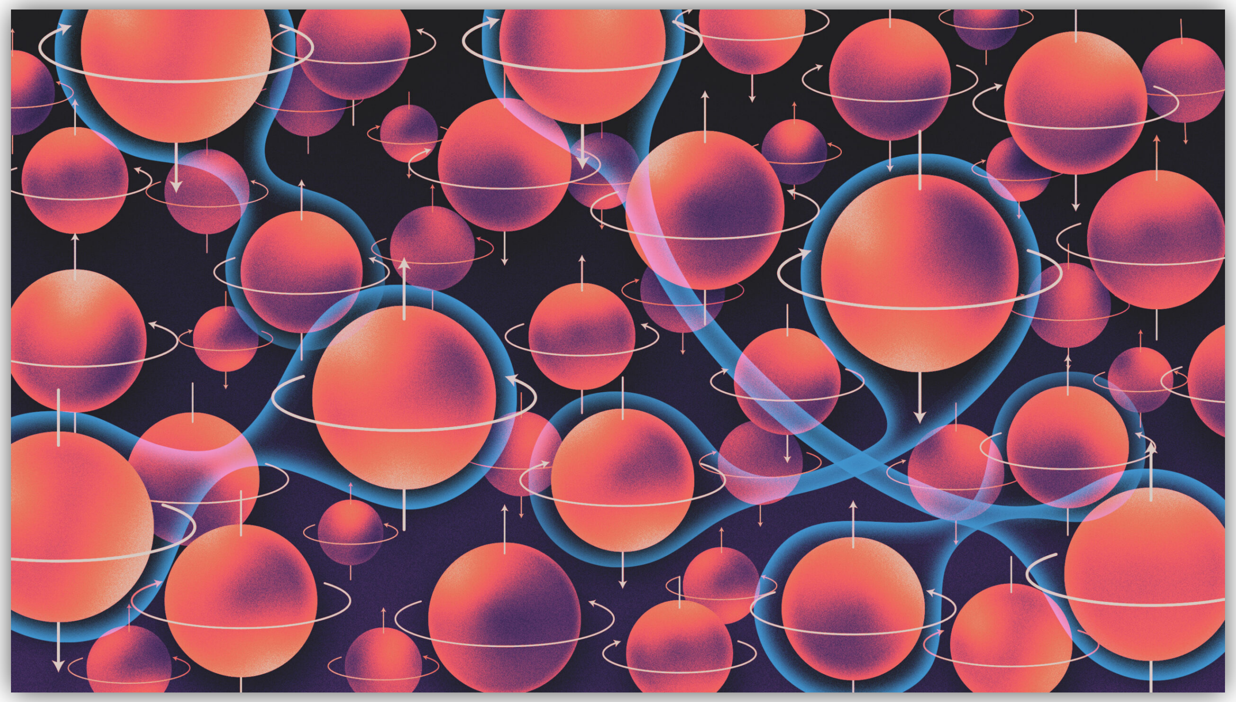
Today's talk: when low-energy states are hard to describe

Outline for the remainder of the talk

- NLTS and QPCP conjectures (description lower bounds)
- Stronger lower bounds in distribution-testing
- Defining state complexity
- Ideas for future research and open problems

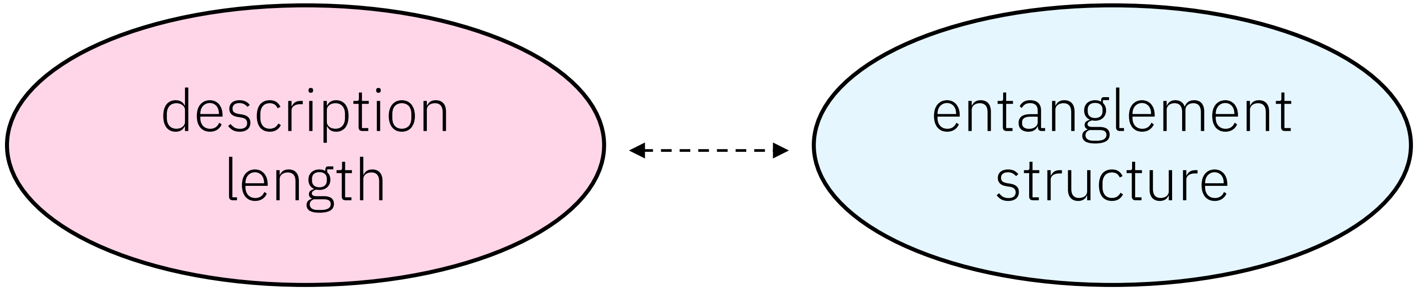
Part 1: The NLTS conjecture

lower bounds on the description complexity of quantum states



Kristina Armitage for *Quanta Magazine*

The relationship between description complexity and entanglement



quantum entanglement
doesn't suffice to describe each individual particle

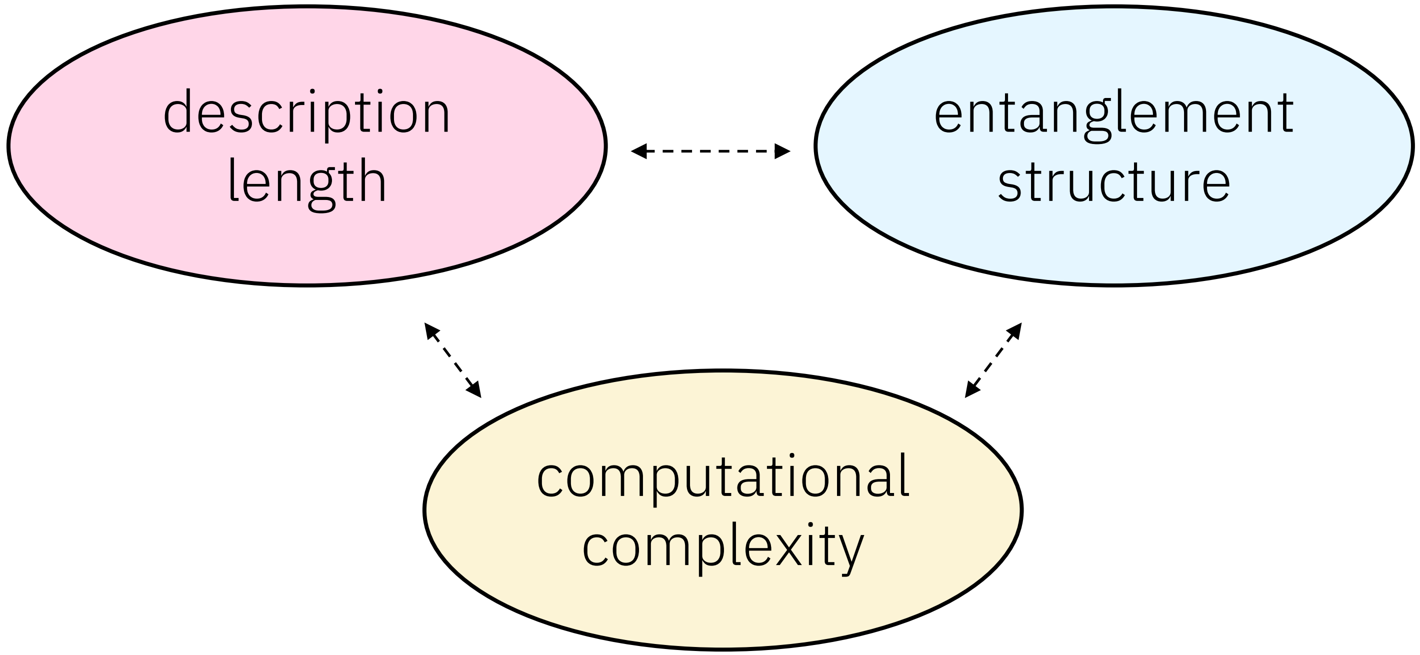
the longer the description ⇛ the more "complex" the entanglement

description length is a "measure" of entanglement complexity

today's central question

Are there local Hamiltonians with no short description low-energy states?

The relationship between description complexity and entanglement

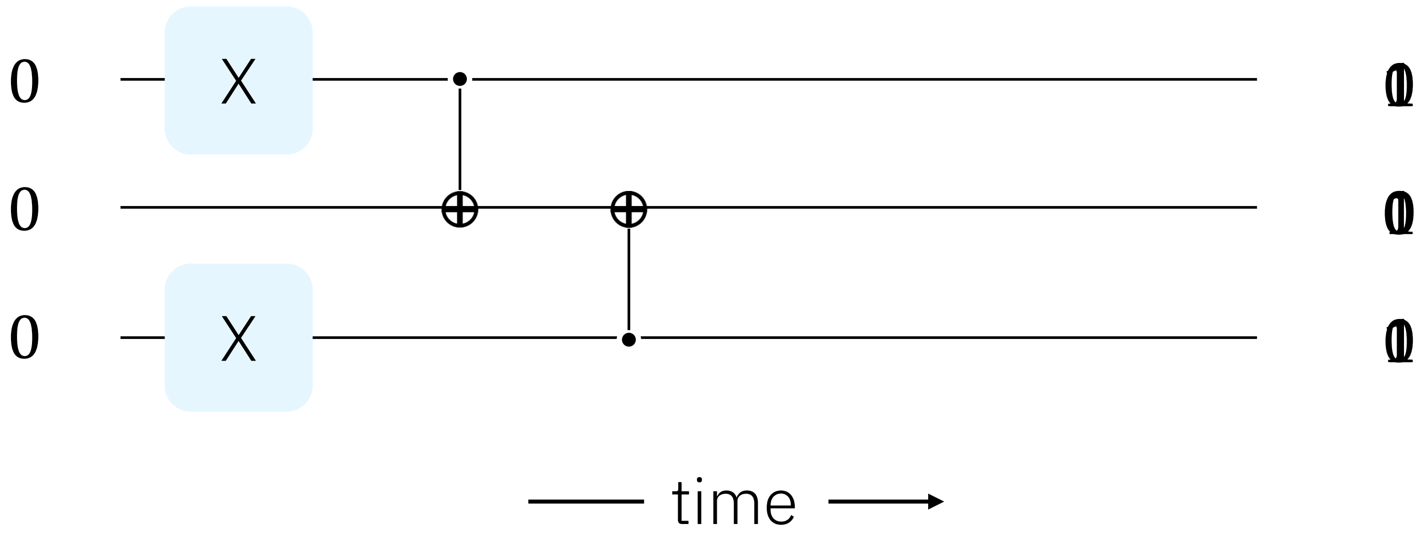


today's central question

Are there local Hamiltonians with no short description low-energy states?

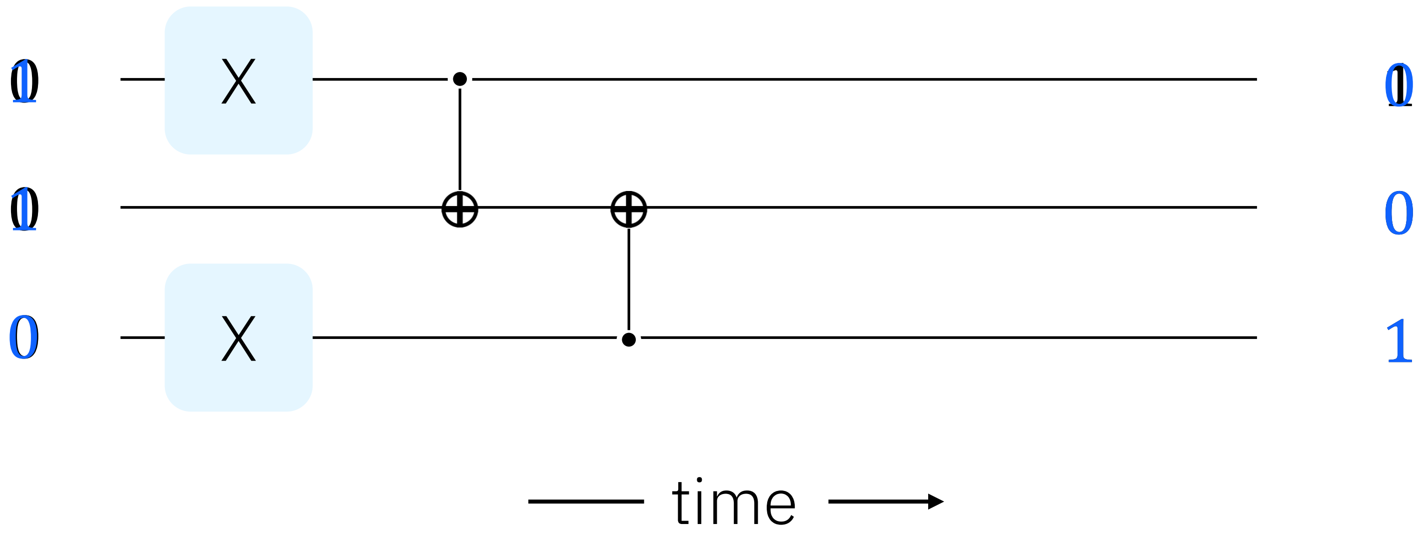
The circuit model

computation can be described in the *circuit* model



The circuit model

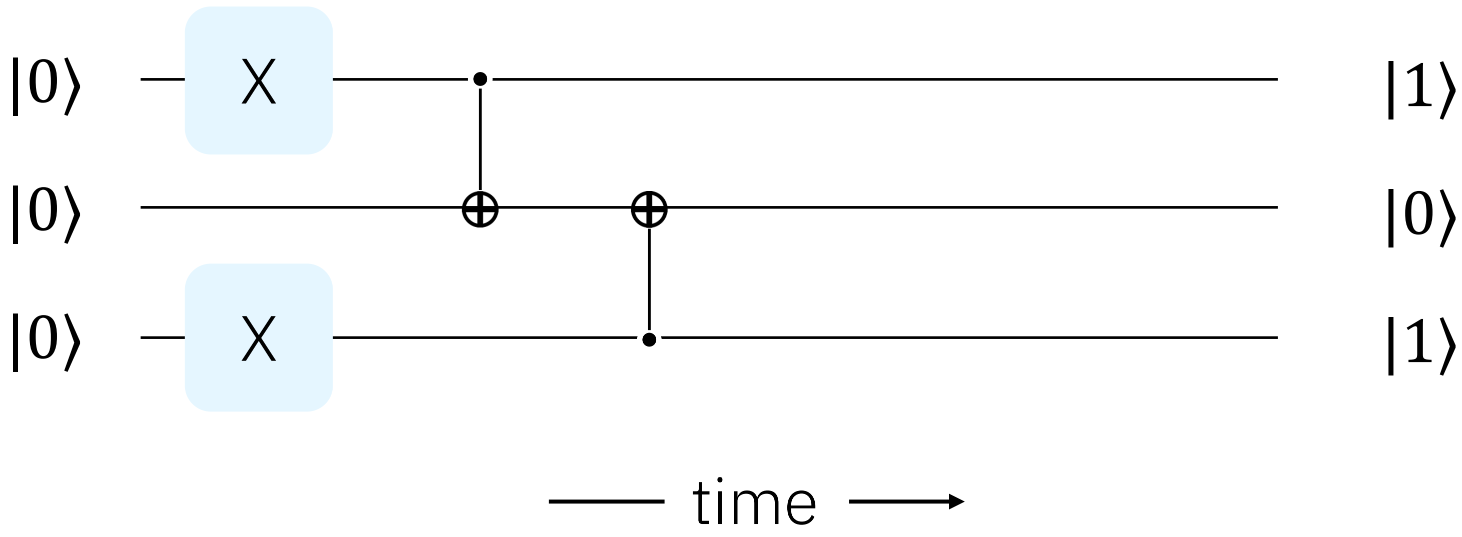
computation can be described in the *circuit* model



computation can be viewed as an input/output function

The circuit model

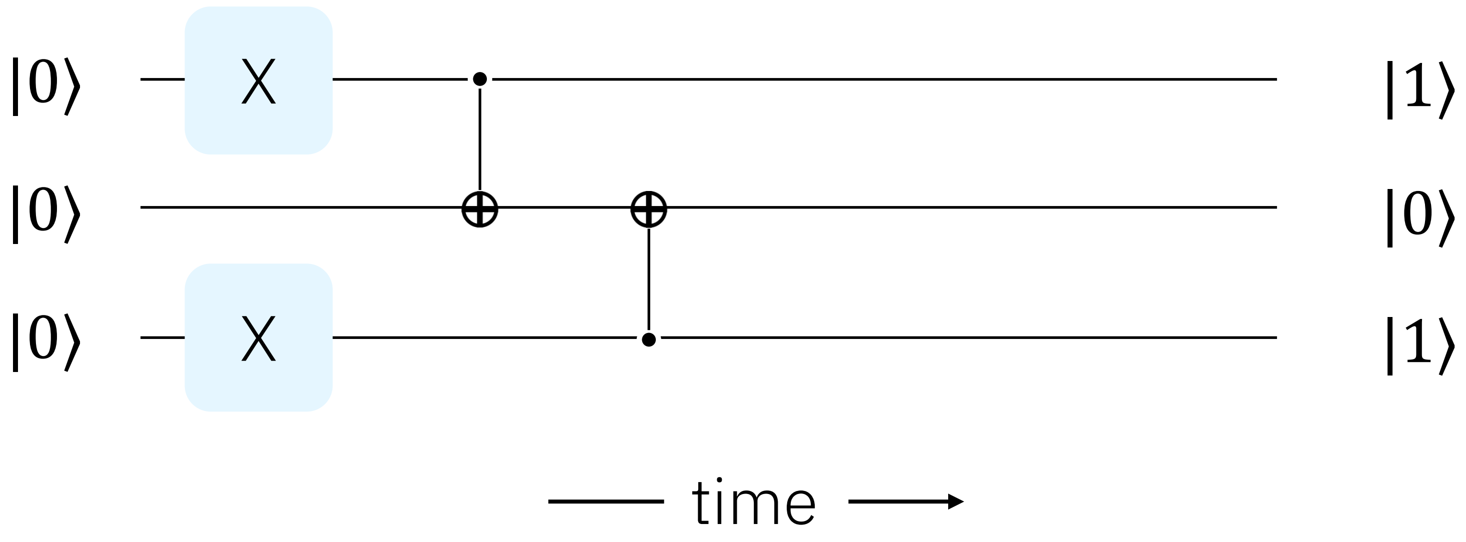
likewise, quantum computation can be described in the *circuit* model



The circuit model

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

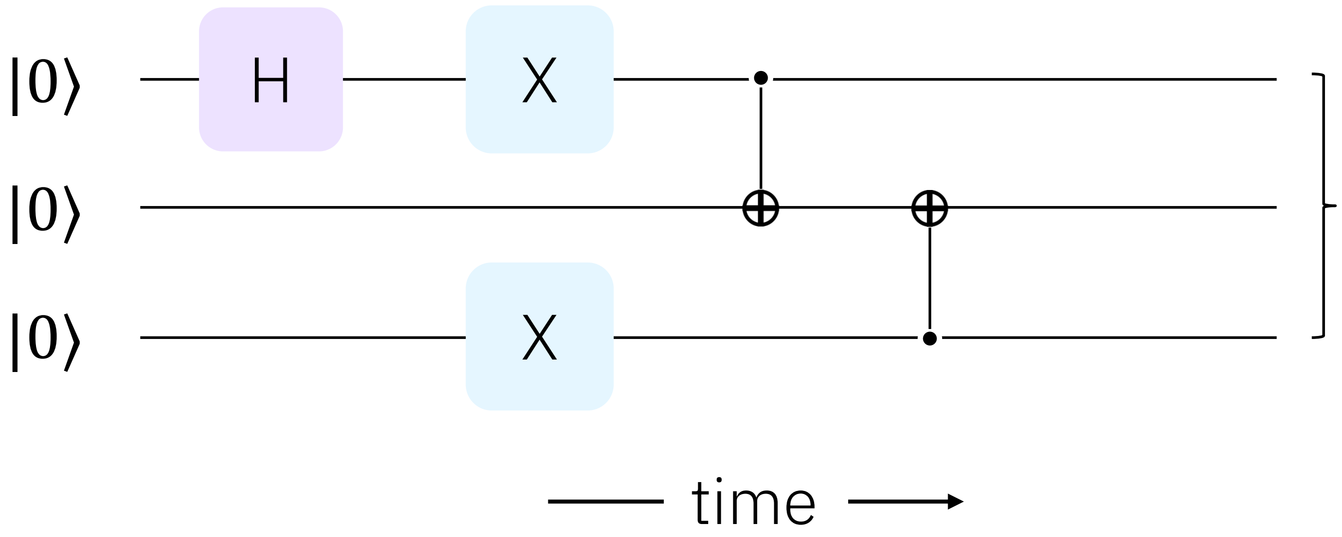
likewise, quantum computation can be described in the *circuit* model



The circuit model

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

likewise, quantum computation can be described in the *circuit* model

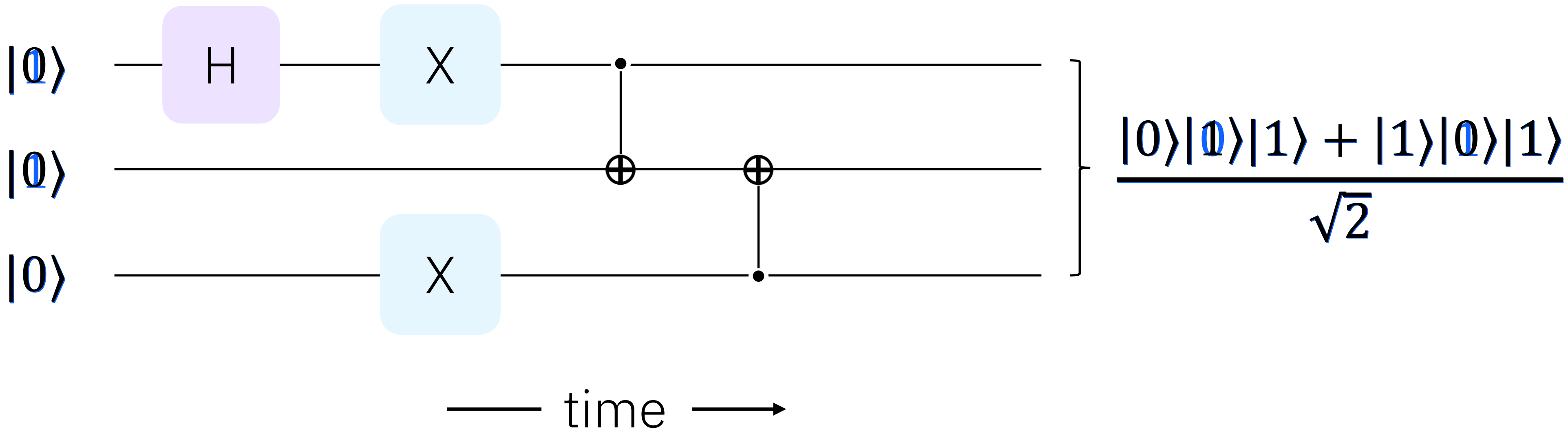


$$\frac{|0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle}{\sqrt{2}}$$

The circuit model

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

likewise, quantum computation can be described in the *circuit* model

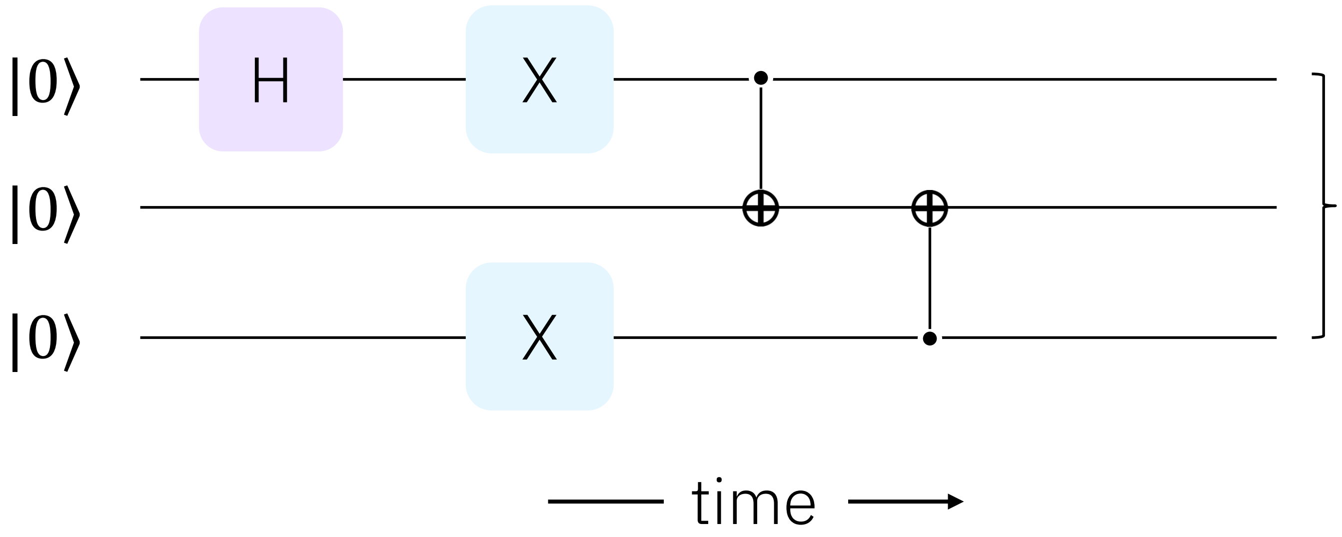


quantum computation also can be viewed as an input/output function

The circuit model

$$\boxed{H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}$$

likewise, quantum computation can be described in the *circuit* model



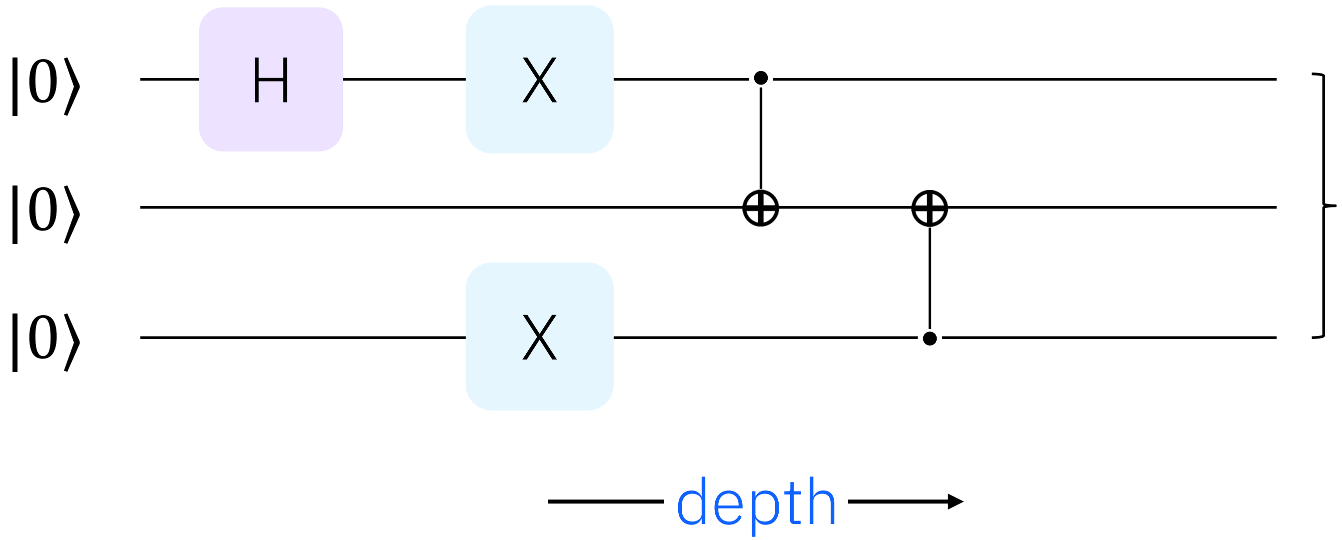
$$\frac{|0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle}{\sqrt{2}}$$

quantum computation also gives us a measure of complexity for states!

Circuit depth as a measure of complexity

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

likewise, quantum computation can be described in the *circuit* model



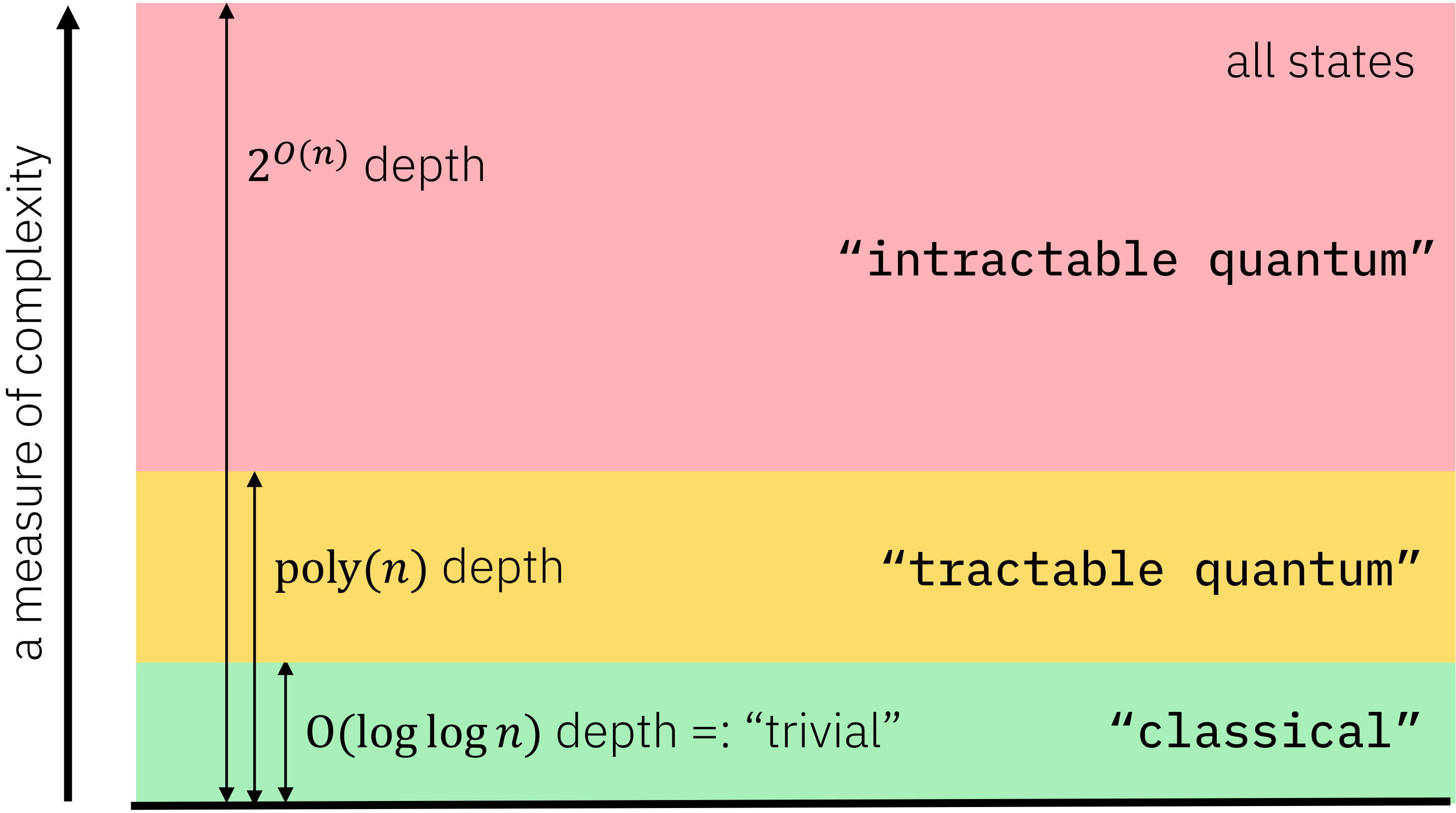
$$\frac{|0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle}{\sqrt{2}}$$

quantum computation also gives us a measure of complexity for states!

definition: $\mathbf{depth}(|v\rangle) =$ minimum depth over all circuits outputting $|v\rangle$ from $|00 \ldots 0\rangle$

The (quantum) computational yardstick

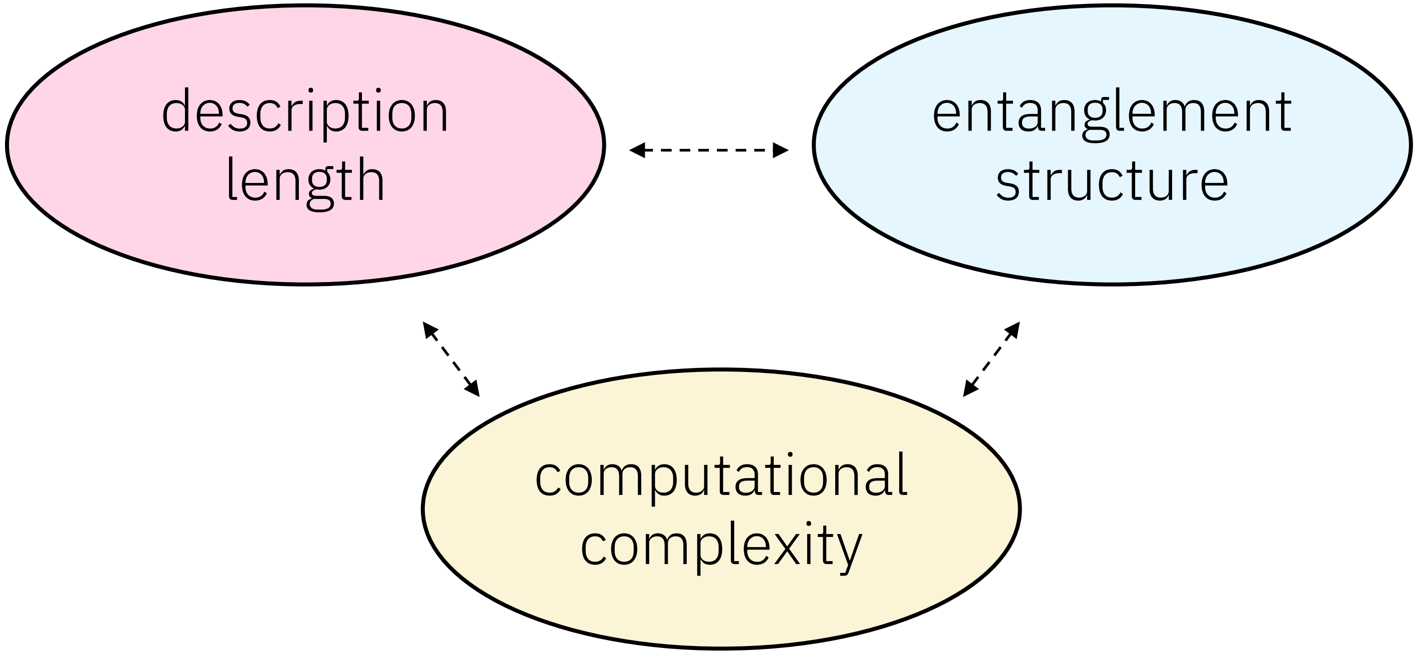
$\mathbf{depth}(|v\rangle)$ = minimum depth of circuit with output $|v\rangle$



efficient quantum algorithm for calculating the energy of $|v\rangle$ for any LH $\mathbf{H}$

efficient classical algorithm for calculating the energy of $|v\rangle$ for any LH $\mathbf{H}$

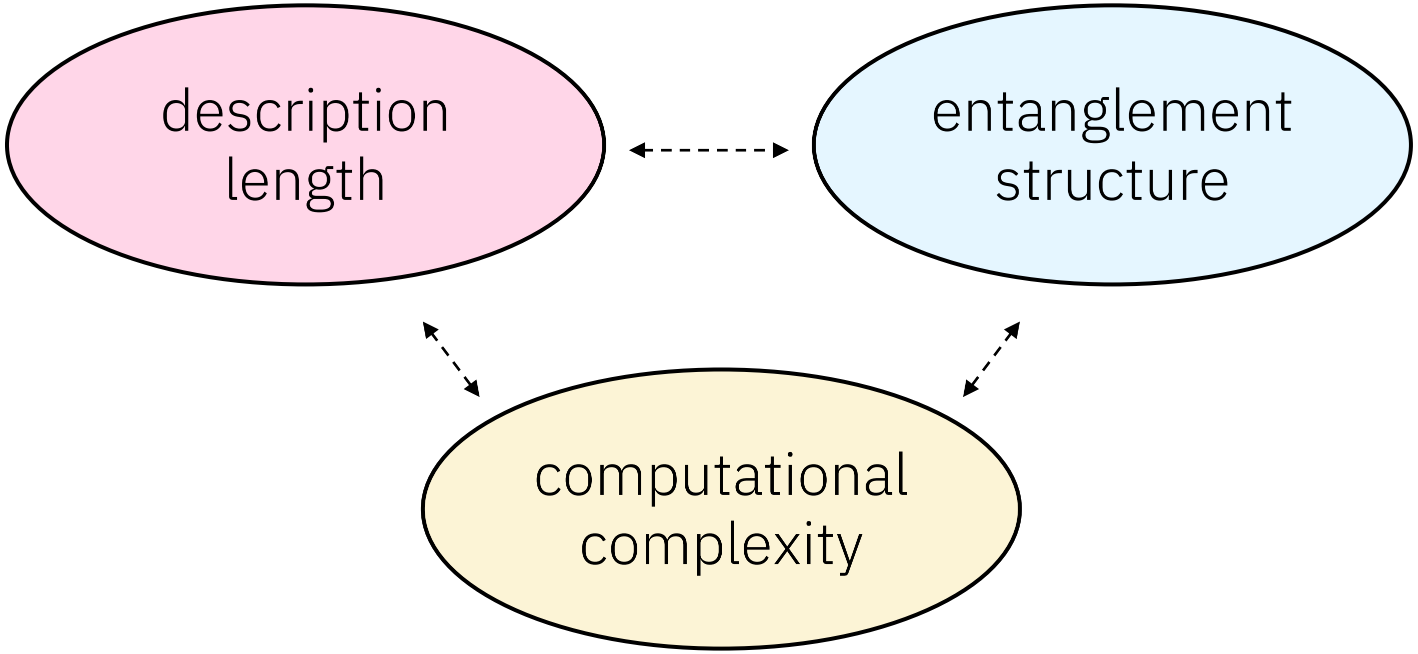
Our motivating question, reframed



today's central question

Are there local Hamiltonians with no short description low-energy states?

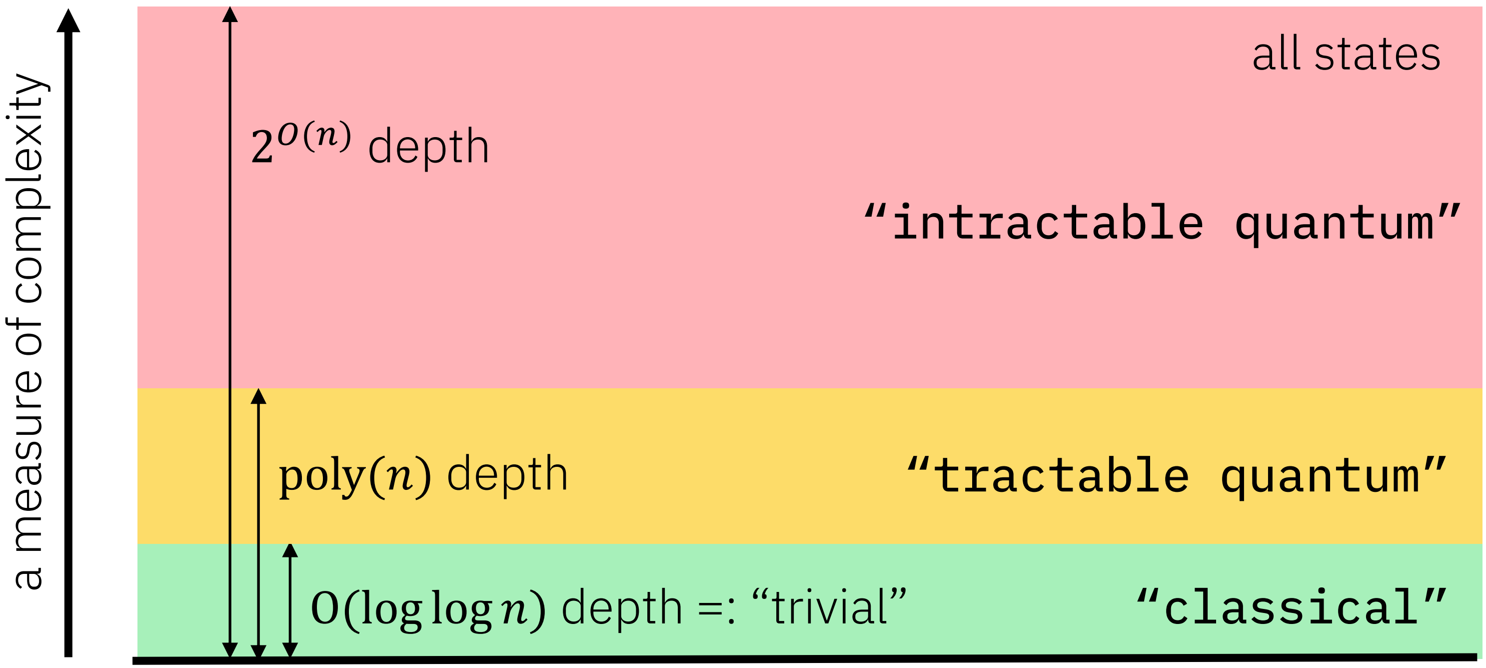
Our motivating question, reframed



today's central question

Are there local Hamiltonians with no trivial-depth low-energy states?

Our motivating question, reframed



today's central question

Are there local Hamiltonians with no trivial-depth low-energy states?

The NLTS problem

No Low-energy Trivial States (NLTS) Conjecture
Freedman and Hastings ‘14.

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 $\omega(\log\log n)$ circuit depth.

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

low-*error* states

thermal states

“one-sided” low-energy states

every $\leq o(n)$-energy state

all low-energy “combinatorial” states

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 every $\leq \epsilon n$-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 warm temperature!

NLTS is an *engineering* feat – construction builds on Hamiltonian complexity, error-correction, and expander graphs

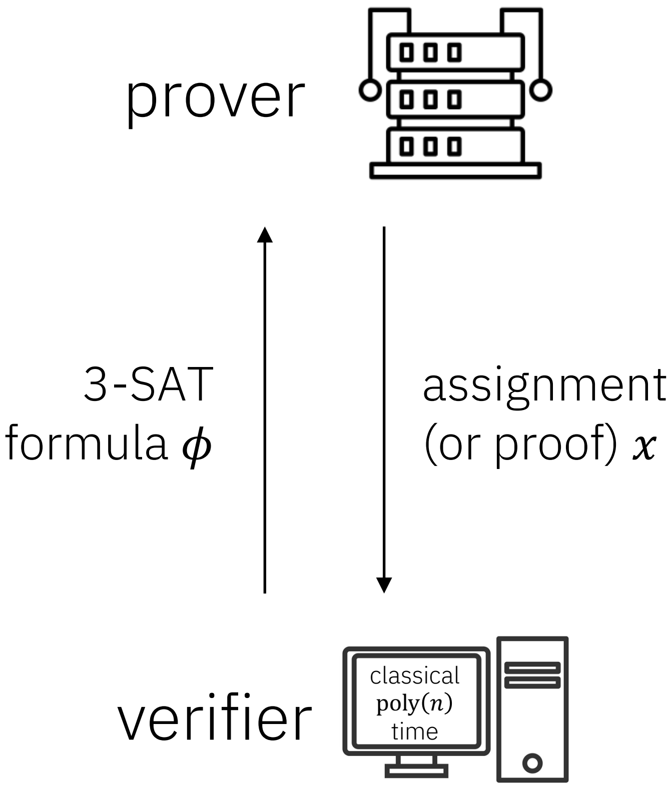
First evidence of the entanglement conjectured to exist by the quantum PCP conjecture (more on this next)

Part 1b: The quantum PCP conjecture

Quanta Magazine

The classical PCP theorem

"the most important result in complexity theory since Cook's theorem" –Ingo Wegener



NP

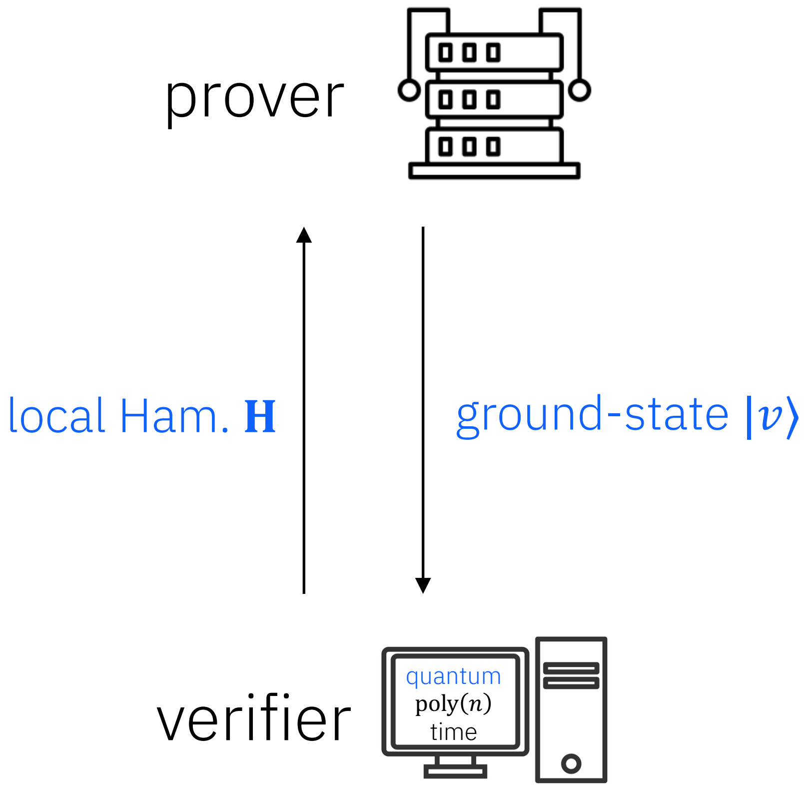
A verifier needs to read the entire proof x to check correctness

PCP theorem (proof checking): there is a family of NP-complete proofs so that only a constant number of bits need to be read!

PCP Theorem (satisfiability) [AS'92]:
NP-complete to estimate the satisfiability of a SAT formula ϕ to 1% multiplicative error

What is the quantum analog?

The quantum PCP conjecture

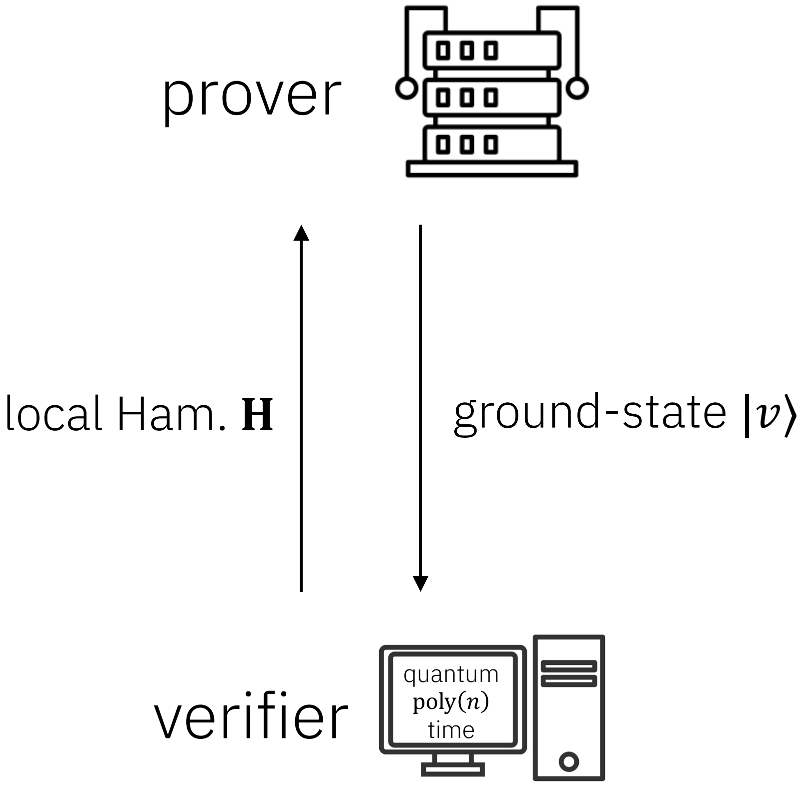


QMA

PCP Theorem (satisfiability) [AS'92]:
NP-complete to estimate the satisfiability of a SAT formula ϕ to 1% multiplicative error

QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to estimate the ground-energy of a local Hamiltonian up to 1% multiplicative error

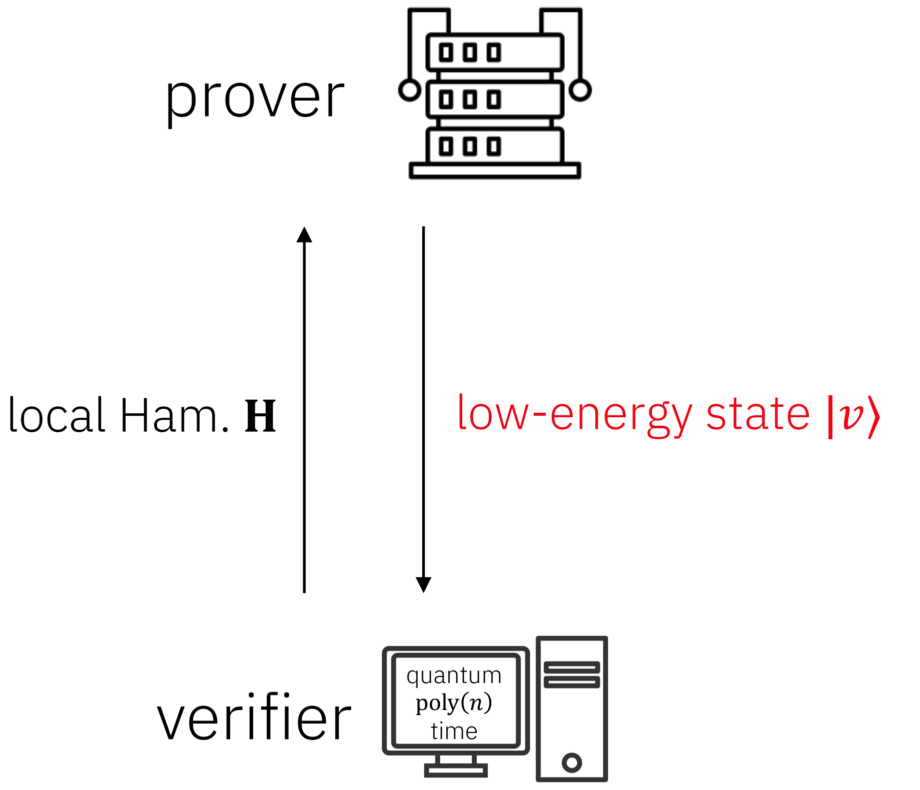
Implications for robust entanglement



QMA

QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to estimate the ground-energy of a local Hamiltonian up to 1% multiplicative error

Implications for robust entanglement

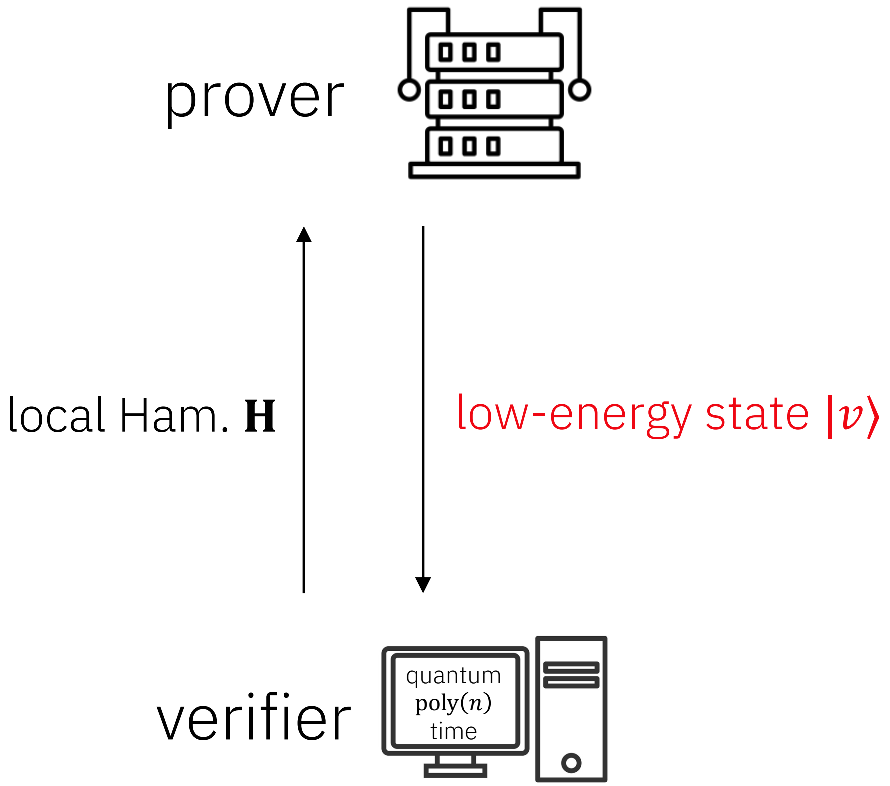


assuming the QPCP conjecture

QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to estimate the ground-energy of a local Hamiltonian up to 1% multiplicative error

QMA

Implications for robust entanglement



QMA

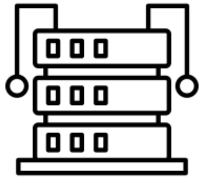
QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to estimate the ground-energy of a local Hamiltonian up to 1% multiplicative error

assuming the QPCP conjecture

If there always exists a low-energy state $|v\rangle$ which is the output of a trivial-depth circuit C,

Implications for robust entanglement

prover

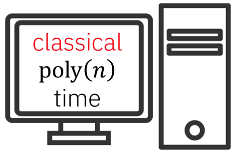


local Ham. $\mathbf{H}$

~~low-energy state $|v\rangle$~~

description of C

verifier



QMA = NP

QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to <u>estimate</u> the ground-energy of a local Hamiltonian up to 1% multiplicative error

assuming the QPCP conjecture

If there always exists a low-energy state $|v\rangle$ which is the output of a trivial-depth circuit C,

then the prover can send the description of C instead.

widely believed to be false

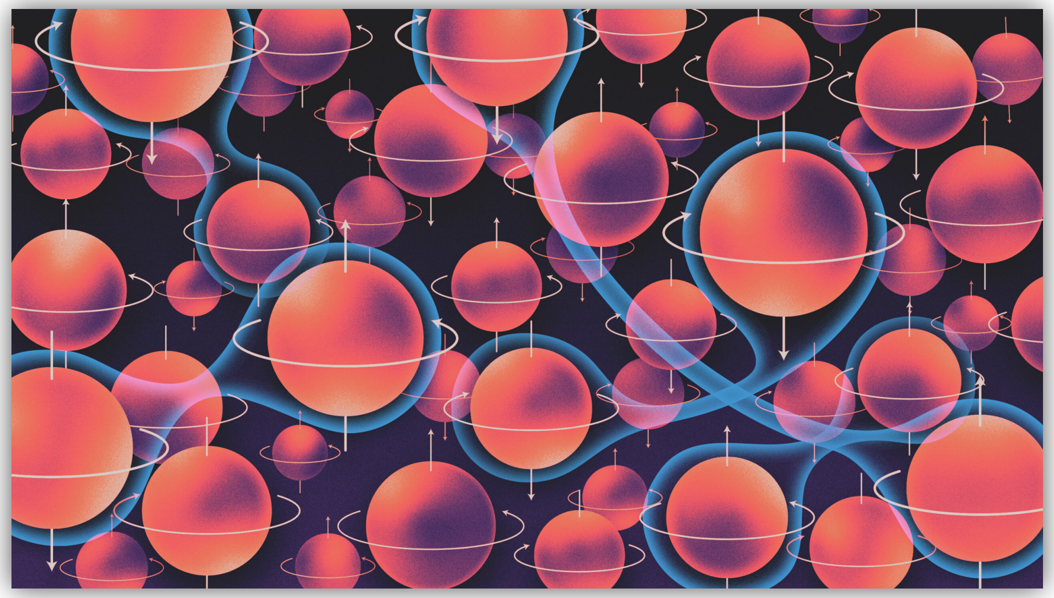
Implications for robust entanglement

QPCP Conjecture (satisfiability) [AN'02]:
QMA-complete to estimate the ground-energy of a local Hamiltonian up to 1% multiplicative error

(assuming QMA ≠ NP)

NLTS Theorem:
There exist local Hamiltonian systems with every $\leq 0.01n$-energy state requiring at least $\Omega(\log n)$ circuit depth

NLTS proof intuition



Kristina Armitage for *Quanta Magazine*

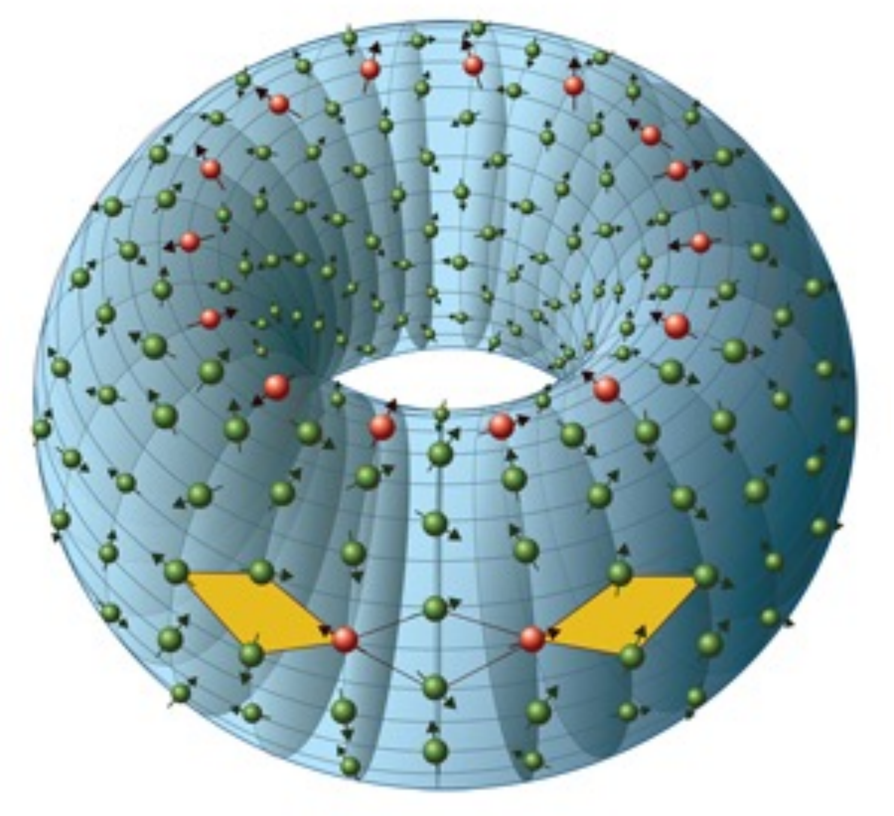
- Exotic examples of entanglement
- Intuition for circuit lower bounds
- Making the circuit lower bounds robust

Quantum error-correcting codes

are a rich source of local Hamiltonian examples with exotic entanglement

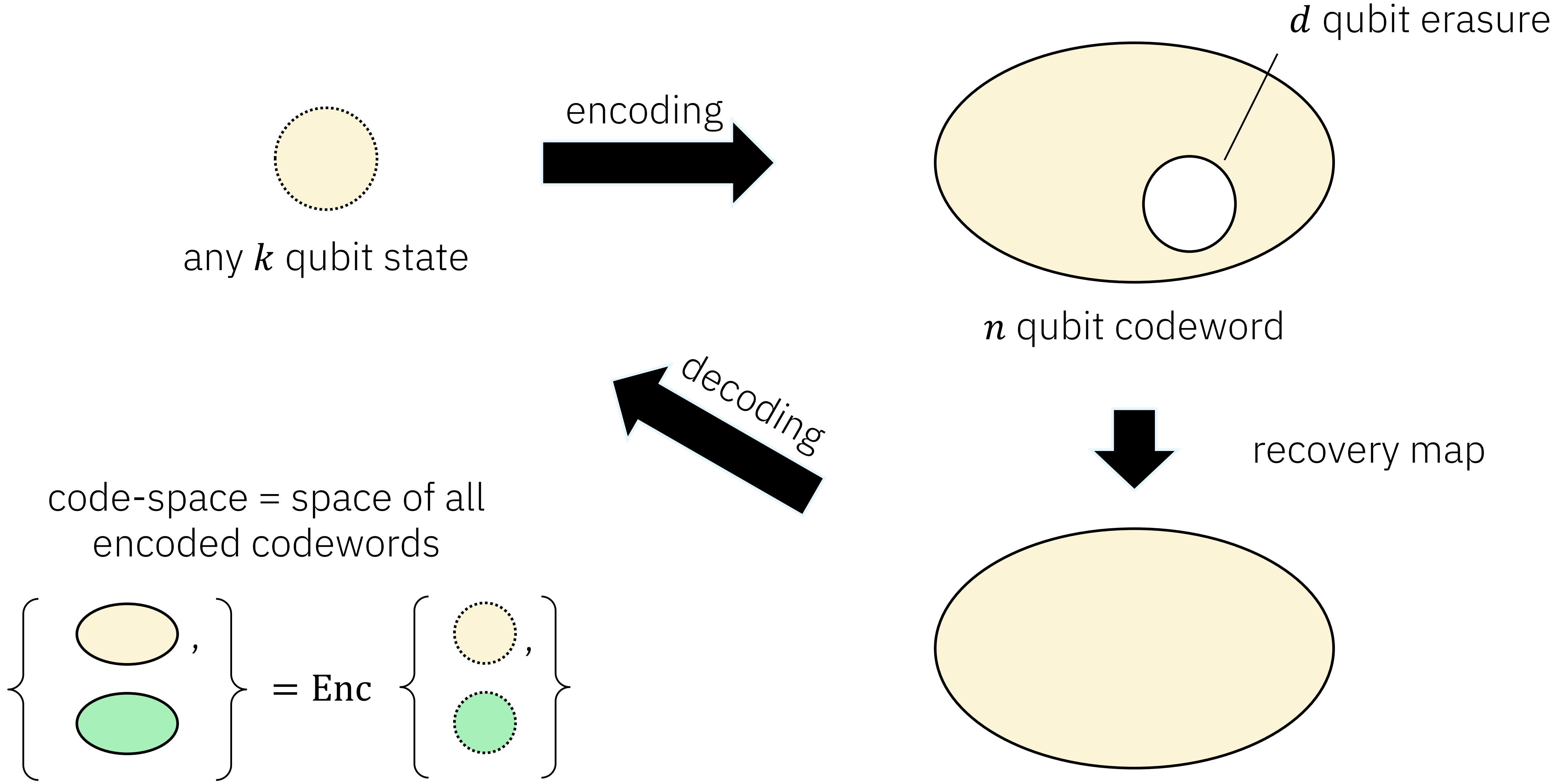
parity check C_i	$\Leftrightarrow$	local Ham. term h_i
code-space	$\Leftrightarrow$	ground-space

Error-correcting codes are good candidates for **NLTS** because there is a folklore proof that the code-states are not trivial



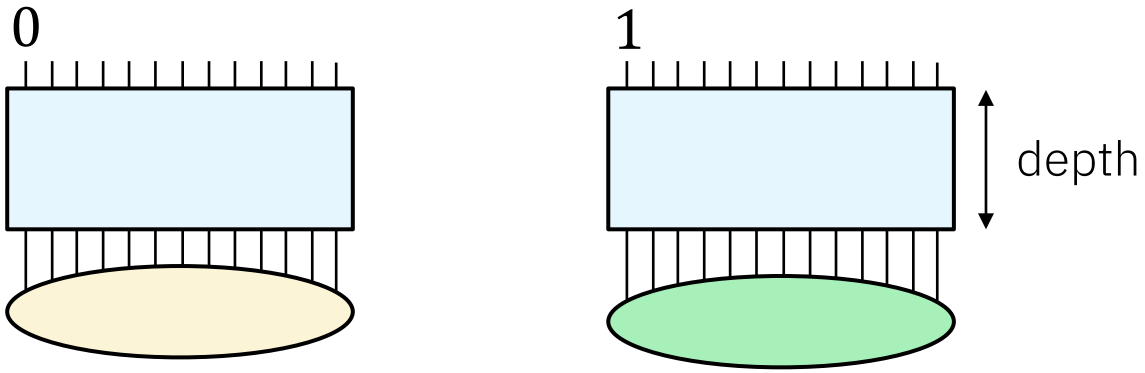
APS/Alexandra Iosub

A primer on quantum error-correcting codes



Minimum depth distinguisher

What is the minimum depth circuit which distinguishes two orthogonal codewords?



This is a quantum phenomenon!
It does not occur classically; ex. repetition code

$$0 \mapsto 000 \ldots 000$$
$$1 \mapsto 111 \ldots 111$$

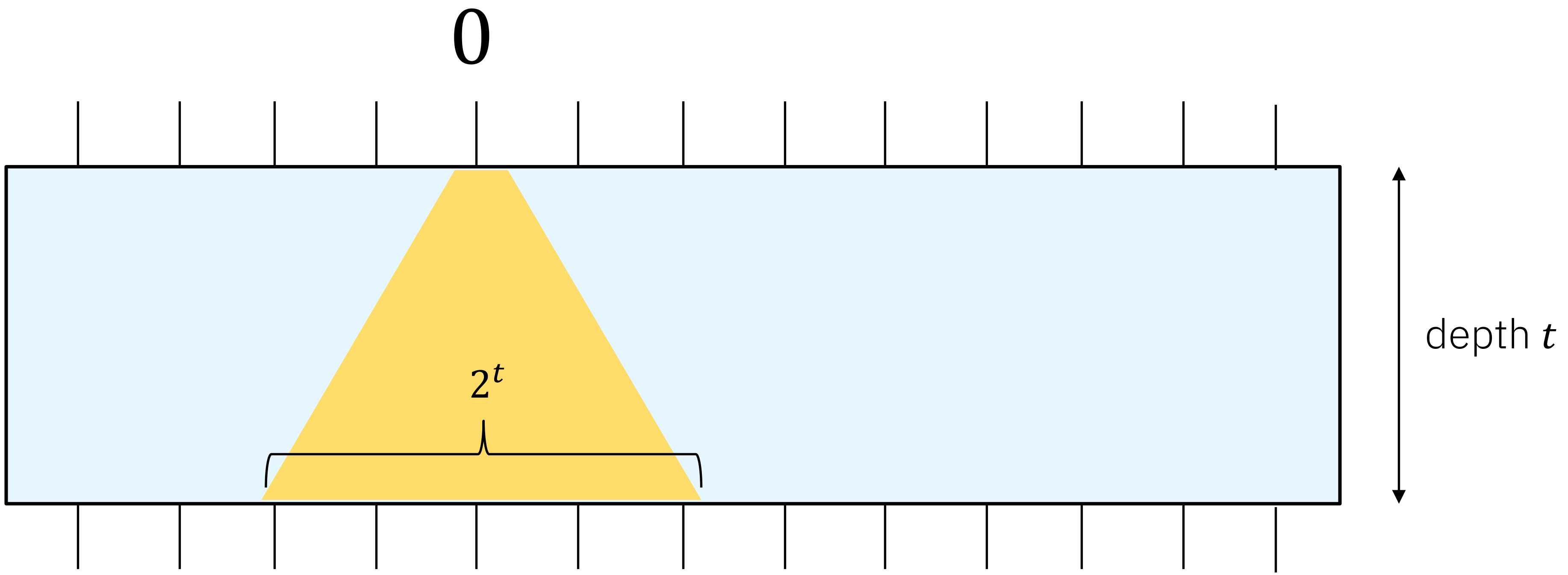
Thm (folklore)
Any distinguishing circuit must have depth at least $\Omega(\log d)$ where d is the code distance.

Corollary (folklore)
Codewords require circuits of depth $\Omega(\log d)$ to generate.

Properties of trivial-depth states

Thm (folklore)
Any distinguishing circuit must have depth at least $\Omega(\log d)$ where d is the code distance.

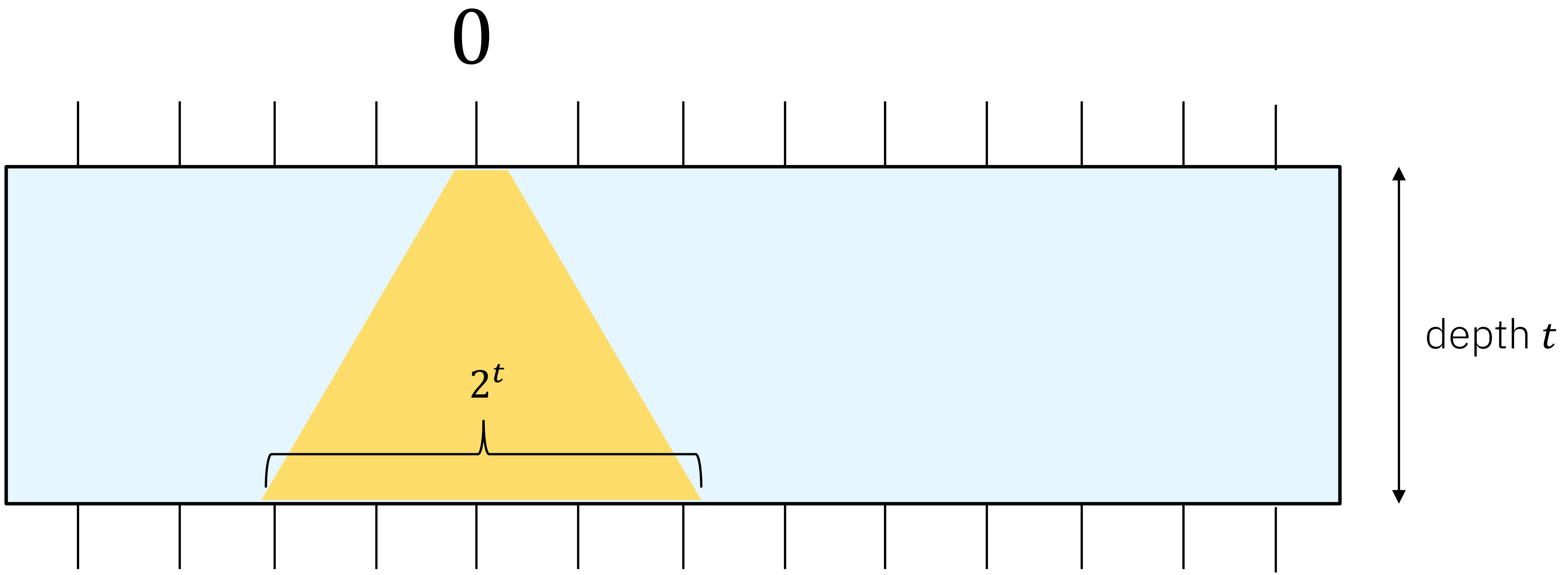
output qubit only depend on few input qubits for low-depth circuits



Properties of trivial-depth states

Thm (folklore)
Any distinguishing circuit must depend on at least $d+1$ qubits where d is the code distance.

output qubit only depend on few input qubits for low-depth circuits

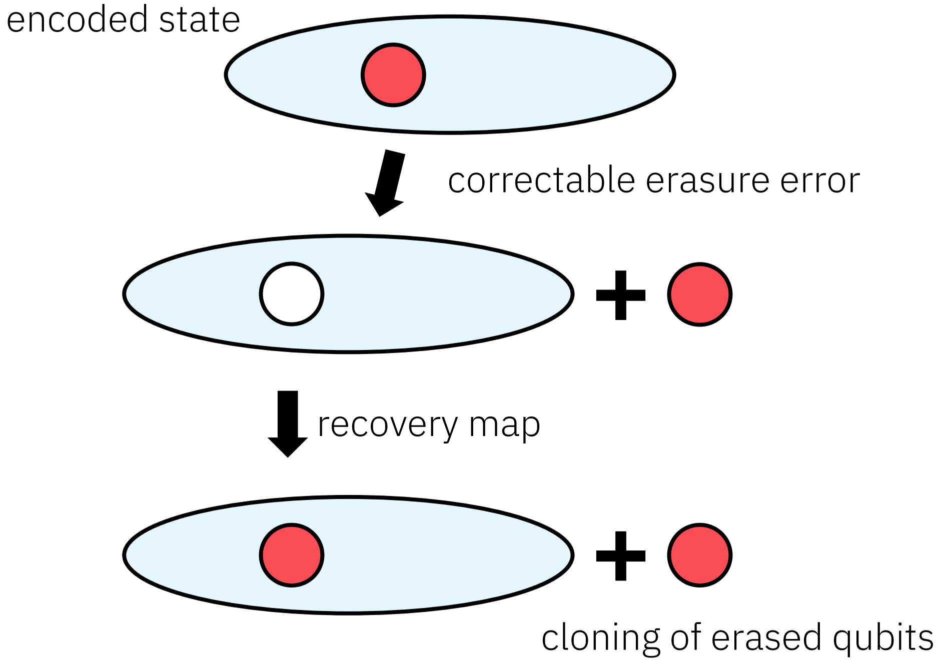


Local indistinguishability of codewords

Thm (folklore)
Any distinguishing circuit must depend on at least $d + 1$ qubits where d is the code distance.

No Cloning Theorem + Quantum Error-Correction ⇒ Local Indistinguishability

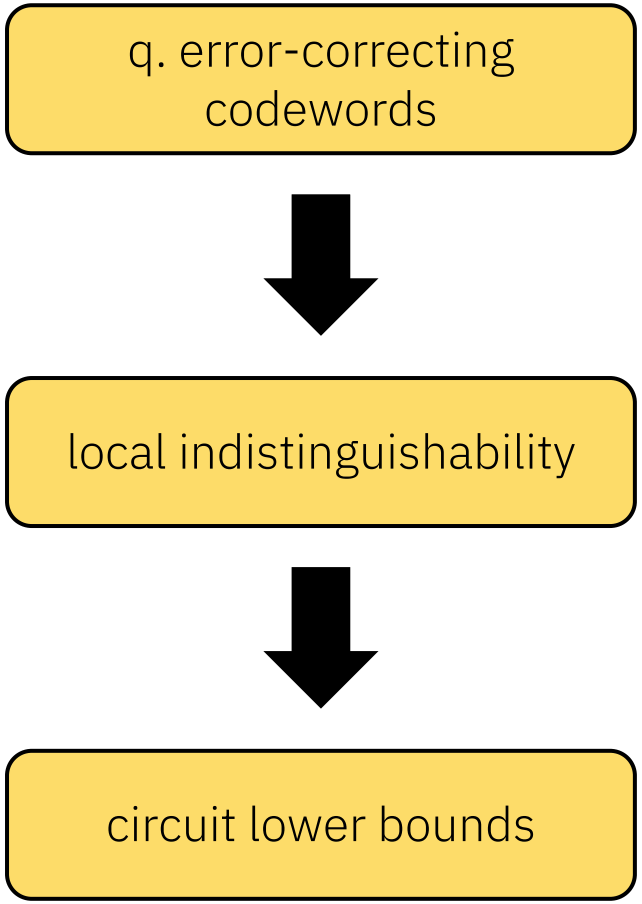
$$|\Psi\rangle|0\rangle \not\mapsto |\Psi\rangle|\Psi\rangle$$



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

qubit state does not depend on which state is encoded

Extending the lower bounds to low-energy states



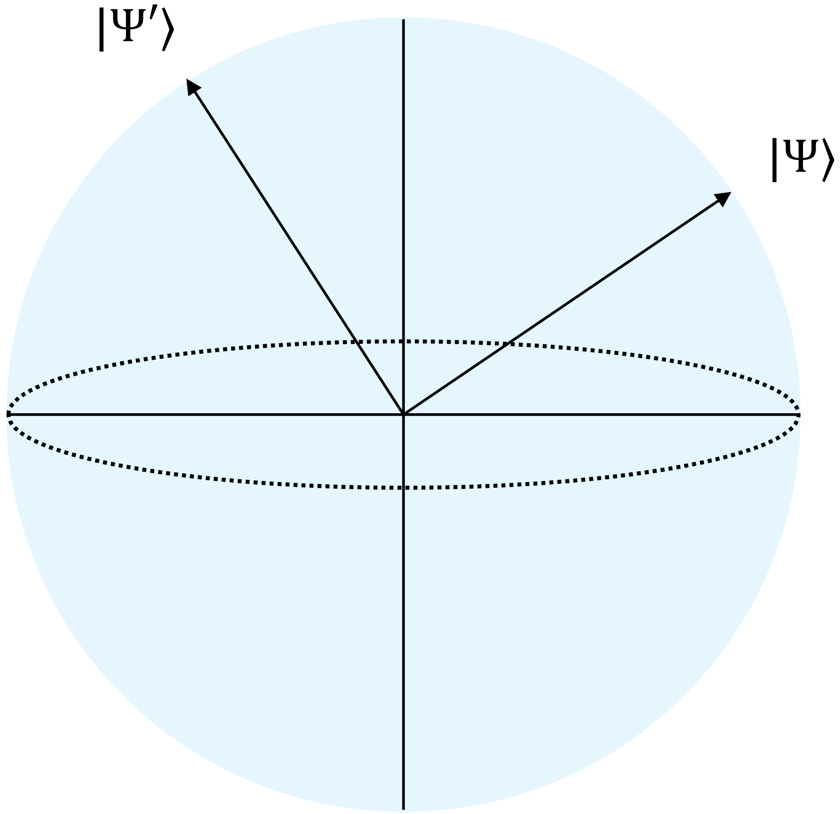
ground-states of error-correcting code Hamiltonians have circuit-depth lower bounds

What about low-energy states?

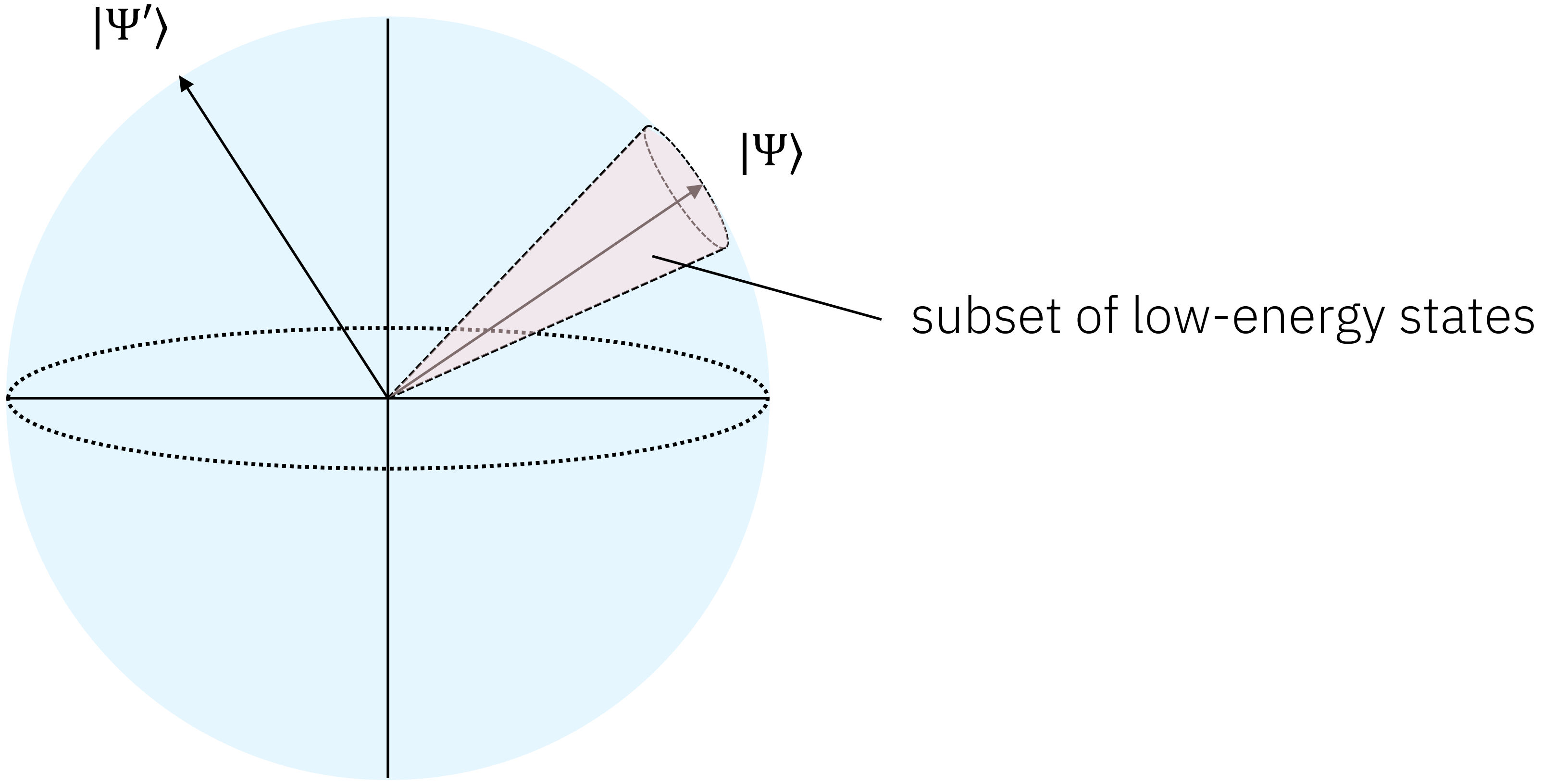
Local indistinguishability is a brittle

Requires proving a “robust” version of the proof technique in order to apply

Local indistinguishability is a brittle proof technique

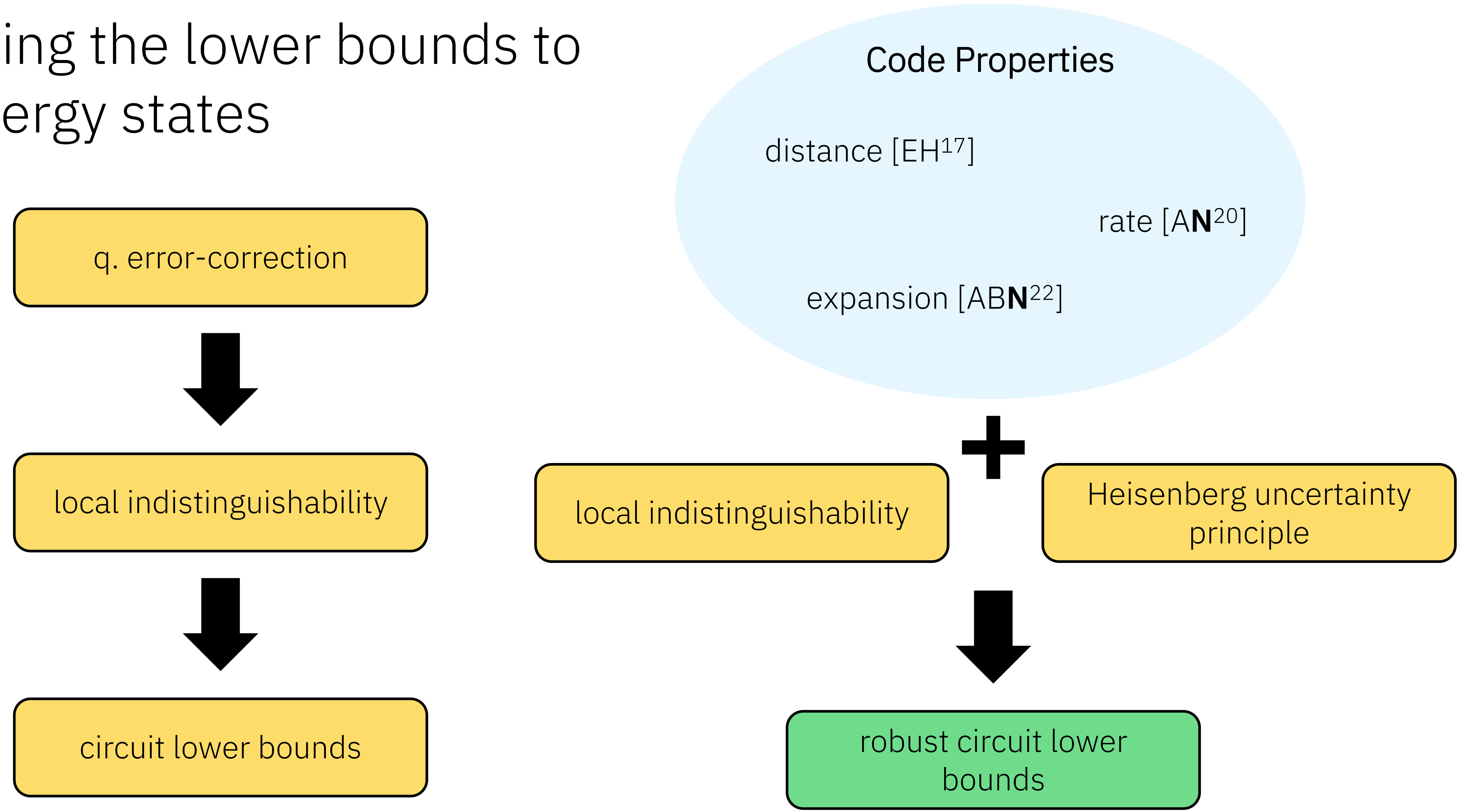


Local indistinguishability is a brittle proof technique



Need a technique for extending lower-bound to the cone around $|\psi\rangle$

Extending the lower bounds to low-energy states



Emergence of optimal-parameter quantum error-correcting codes

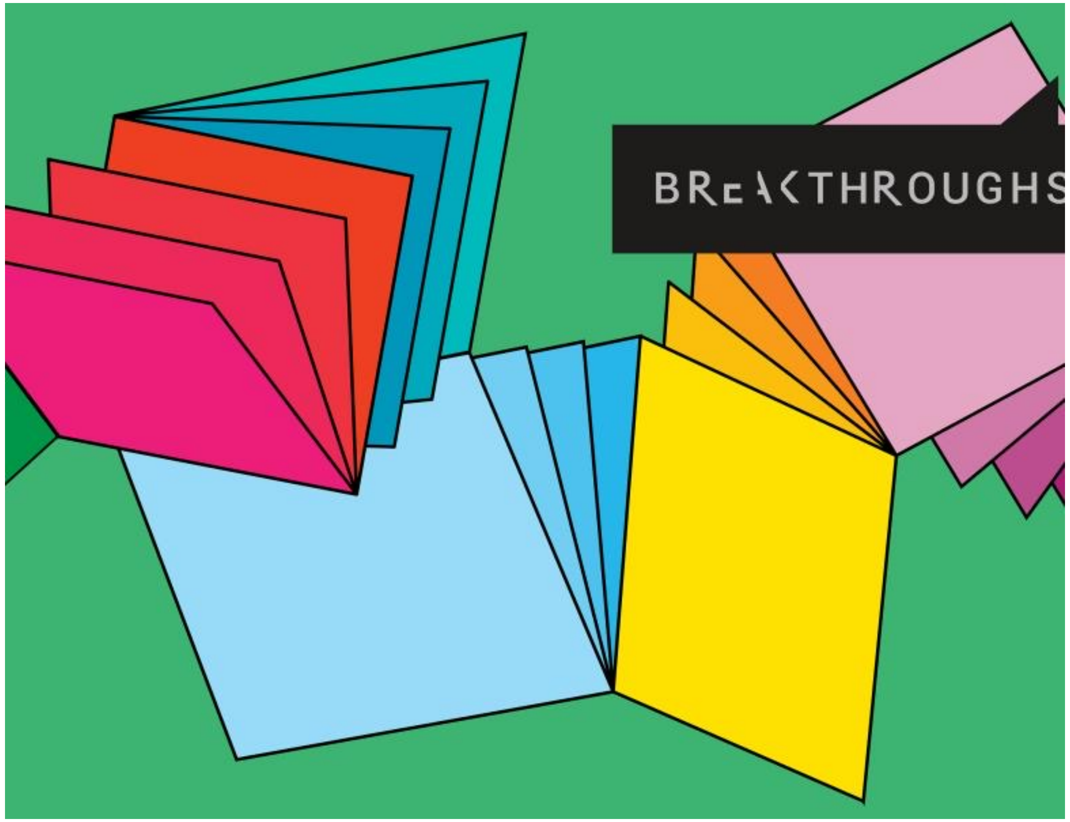
Oct 2021: [Dinur-Evra-Livne-Lubotzky-Mozes[21]] construction of c^3 classical codes (constant rate, constant fraction distance, constant local testability)

Nov 2021: [Panteleev-Kalachev[21]]
Independent construction of linear-rate and -distance quantum codes and c^3 classical codes

Feb 2022: [Leverrier-Zémor[22]]
simplified proof of linear-rate and -distance quantum codes

Jun 2022: [Anshu-Breuckmann-**Nirkhe**[22]]
linear-rate + linear-distance + expanding codes are NLTS

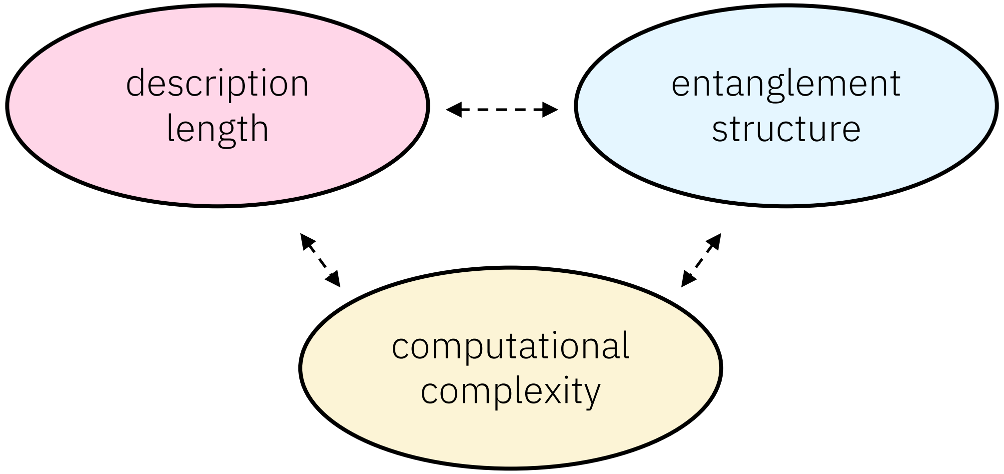
And the Leverrier-Zémor construction has necessary expansion



Simons Institute for the Theory of Computing

Description complexity lower bounds

A broader perspective



- **NLTS** only proves circuit depth lower bounds
- We wanted to prove lower bounds on the length of classical descriptions of low-energy states

Outline for the remainder of the talk

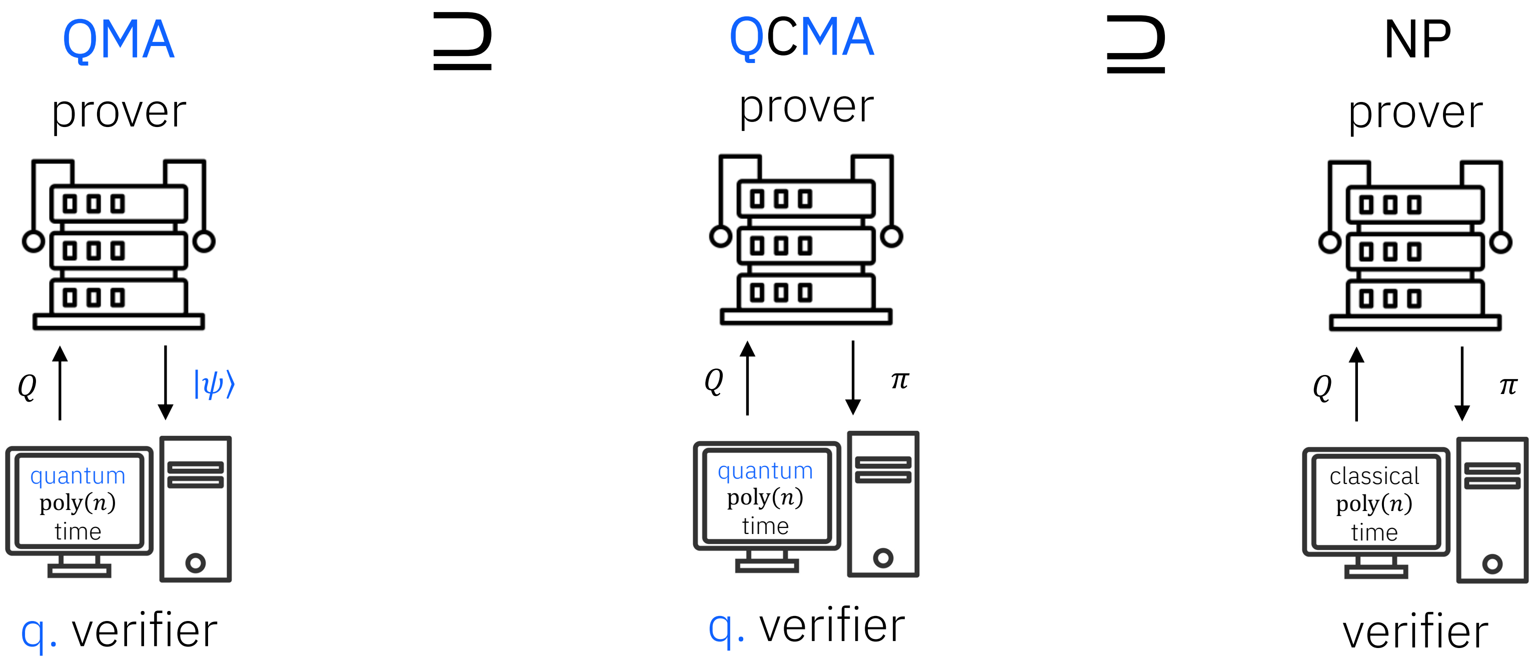
- NLTS and QPCP conjectures
- **Stronger lower bounds in distribution-testing**
- Defining state complexity
- Ideas for future research and open problems

Part 2: exponential lower bounds for ground-states descriptions

A complexity theoretic approach

QCMA

classical proofs for quantum statements

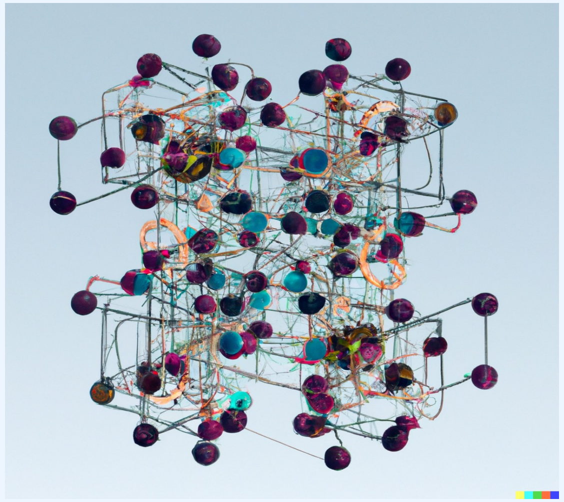


If QMA ≠ QCMA, ⇒ ground-states do not have polynomial-size verifiable classical descriptions.

Proof by contrapositive. If such descriptions exist, then they can be sent in lieu of the original state.

QCMA

classical proofs for quantum statements



VS.

DALL-E 2 renderings.

If QMA ≠ QCMA, ⇒ ground-states do not have polynomial-size verifiable classical descriptions.

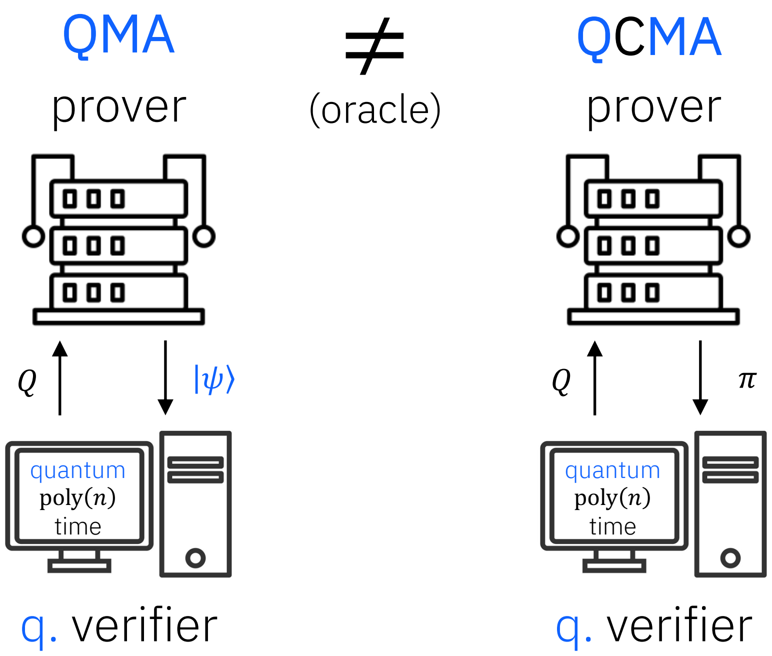
Proof by contrapositive. If such descriptions exist, then they can be sent in lieu of the original state.

Lower bounds for all types of classically verifiable descriptions

NLTS proved that low-depth circuits cannot represent ground- or low-energy states of local Hamiltonians

[Natarajan-**Nirkhe**[22]]:
There exists a generalization of local Hamiltonians for which we can prove that the ground-states cannot be described by <u>any</u> sub-exponential size classical description

More formally prove that a distribution-testing oracle separates QMA and QCMA



Outline for the remainder of the talk

- NLTS and QPCP conjectures
- Stronger lower bounds in distribution-testing
- **Defining state complexity**
- Ideas for future research and open problems

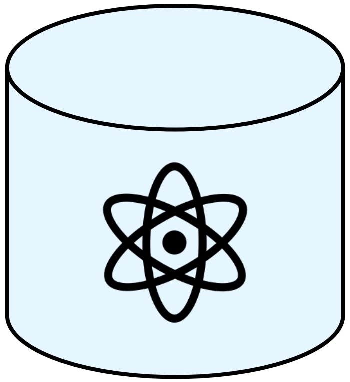
Part 3:
complexity theory for the quantum world

Definitions of state complexity

State complexity classes

Decision Complexity Class

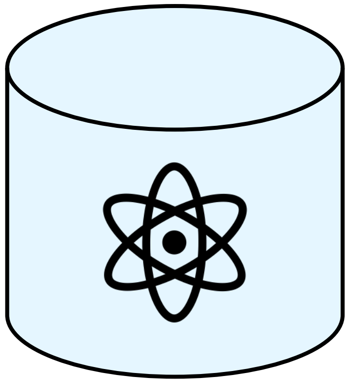
description of a decision problem
ex. Does C accept any quantum state?



yes/no (binary) answer

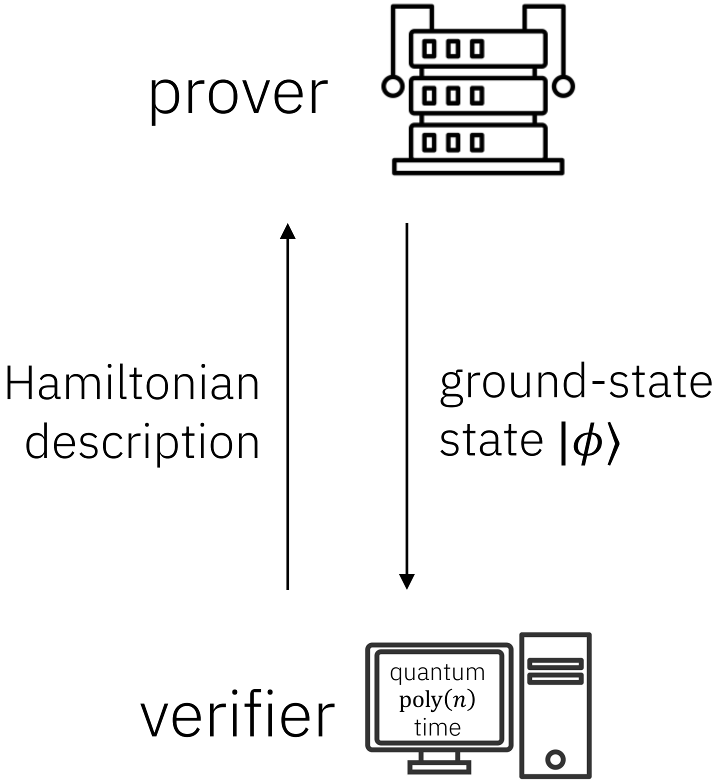
State Complexity Class

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



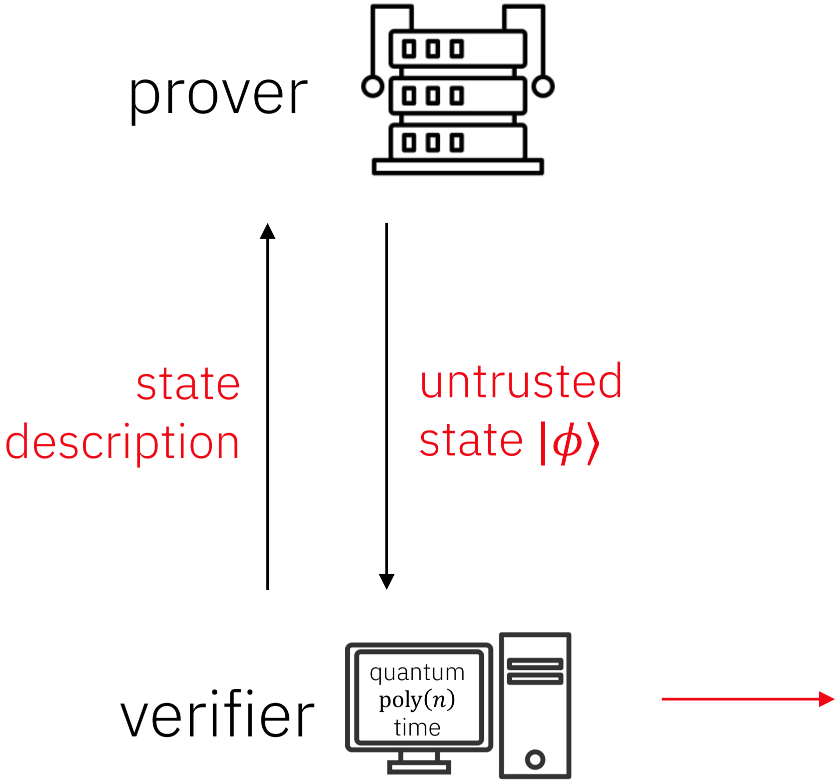
a quantum state ψ matching the description

example complexity class: stateQMA



QMA

example complexity class: **stateQMA**



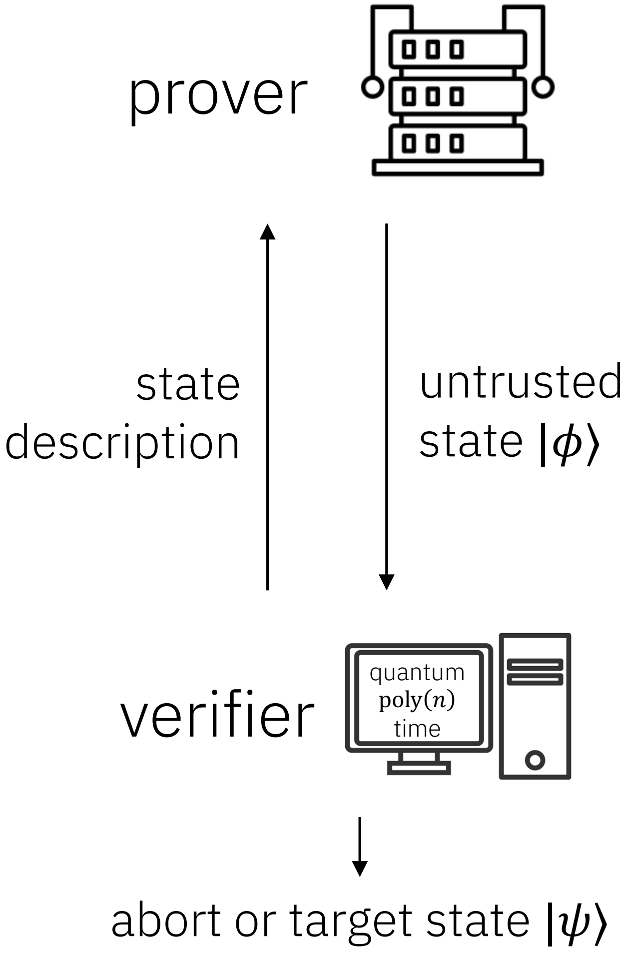
abort or target state $|\psi\rangle$

stateQMA

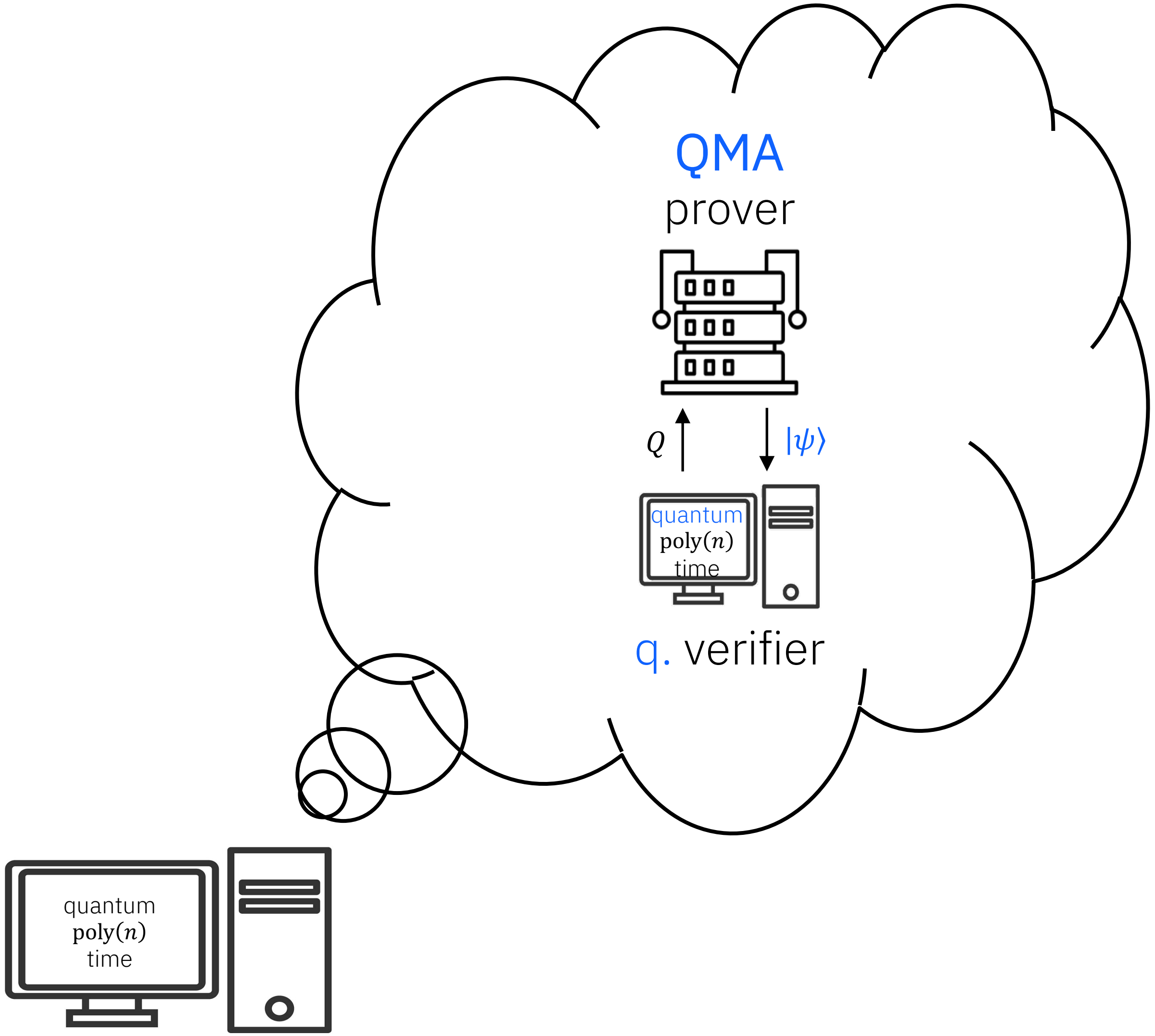
How does **stateQMA** compare to **QMA?**

It is easy to prove that **stateQMA** contains the ground-states of local Hamiltonians

Comparing **stateQMA** and **QMA**

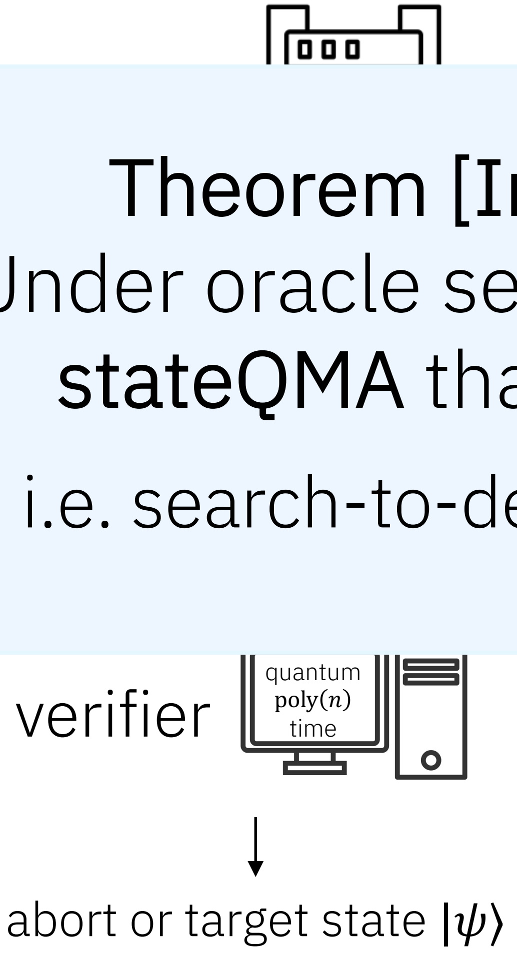


stateQMA



$\text{stateBQP}^{\text{QMA}}$

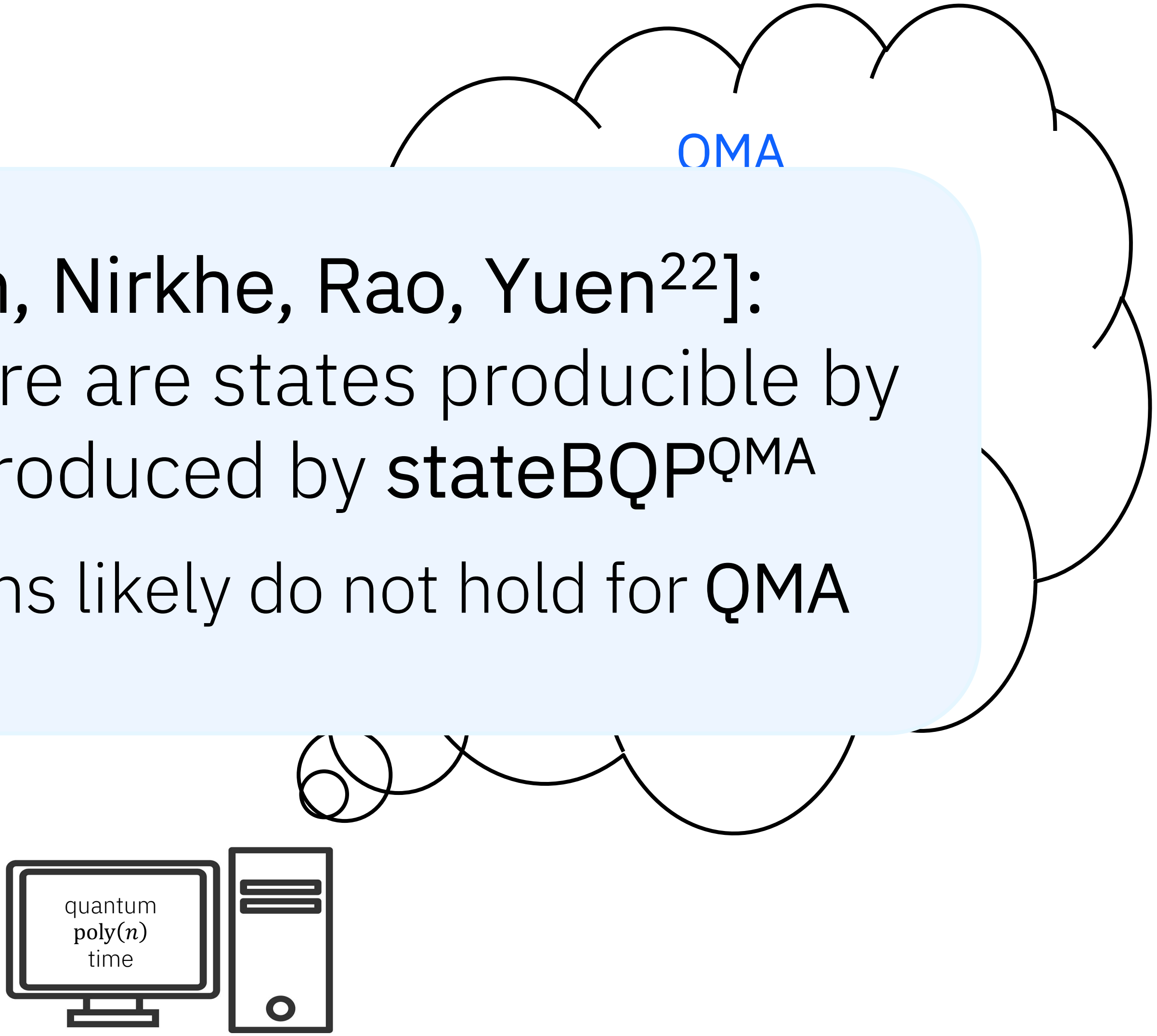
Comparing **stateQMA** and **QMA**



stateQMA

Theorem [Irani, Natarajan, Nirkhe, Rao, Yuen'22]:
Under oracle separations, there are states producible by **stateQMA** that cannot be produced by **stateBQP$^{\text{QMA}}$**

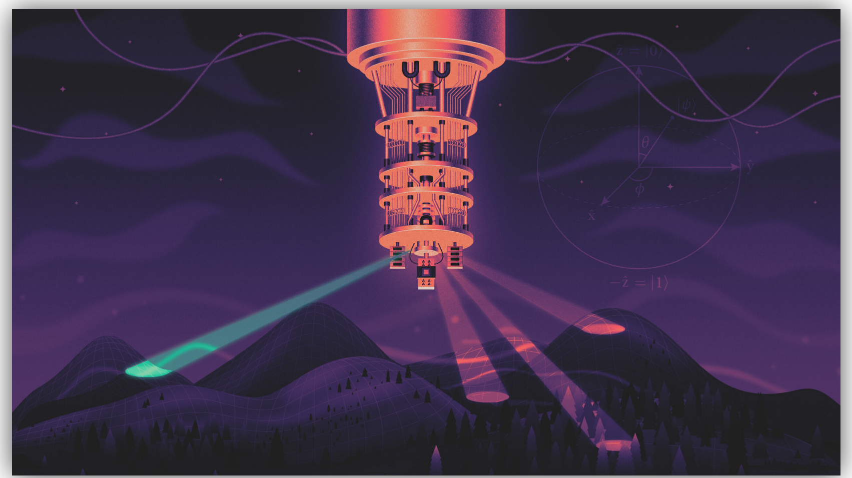
i.e. search-to-decision reductions likely do not hold for **QMA**



stateBQP$^{\text{QMA}}$

Our current understanding of state complexity

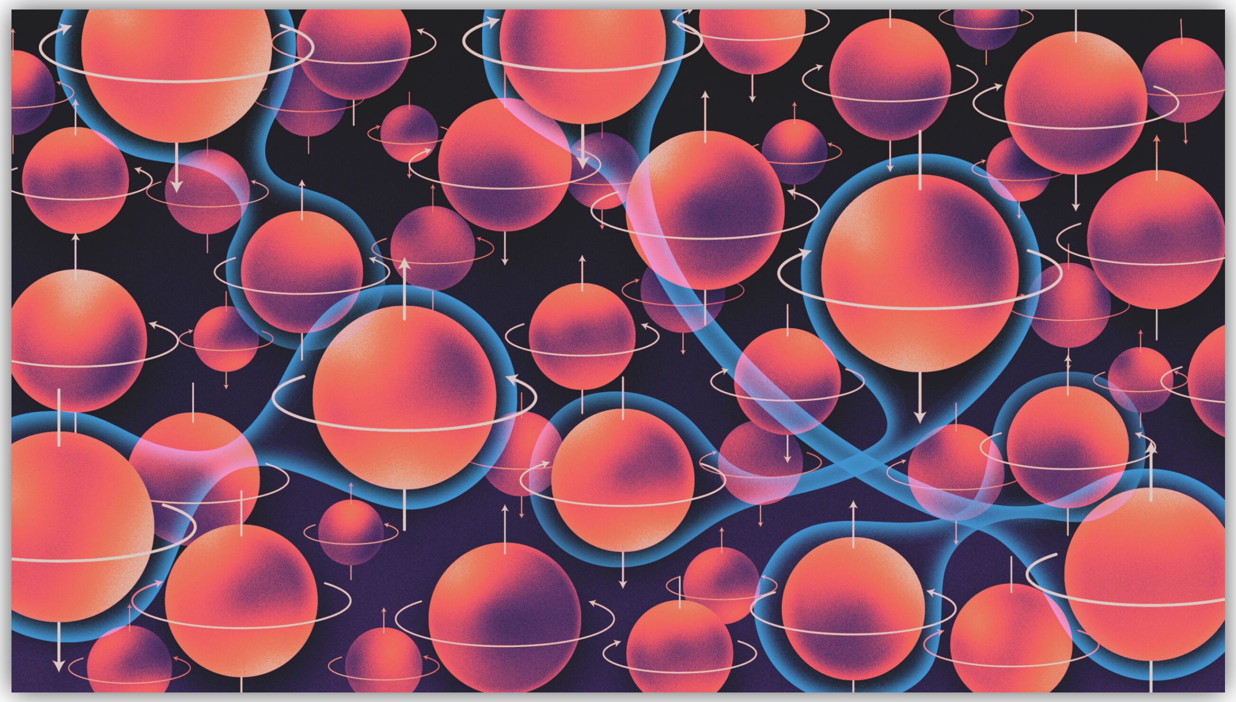
- **stateQMA** is (likely) not equal to $\textbf{stateBQP}^{\textbf{QMA}}$
  - Equivalently, **QMA** does not have search-to-decision reductions
  - [Irani, Natarajan, **Nirkhe**, Rao, Yuen[22]]
- **stateQIP** = **statePSPACE**
  - interactive protocols for state generation are equal to space-bounded constructible states
  - [Rosenthal, Yuen[22] and Metger,Yuen[23]]
- Unitary synthesis problems
  - What can we say about the complexity of quantum state transformations?
  - Can all unitaries be synthesized with access to a suitably powerful oracle? [Aaronson[16]]


Kristina Armitage for *Quanta Magazine*

Outline for the remainder of the talk

- NLTS and QPCP conjectures
- Stronger lower bounds in distribution-testing
- Defining state complexity
- **Ideas for future research and open problems**

Future work and open questions



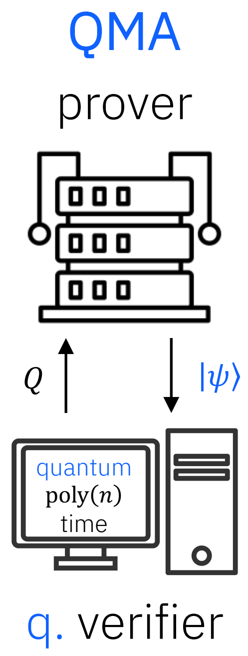
Kristina Armitage for *Quanta Magazine*

Open problems

Quantum Probabilistically Checkable Proofs (QPCP) Conjecture

Is it hard-to-approximate the minimum eigenvalue of local Hamiltonian?

- Biggest open question in quantum complexity theory
- Can we verify "quantum proofs" quickly without reading too many bits?
- Classical PCPs revolutionized theoretical CS (ex. cryptography, approx. algs)
- Help understand the nature of "many-body" entanglement at low-temperature
    - Partially resolved by the NLTS problem (QPCP implies NLTS)

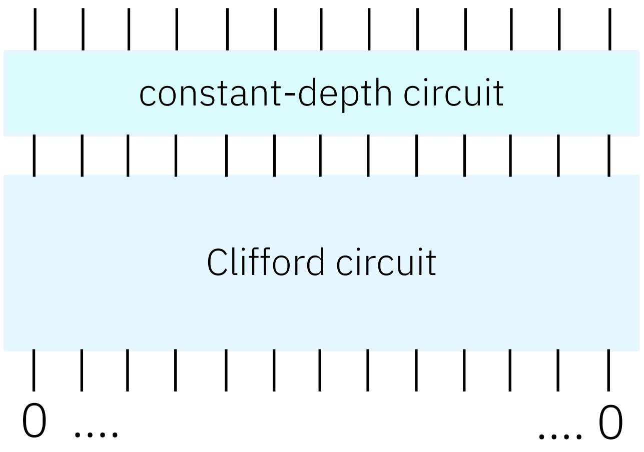


Proving stronger lower bounds than NLTS

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!

Open problems

Fleshing out the notion of state complexity

How should we understand quantum states in relation to the pantheon of results in complexity theory?

- Quantum states generalize distributions, quantum computation, and describe physical phenomenon
- How do we understand their complexity? Meaning we need to understand how to define computation with quantum inputs and/or quantum outputs
  - Notions of reductions, relations to decision complexity
  - hardness-of-approximation, interactive proofs
  - Specifically, what is the correct notion of **stateNP**? How do we generalize NLTS Hamiltonians?

IBM