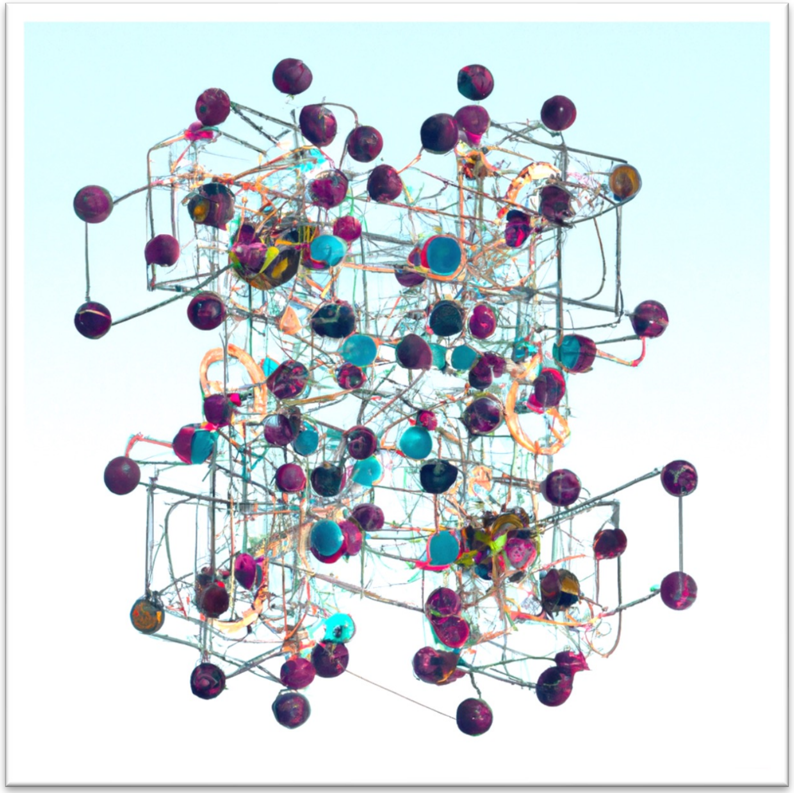
A classical oracle separation between **QMA** and **QCMA**

(or, the hardness of describing physically relevant states)

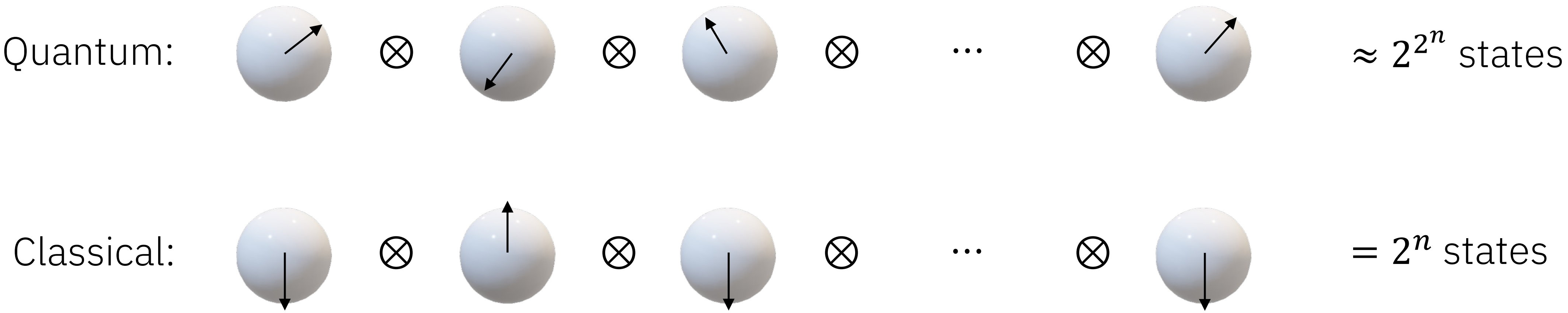


A DALL-E 2 rendering

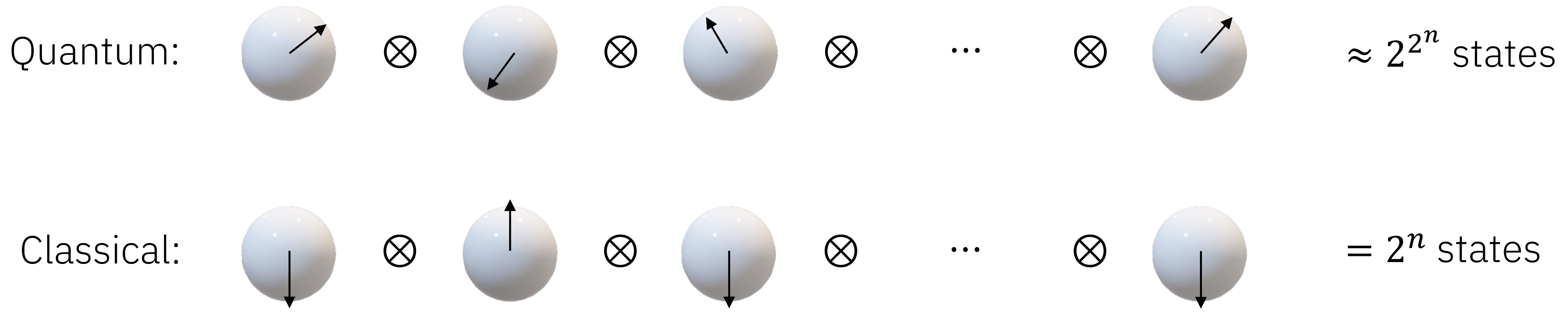
Anand Natarajan (MIT) and **Chinmay Nirkhe (IBM Quantum Cambridge)**

IBM

We know that most quantum states are complex…



but how many of them are interesting for physics?

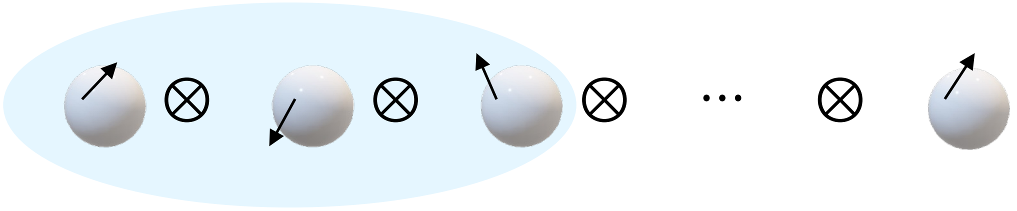


Quantum states that are interesting for physics

The energy operator in quantum mechanics is called the **Hamiltonian**.

Interesting physical systems are defined by Hamiltonians of a special form called **local Hamiltonians**.

$$H = \sum h_i$$



$$h_i = |000\rangle\langle 000| - |111\rangle\langle 111|$$

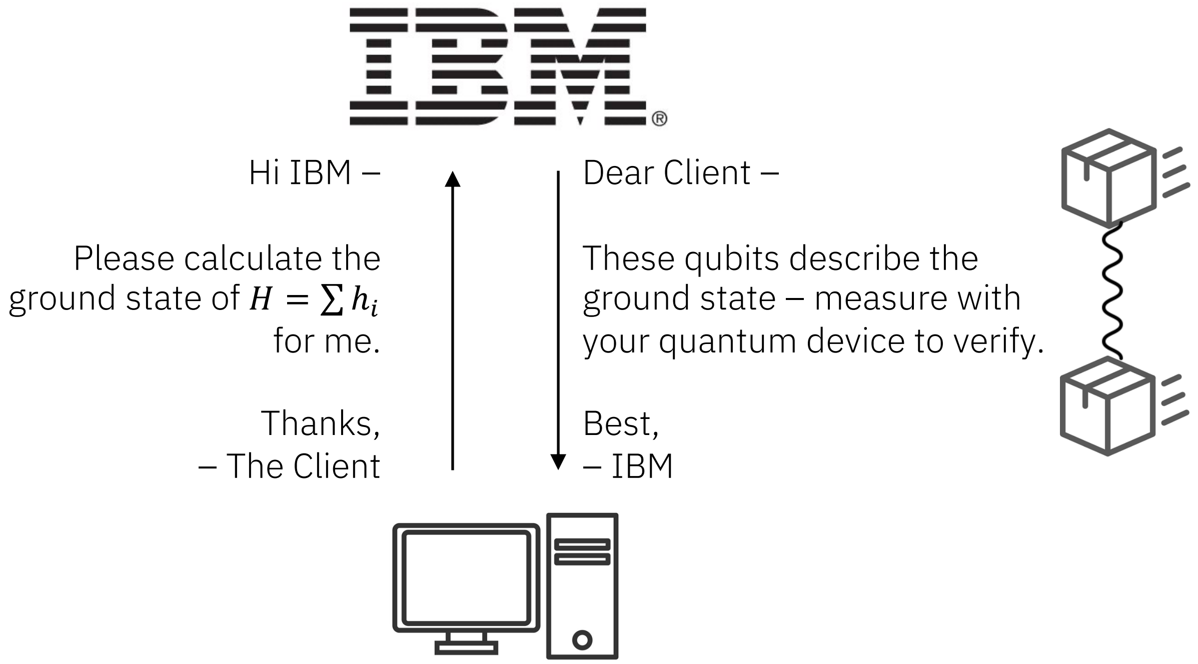
Due to the importance of ground states in condensed matter physics,

we would really like to know if ground states of local Hamiltonians have efficient (i.e. short) classical descriptions.

Our result [Natarajan-Nirkhe]: Probably not.

We can construct some *nearly* physical Hamiltonians for which there are provably no efficient classical descriptions.

Why IBM Quantum should care about this problem...

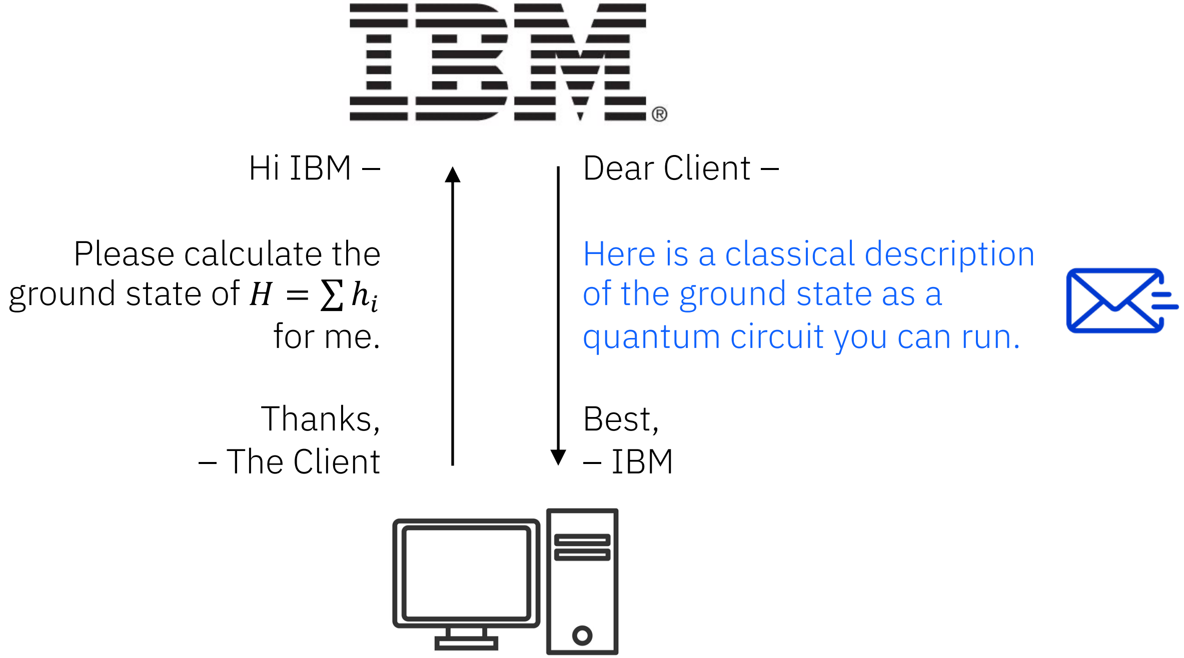


Receiving $|\psi\rangle$ as a quantum state requires that the client can receive qubits from IBM.

This isn't realistic.

However, it would be nice if instead we could send a *convincing* description of $|\psi\rangle$.

Why IBM Quantum should care about this problem...



Receiving $|\psi\rangle$ as a quantum state requires that the client can receive qubits from IBM.

This isn't realistic.

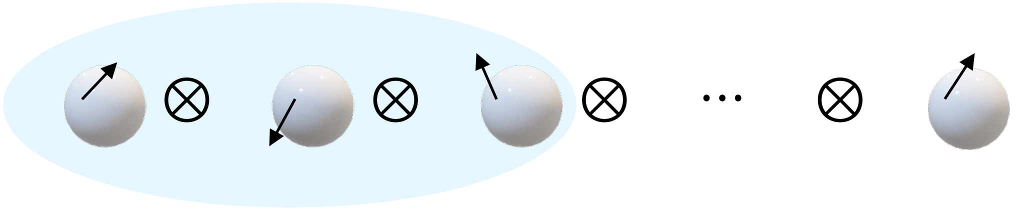
However, it would be nice if instead we could send a *convincing* description of $|\psi\rangle$.

The connection to the theory of quantum computation

The energy operator in quantum mechanics is called the **Hamiltonian**.

Interesting physical systems are defined by Hamiltonians of a special form called **local Hamiltonians**.

$$H = \sum h_i$$



$$h_i = |000\rangle\langle 000| - |111\rangle\langle 111|$$

The problem of calculating the ground energy

$$E = \min_{|\psi\rangle} \langle\psi|H|\psi\rangle$$

famously connects physics to computer science as the problem is *complete* for the class **QMA.**

QMA = Quantum Merlin-Arthur

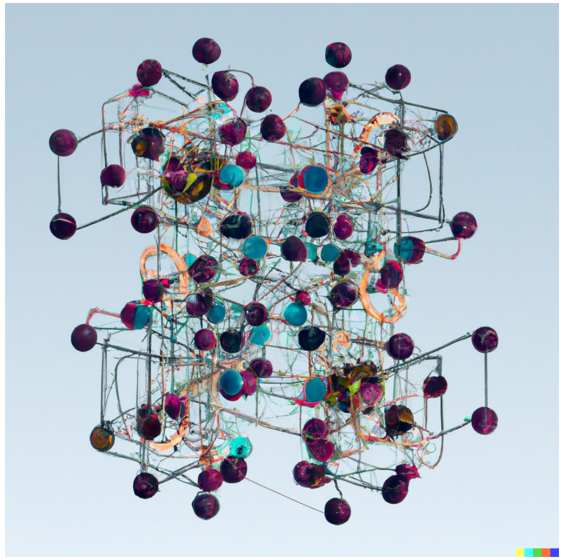
If the ground state can always be *verifiably* classically described, then the problem is complete for the class **QCMA.**

QCMA = Quantum-Classical Merlin-Arthur

Proving that **not** all ground states of local Hamiltonians can be (verifiably) classically described is

equivalent to

proving that QCMA $\neq$ QMA.



vs.

DALL-E 2 renderings.

Theorem [Natarajan-Nirkhe]: There is a black-box distribution D for which we can prove that

$$\mathrm{QCMA}^{D} \neq \mathrm{QMA}^{D}.$$

This is the strongest evidence yet that ground states cannot be classically described.

Proving **QCMA ≠ QMA** outright would have incredible implications for complexity theory. Consequently, it requires truly novel techniques.

Instead, the best we can do is slightly generalize the notion of local Hamiltonians until we can prove **QCMA ≠ QMA.**

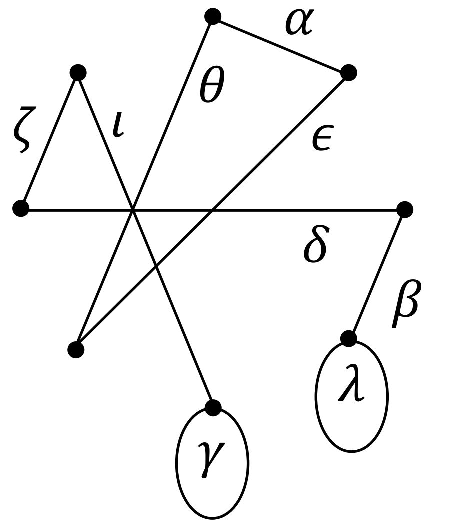
Local Hamiltonians	=	Sparse Hamiltonians	$\Rightarrow$	n-bit boolean functions (classical oracles)	$\Rightarrow$	Distributions over n-bit boolean functions (distribution oracles)	$\Rightarrow$	n-qubit quantum unitaries (unitary oracles)
				Optimal oracle separation		This work!		Previous constructions [AK07, FK18]

Generalizing sparse Hamiltonians to graphs

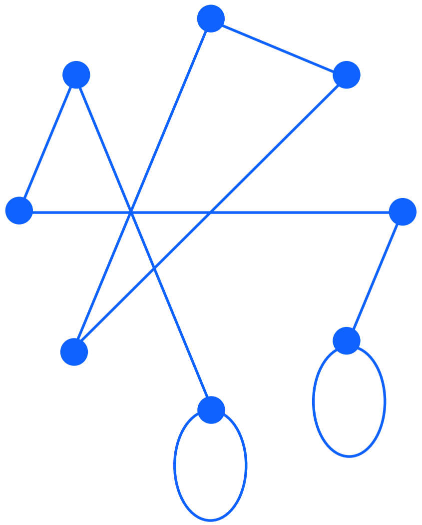
$$H = \begin{pmatrix} 0 & \alpha & 0 & 0 & 0 & \theta & 0 & 0 \\ \alpha & 0 & 0 & 0 & 0 & \epsilon & 0 & 0 \\ 0 & 0 & 0 & \beta & 0 & 0 & \delta & 0 \\ 0 & 0 & \beta & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma & 0 & 0 & \iota \\ \theta & \epsilon & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 & 0 & 0 & 0 & \zeta \\ 0 & 0 & 0 & 0 & \iota & 0 & \zeta & 0 \end{pmatrix}$$

n-qubit sparse Hamiltonian

$\Longrightarrow$



2^n vertex weighted graph



2^n vertex **unweighted** graph

$\Longrightarrow$

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

Adjacency matrix of graph

Low energies of sparse graph Hamiltonians

If H is the Hamiltonian corresponding to a d-regular sparse graph,

then $-H$ is a Hamiltonian with ground energy equal to $-d$ with a ground state of $\sum_{x\in\{0,1\}^n}|x\rangle$, the uniform super position.

What is the second smallest eigenvalue?

If the graph has ≥ 2 connected components,
it is also $-d$.

If the graph is α-expanding,
it is $-d+\alpha d$.

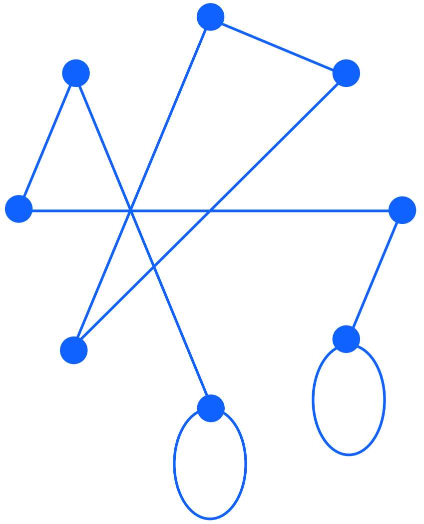
Theorem 1: Deciding if a graph (given as black-box sparse adjacency list) either has multiple connected components or is 0.01-expanding is in QMA.

This also holds for certain distributions over graphs.

Theorem 2: For the same set of distributions, we can show that no efficient QCMA algorithm exists.

Together they prove $\text{QCMA}^{D} \neq \text{QMA}^{D}$.

The **QMA** algorithm



$$|\xi_1\rangle = \frac{|3\rangle + |4\rangle + |5\rangle + |7\rangle + |8\rangle}{\sqrt{5}} \qquad |\xi_2\rangle = \frac{|1\rangle + |2\rangle + |6\rangle}{\sqrt{3}}$$

Easy to check that

$$|\xi_{\text{solution}}\rangle = \frac{\sqrt{5}}{\sqrt{8}}|\xi_2\rangle - \frac{\sqrt{3}}{\sqrt{8}}|\xi_1\rangle$$

is a eigenvector of eigenvalue $-d$ as well and is orthogonal to $\sum_{x\in\{0,1\}^n} |x\rangle$.

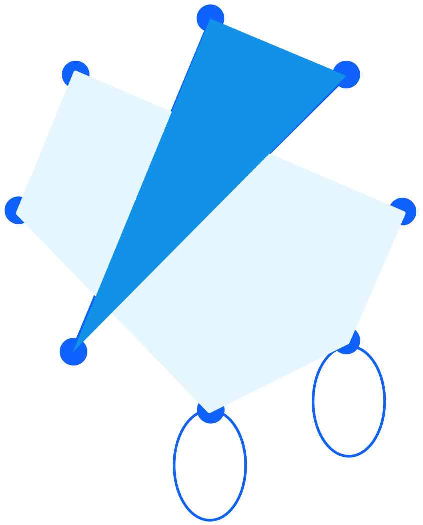
Quantum solution is to provide $|\xi_{\text{solution}}\rangle$ which proves that there are 2 eigenvectors of eigenvalue $-d$.

If the graph is α-expanding, this test **fails** with probability $\alpha/4$ as there is only 1 eigenvector of eigenvalue $-d$ and the next eigenvalue is $-d + \alpha d$.

Sketch of **QCMA** impossibility result

In the QMA algorithm, we saw that the solution state only depends on the *vertices* in the connected component.

Step 1: "Blind" the problem using distributions over graphs so that solutions can only depend on the vertices in the connected component.



Step 2: Use counting arguments to show that the number of connected components is $\geq 2^{2^{\sqrt{n}}}$ while the number of classical descriptions is $\leq 2^{\mathbf{poly}(n)}$.

So many ($2^{1.9^{\sqrt{n}}}$) graphs must correspond to the same proof.

Step 3: Argue with *Ramsey theory* that the set of graphs corresponding to the same proof includes a very *structured* set of graphs (called a sunflower).

Step 4: If a QCMA algorithm existed, then there is a BQP algorithm for just the sunflower. Prove this is impossible using a combination of the *polynomial and adversary* methods (~30 page proof).

Future directions

- How can we remove the distributions from the oracle separations of QCMA and QMA?
- Can we use the techniques to prove oracle separations for other quantum complexity classes such as QMA(2) and QMA?
- What does the problem say about the quantum probabilistically checkable proofs conjecture and the inapproximability problem for local Hamiltonians?
- Does this oracle improve the hardness of search-to-decision impossibility results for QMA?

Thank you for listening.

Chinmay Nirkhe (IBM Quantum Cambridge) and Anand Natarajan (MIT)

IBM