Separating QMA from QCMA with a classical oracle

John Bostanci, Jonas Haferkamp, Chinmay Nirkhe, and Mark Zhandry

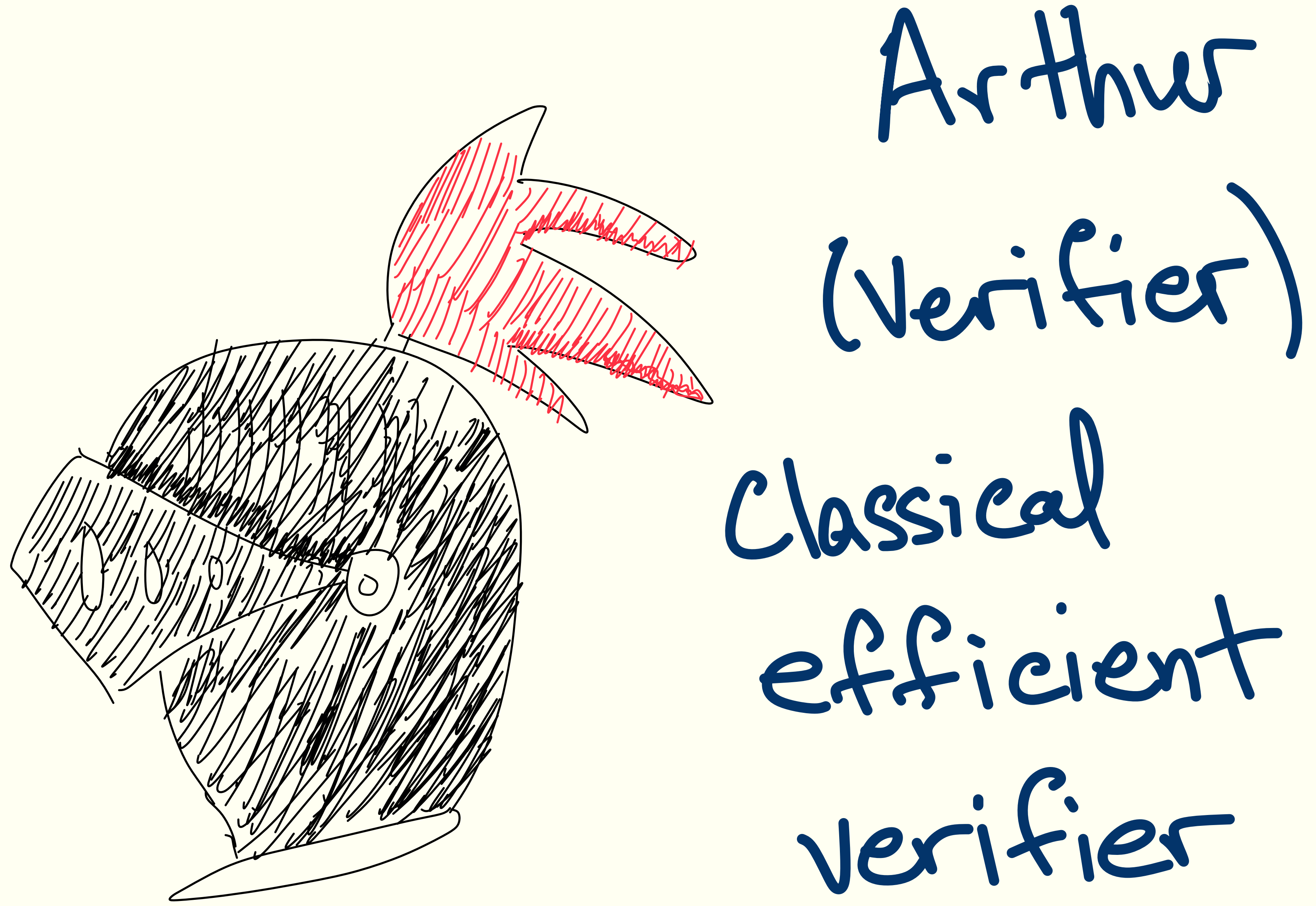
Chicago junior theorists workshop, 2025

How do model the power of proofs?

In complexity theory, the class NP captures the kinds of problems that we hope to be able to prove to one another.

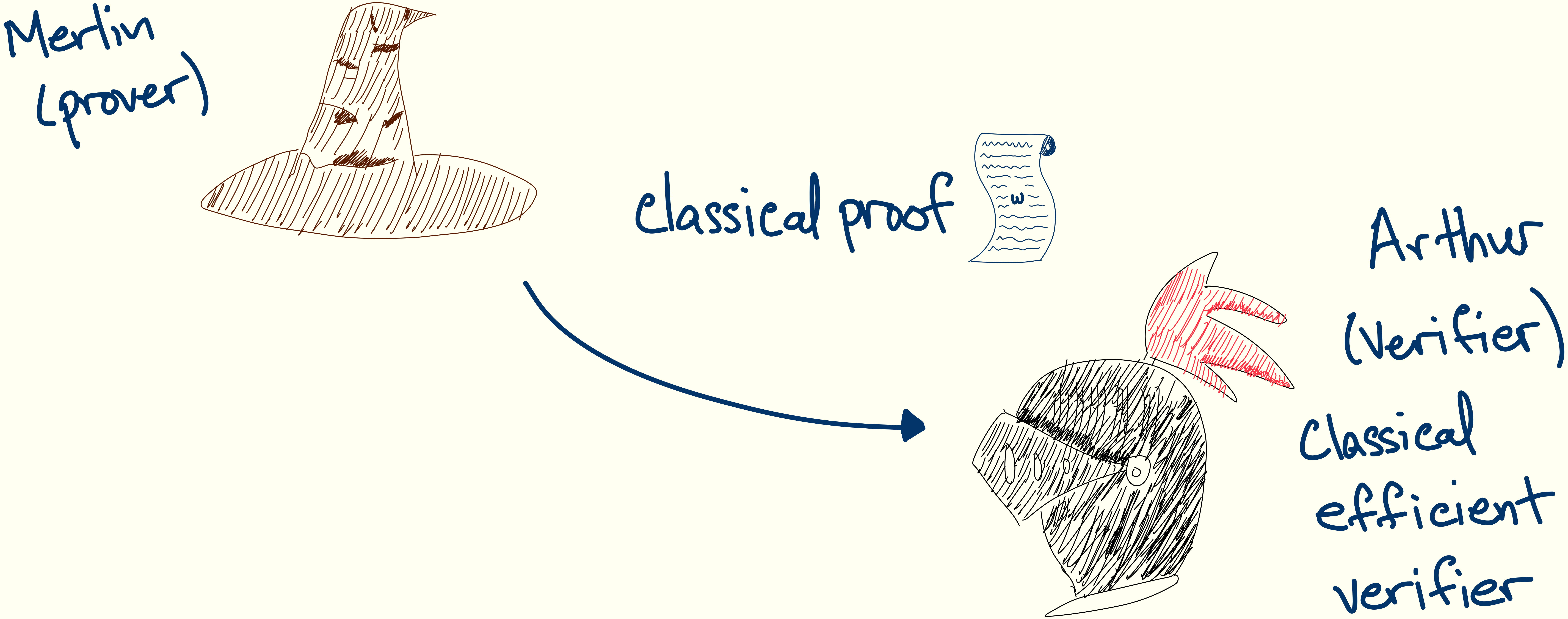
How do model the power of proofs?

In complexity theory, the class NP captures the kinds of problems that we hope to be able to prove to one another.

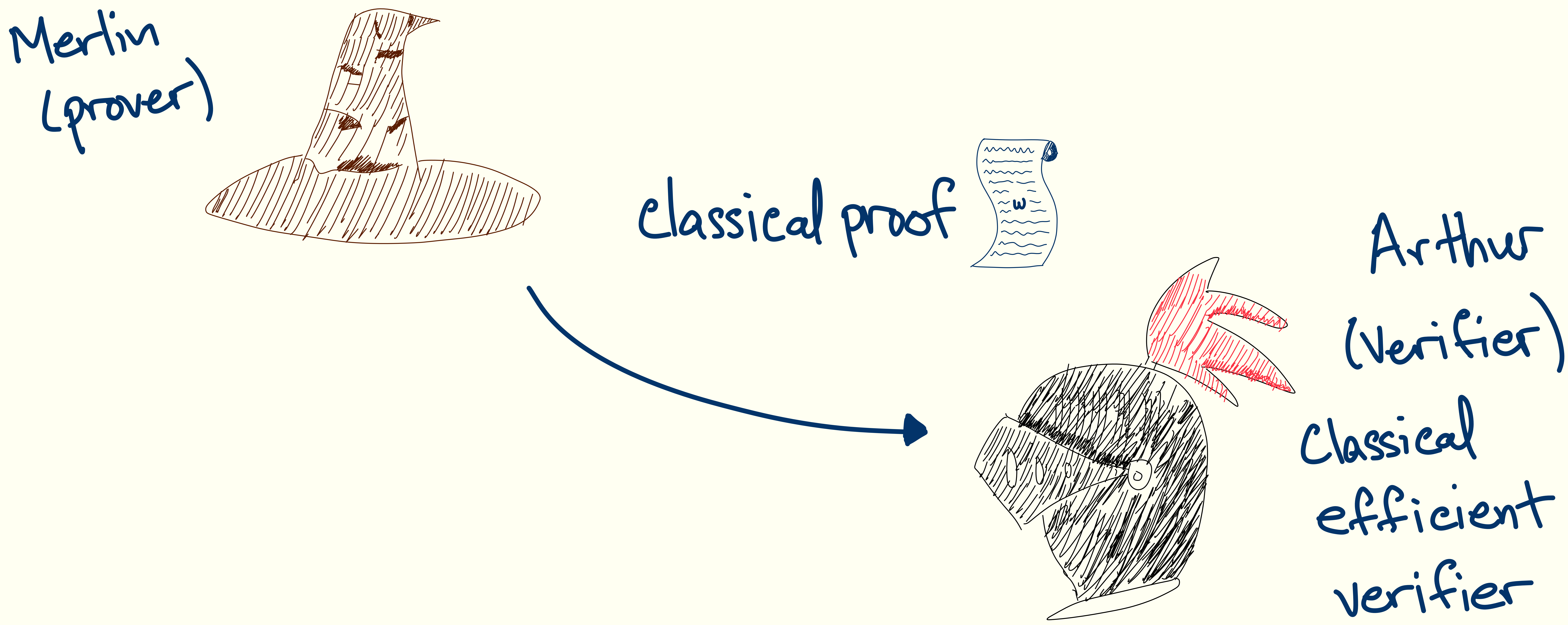


How do model the power of proofs?

In complexity theory, the class NP captures the kinds of problems that we hope to be able to prove to one another.

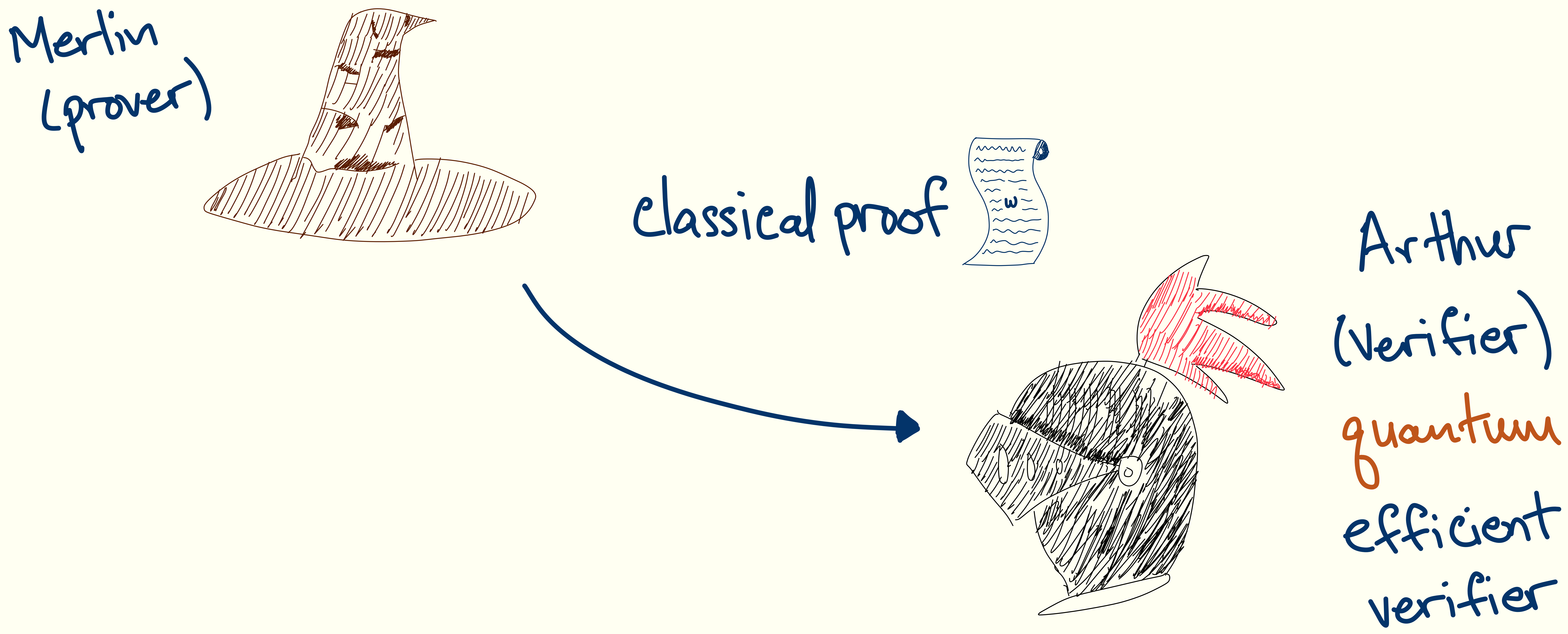


How do model the power of quantum proofs?



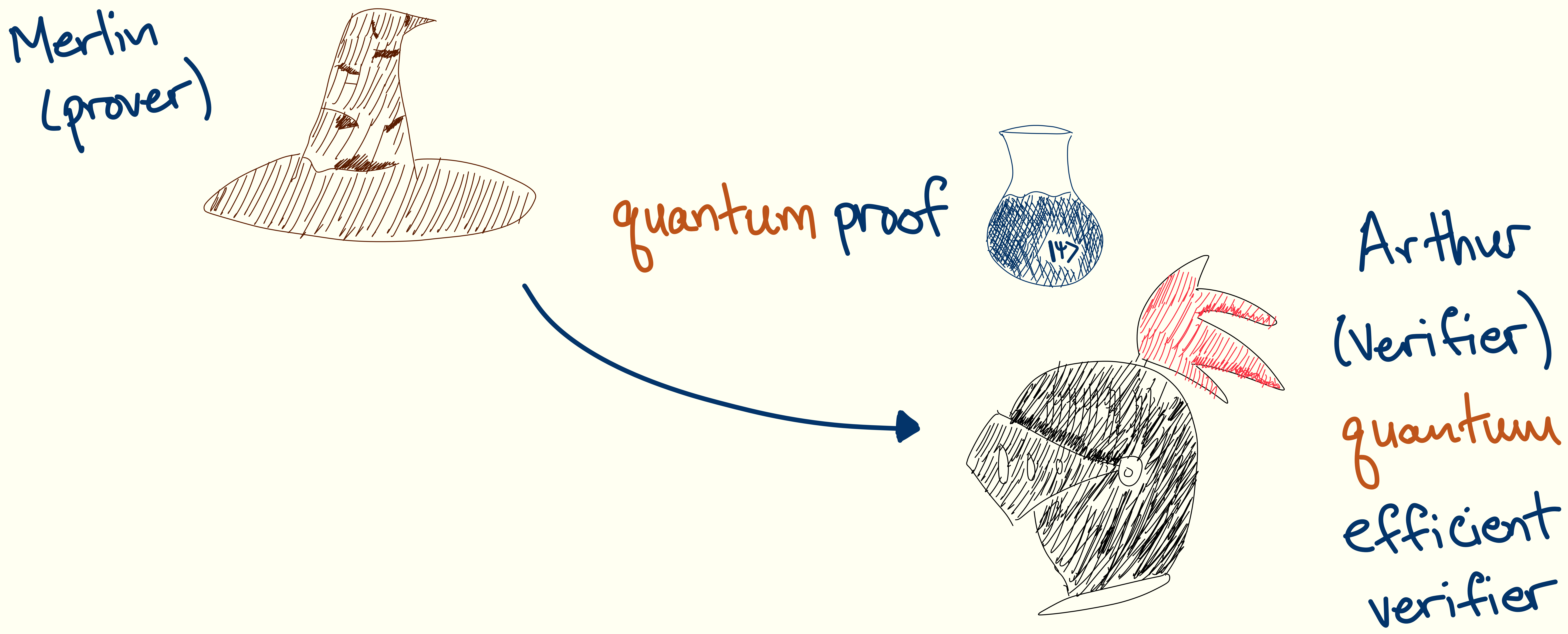
How do model the power of quantum proofs?

With quantum computers, we can compare the relative powers of quantum proofs and classical proofs. QCMA captures the kinds of problems we could prove classically.

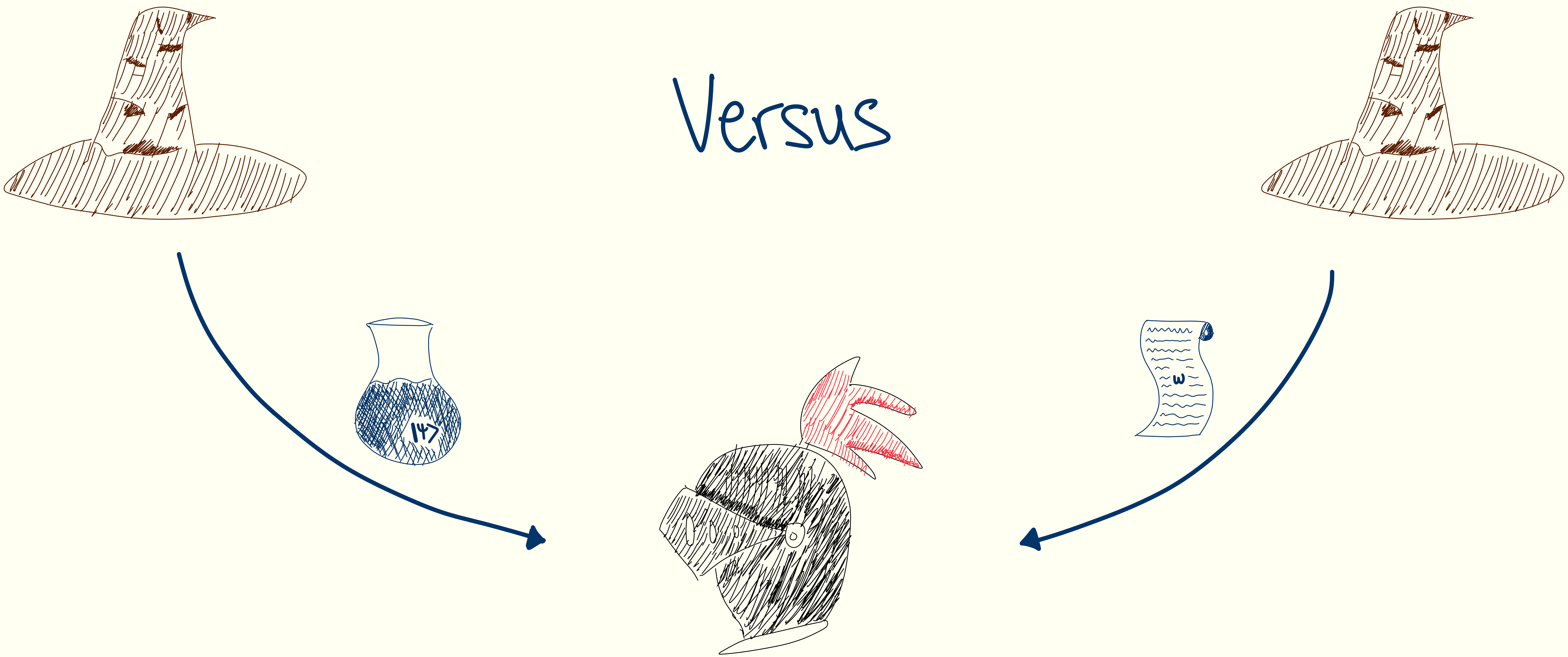


How do model the power of quantum proofs?

With quantum computers, we can compare the relative powers of quantum proofs and classical proofs. QMA captures the kinds of problems we could prove quantumly.



Is QMA = QCMA? [AN'02]



Why care about QMA **versus** QCMA**?**

To me, the outcome would be surprising either way!

Why care about QMA versus QCMA?

To me, the outcome would be surprising either way!

If QCMA = QMA, then anything you could verify about a quantum state could be written down as a classical string!

Why care about QMA versus QCMA?

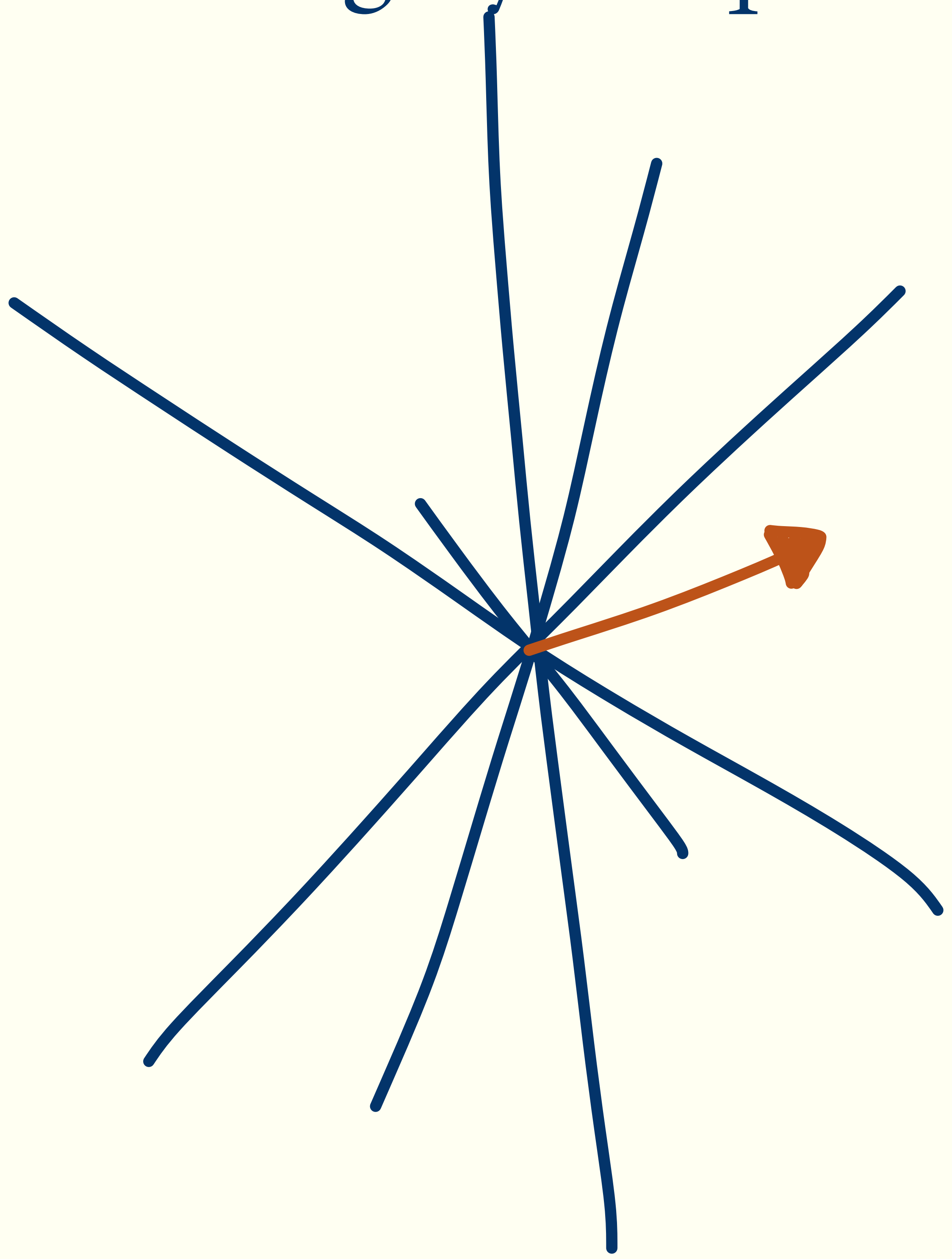
To me, the outcome would be surprising either way!

If QCMA = QMA, then anything you could verify about a quantum state could be written down as a classical string!

Otherwise, there must be something interesting you could verify about a quantum state that you can only learn from having a copy of the state!

A quantum oracle separation [AK'06]

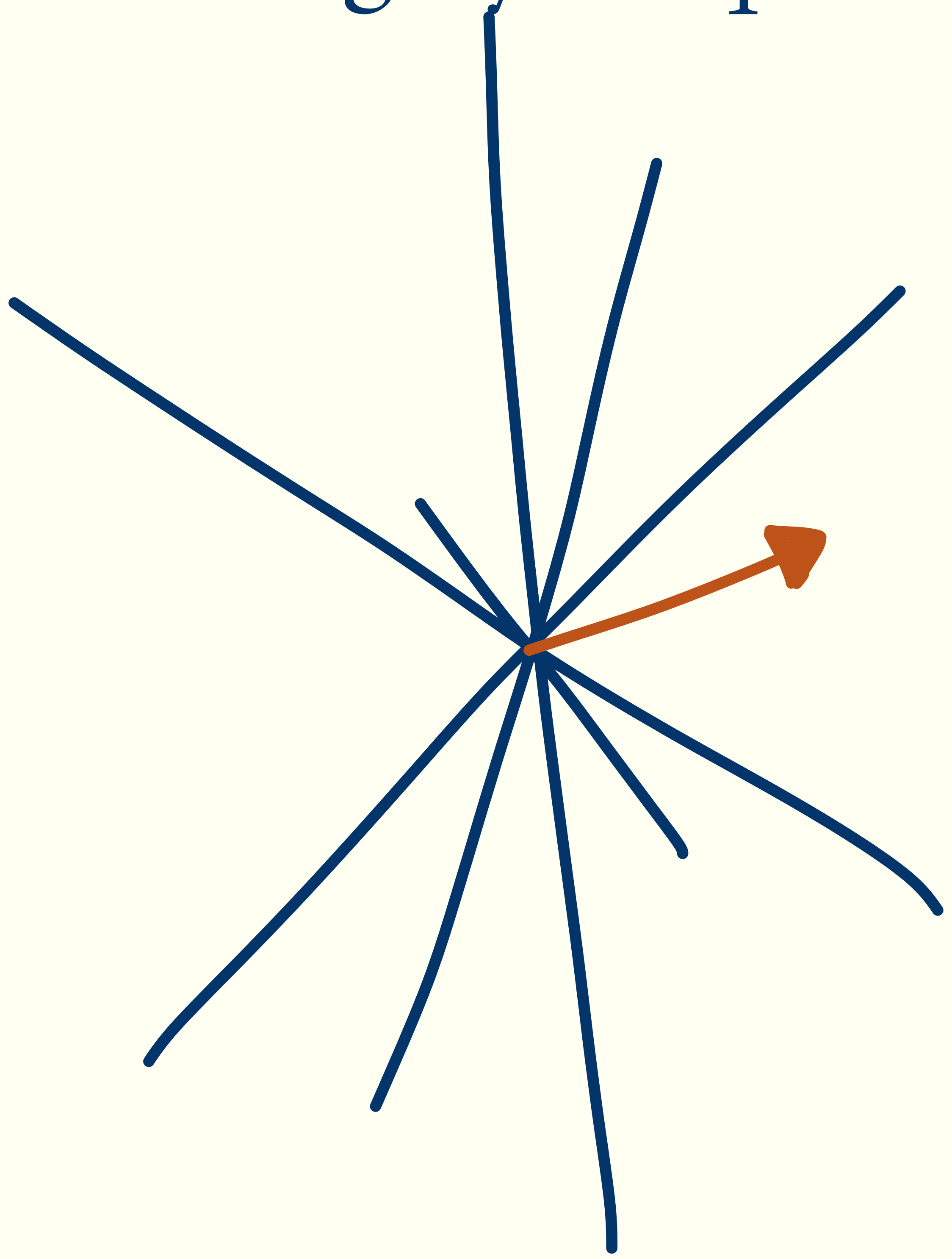
Recall: A quantum state on n-qubits is a vector of 2^n complex numbers
→ there are roughly 2^{2^n} quantum states on n-qubits.



$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

A quantum oracle separation [AK'06]

Recall: A quantum state on n-qubits is a vector of 2^n complex numbers
→ there are roughly 2^{2^n} quantum states on n-qubits.

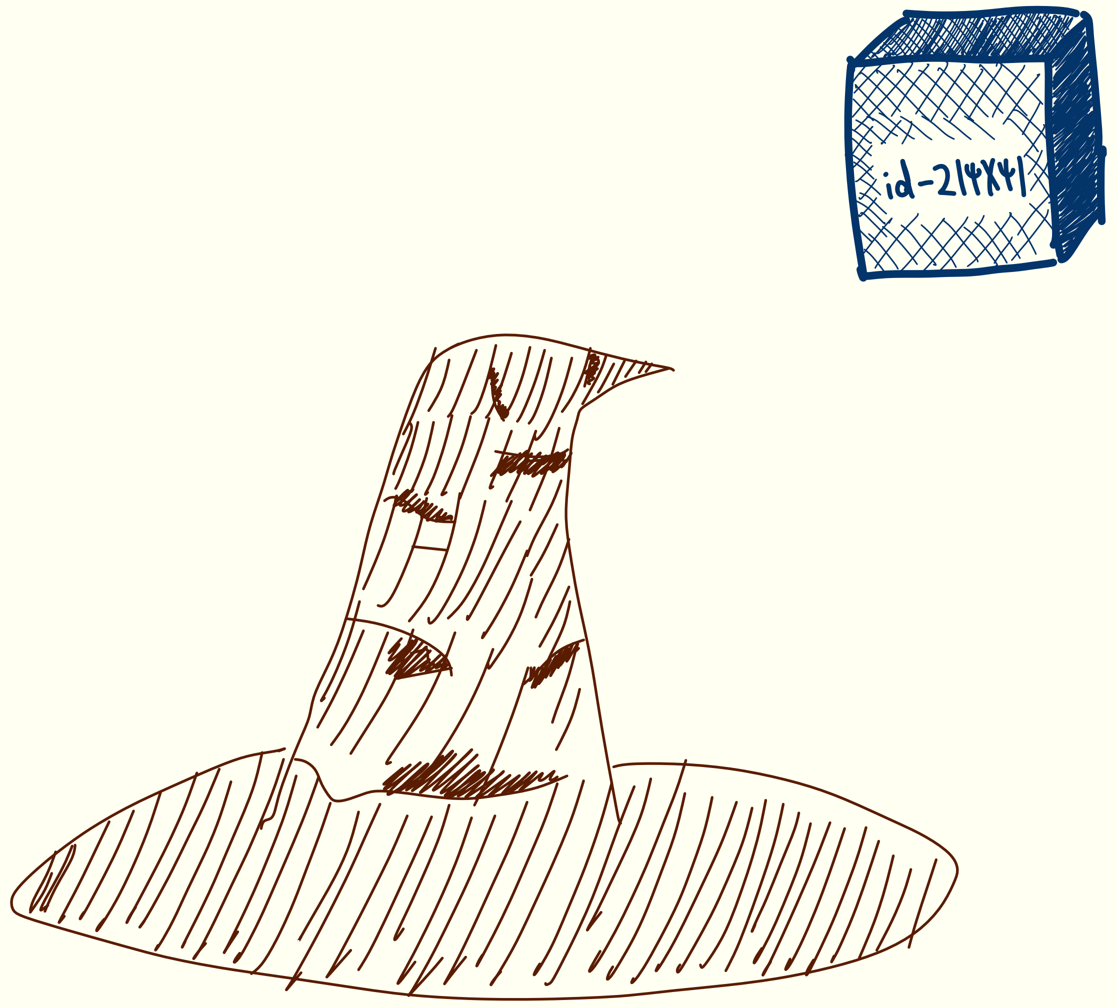


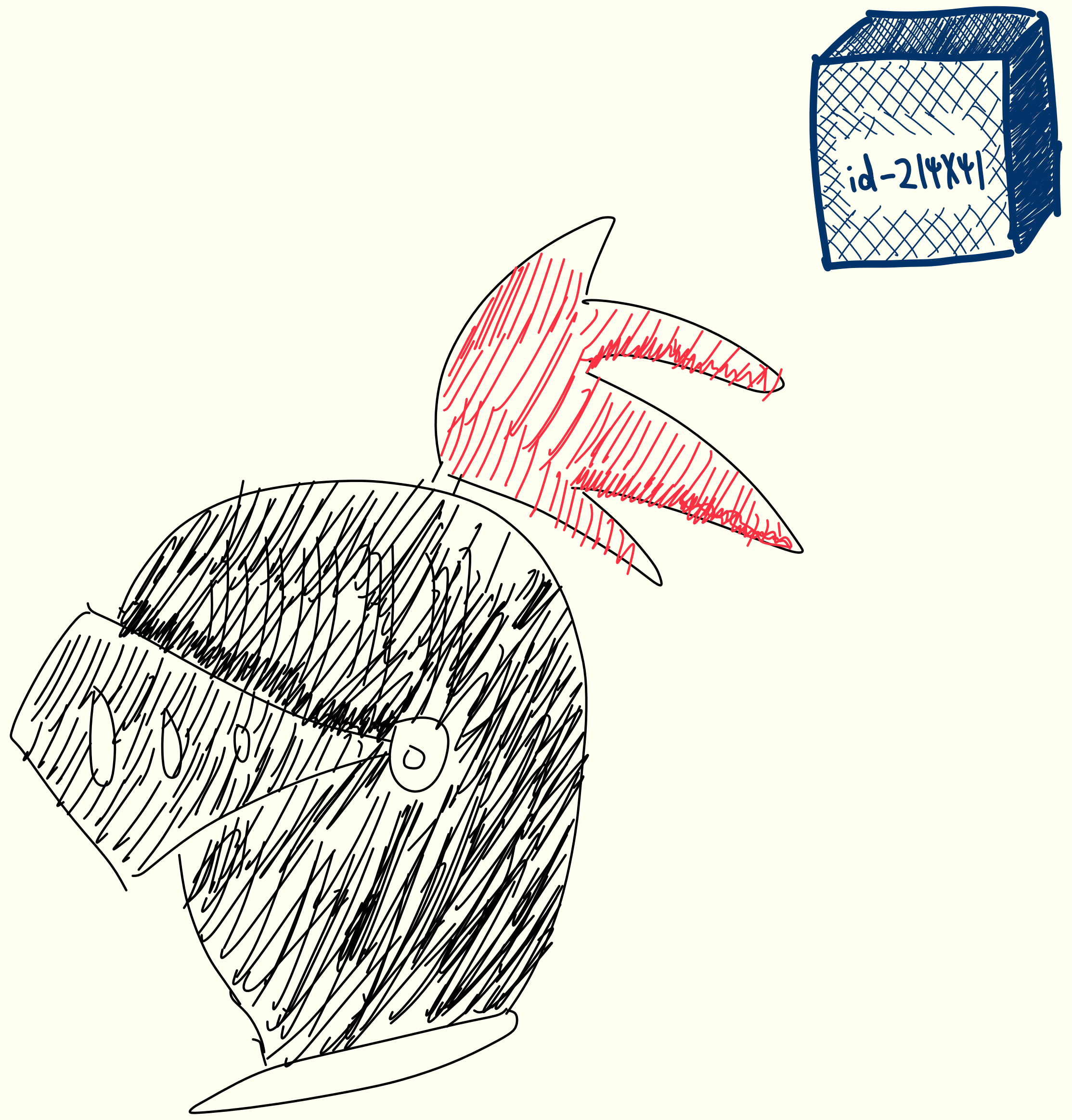
$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Concentration: Any collection of $2^{\mathrm{poly}(n)}$ states will fail to be close to a random state!

A quantum oracle separation [AK'06]

Claim: Oracle that accepts a random state (or nothing) separates QMA from QCMA.

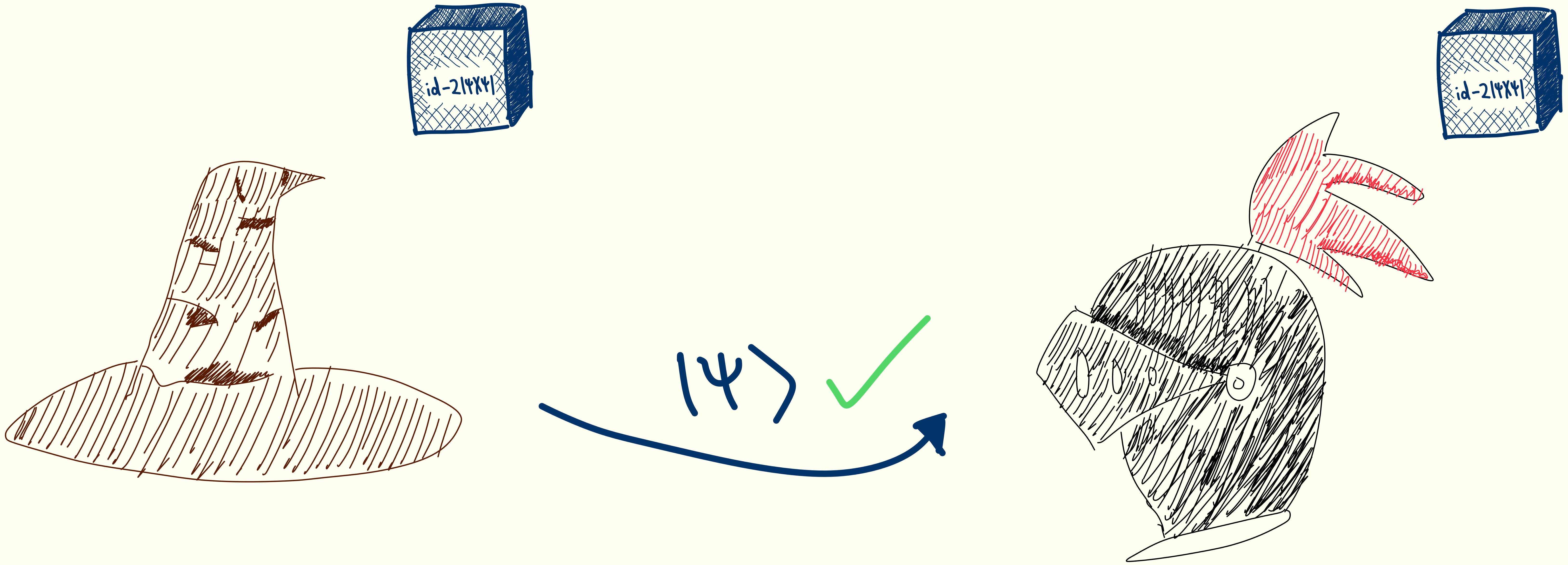




A quantum oracle separation [AK'06]

Claim: Oracle that accepts a random state (or nothing) separates QMA from QCMA.

→ A QMA prover can send a copy of $|\psi\rangle$.

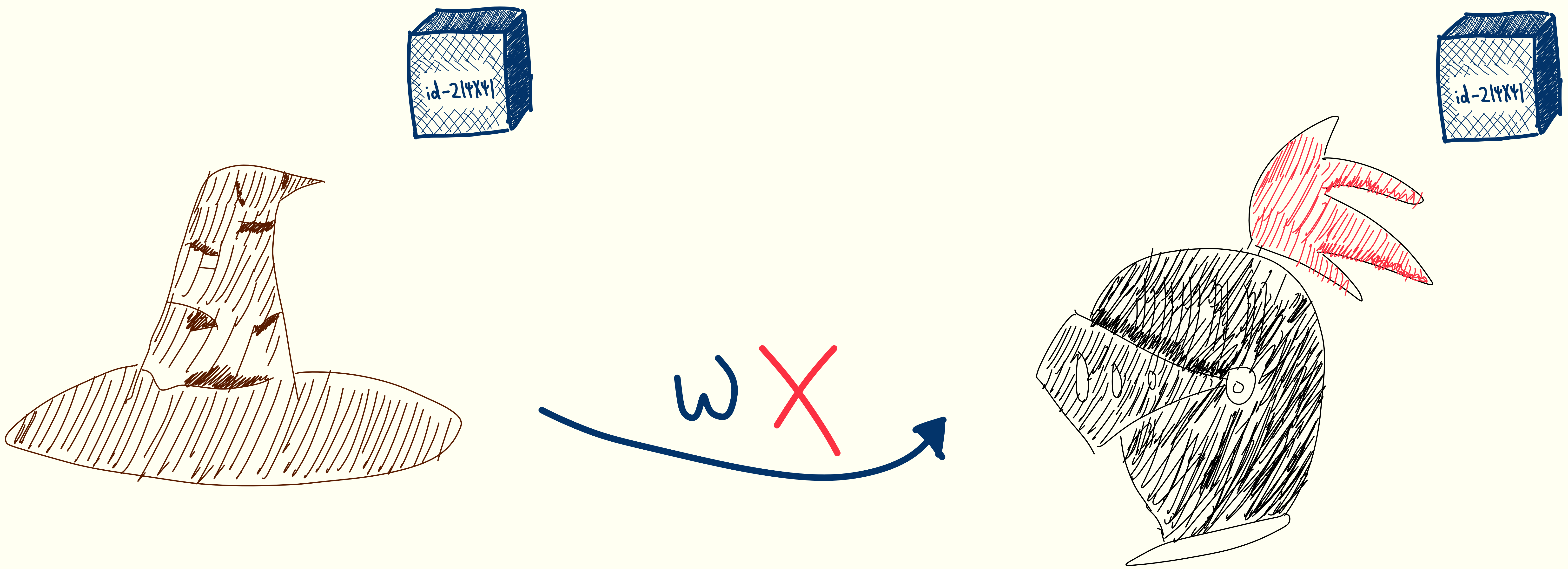


A quantum oracle separation [AK'06]

Claim: Oracle that accepts a random state (or nothing) separates QMA from QCMA.

→ A QMA prover can send a copy of $|\psi\rangle$.

→ Any QCMA verifier will only be able to check $2^{\text{poly}(n)}$ different quantum states. For almost all random states, it won't be able to check.



A classical oracle separation?

A classical oracle separation?

The AK'06 oracle is, in some ways, too powerful: Even if the adversary trusts the prover, they can't find an input to the oracle for which it isn't identity!

A classical oracle separation?

The AK'06 oracle is, in some ways, too powerful: Even if the adversary trusts the prover, they can't find an input to the oracle for which it isn't identity!

But for any "classicalization" of this oracle, classical witness can now actually say something about the oracle, so the problem gets a lot more challenging!

History of the QMA **versus** QCMA **problem**

First proposed in ’02 by
Aharanov and Naveh.

‘02 ‘25

History of the QMA versus QCMA problem

First proposed in '02 by
Aharanov and Naveh.

Aaronson & Kuperberg '06:
Quantum oracle separation.
Each $\mathcal{O}_n = \mathrm{id} - 2|\psi_n\rangle\langle\psi_n|$

'02 '25

History of the QMA versus QCMA problem

First proposed in '02 by **Aharanov and Naveh.**

Aaronson & Kuperberg '06:
Quantum oracle separation.
Each $\mathcal{O}_n = \mathrm{id} - 2|\psi_n\rangle\langle\psi_n|$

'02 —— '25

Lutomirski '11: Proposed the expander mixing problem as a candidate classical oracle separation.

History of the QMA versus QCMA problem

First proposed in '02 by **Aharanov and Naveh.**

Aaronson & Kuperberg '06: Quantum oracle separation. Each $\mathcal{O}_n = \mathrm{id} - 2|\psi_n\rangle\langle\psi_n|$

Fefferman & Kimmel '15: In-place permutation oracle. Problem corresponds to set size estimation.

'02 ——— '25

Lutomirski '11: Proposed the expander mixing problem as a candidate classical oracle separation.

History of the QMA versus QCMA problem

First proposed in '02 by **Aharanov and Naveh.**

Aaronson & Kuperberg '06: Quantum oracle separation. Each $\mathcal{O}_n = \text{id} - 2|\psi_n\rangle\langle\psi_n|$

Fefferman & Kimmel '15: In-place permutation oracle. Problem corresponds to set size estimation.

Natarajan & Nirkhe '22: Distribution testing oracle. Problem corresponds to size estimation of an expander graph.

Li, Liu, Pelecanos, Yamakawa '23: Separation assuming only classical queries. Based on "Verifiable Quantum Advantage without Structure".

'02 —————————————————————— '25

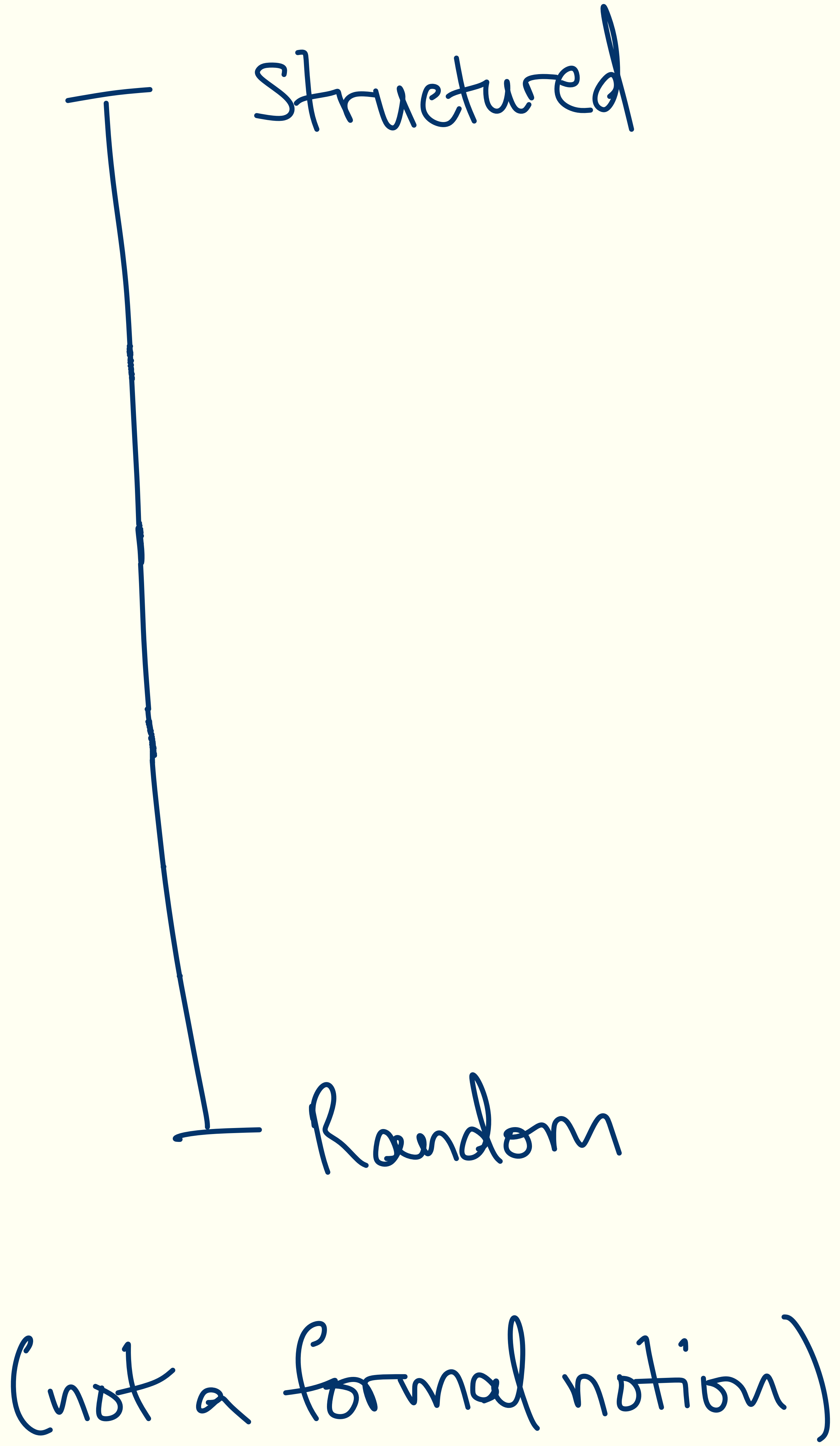
Lutomirski '11: Proposed the expander mixing problem as a candidate classical oracle separation.

Ben-David & Kundu '24: Bounded adaptivity, based on "Verifiable Quantum Advantage without Structure".

Liu, Mutreja, Yuen '25: Aaronson-Ambainis-like conjecture implies QMA QCMA separation. Problem corresponds to size estimation of an expander graph.

Why is this problem so hard?

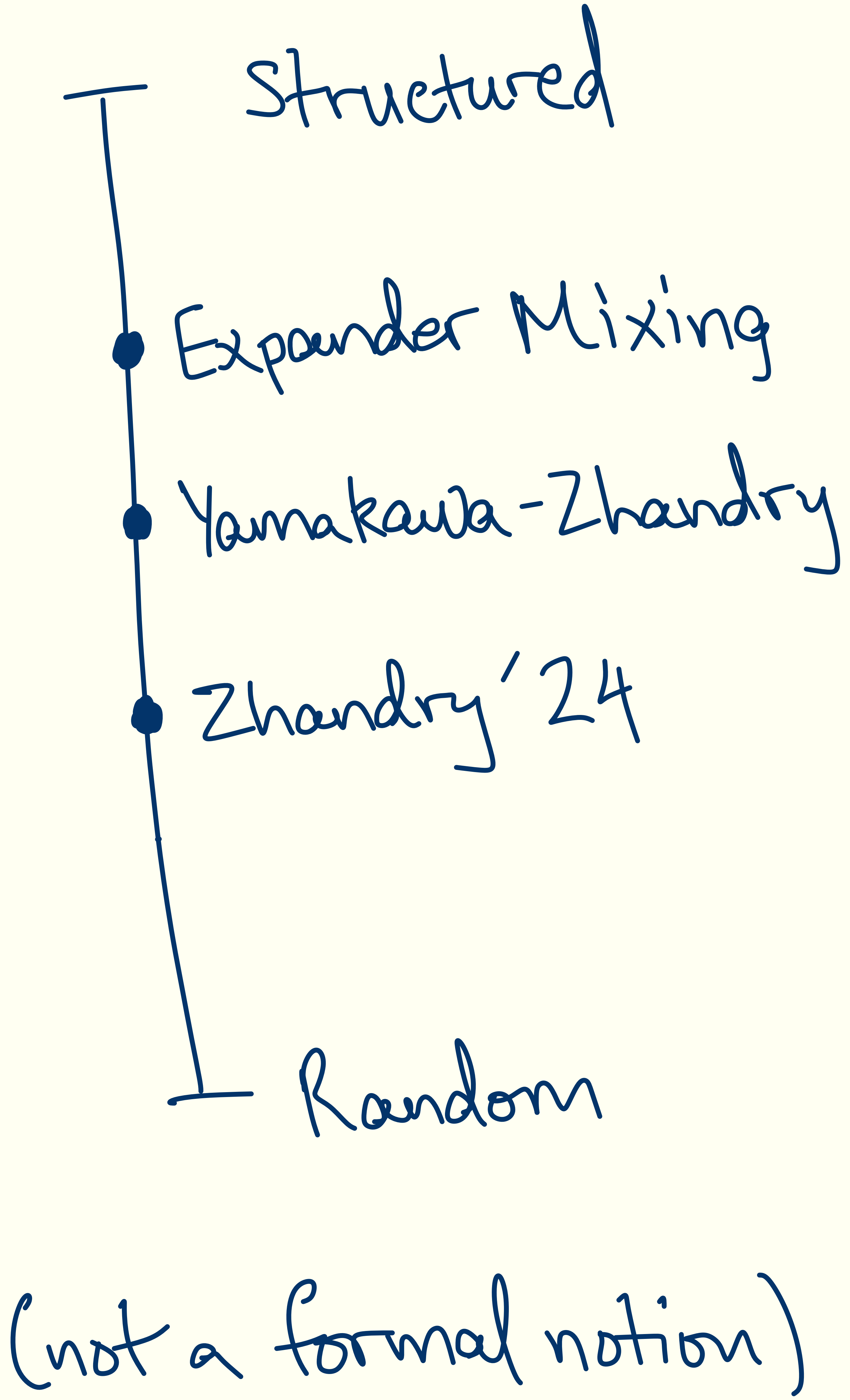
To me, the problem has been "stuck" in between two competing desires for a while.



Why is this problem so hard?

To me, the problem has been "stuck" in between two competing desires for a while.

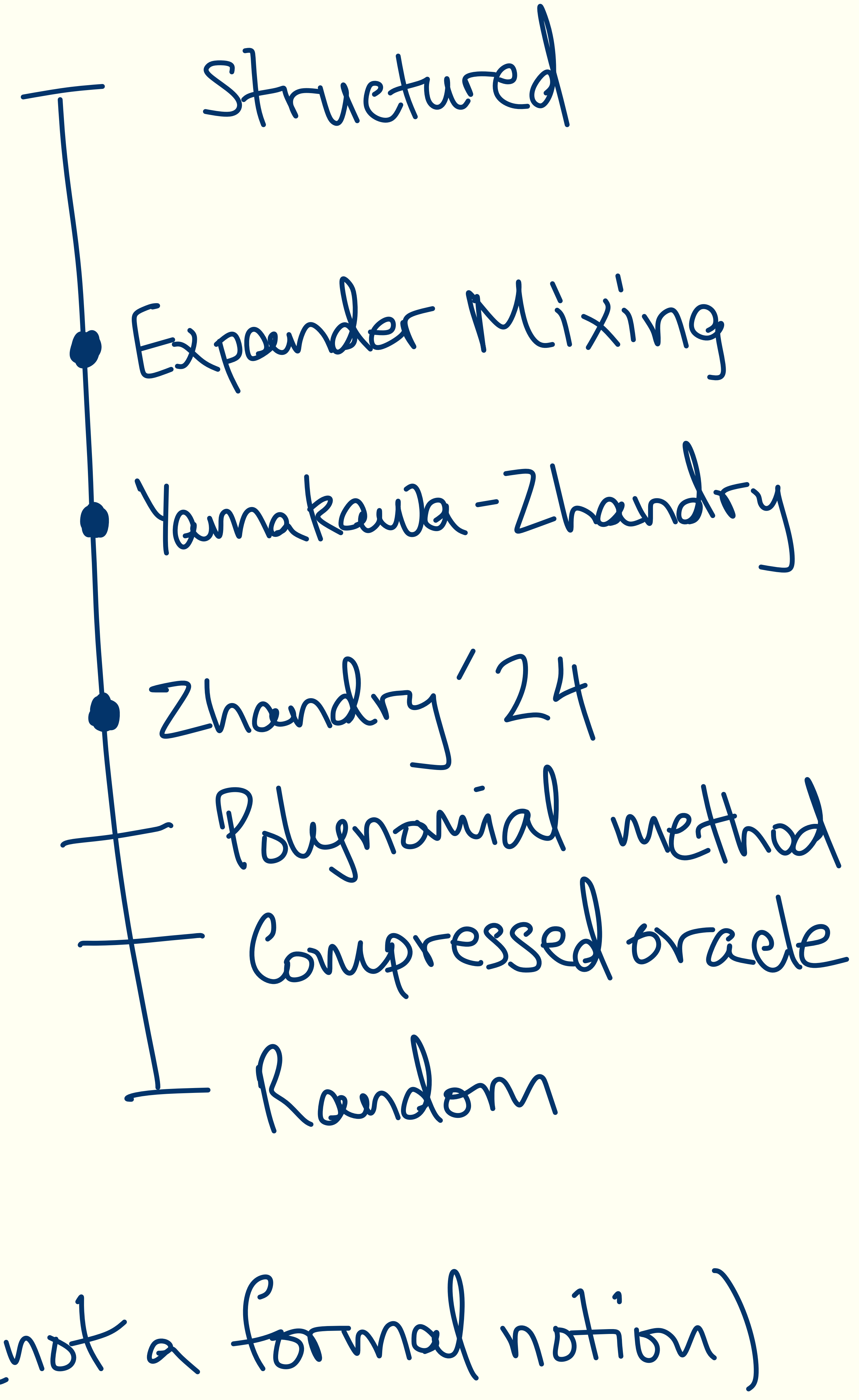
- In any separation, the QMA must do more than just measure their quantum state
  → The oracle should have some hidden global structure that is "visible" to a quantum proof.



Why is this problem so hard?

To me, the problem has been "stuck" in between two competing desires for a while.

- In any separation, the QMA must do more than just measure their quantum state
  → The oracle should have some hidden global structure that is "visible" to a quantum proof.
- But, quantum lower bound techniques usually take advantage of the randomness of the oracle.
  → Need a new technique for analyzing some kind of structured classical oracles.

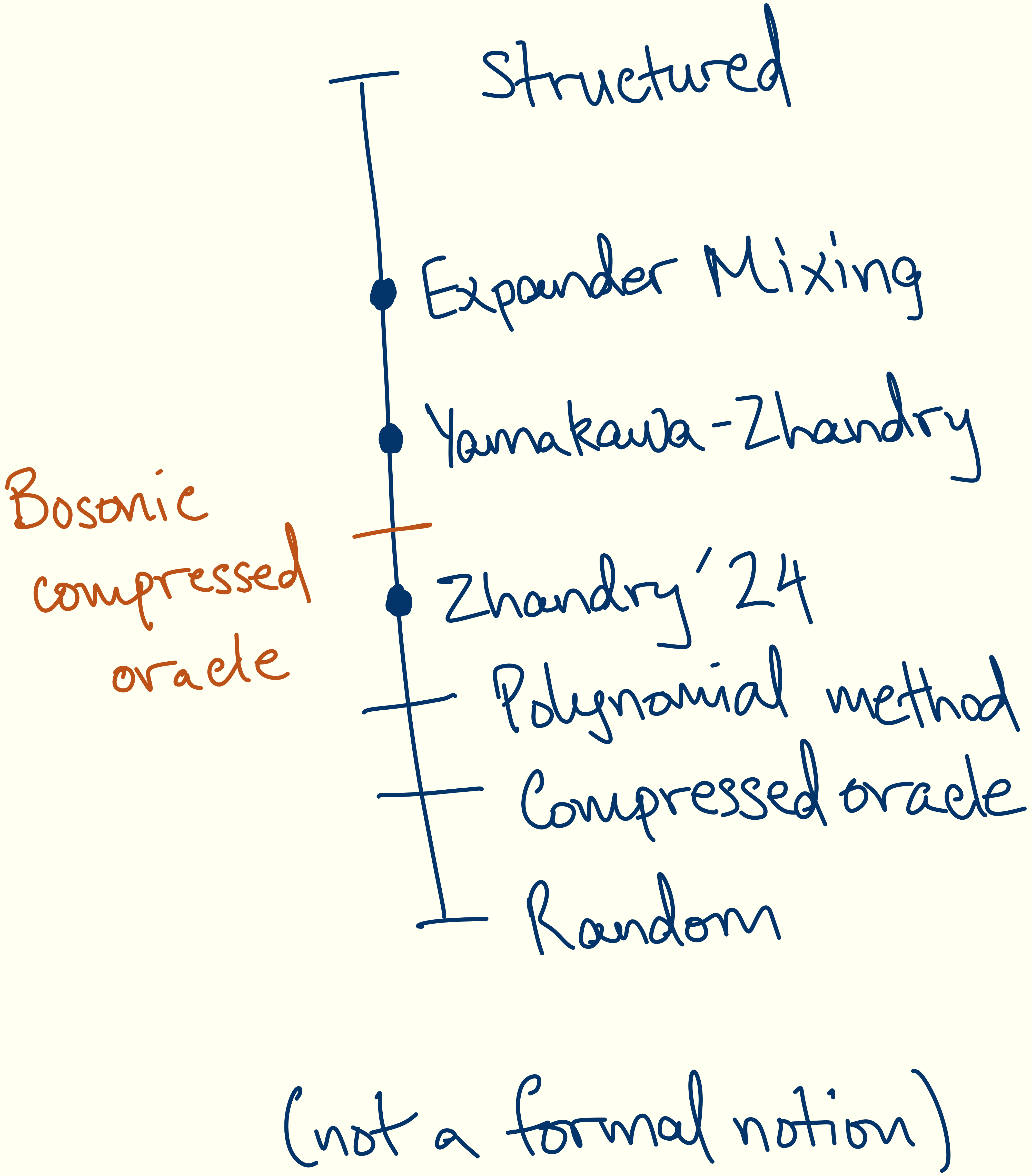


Why is this problem so hard?

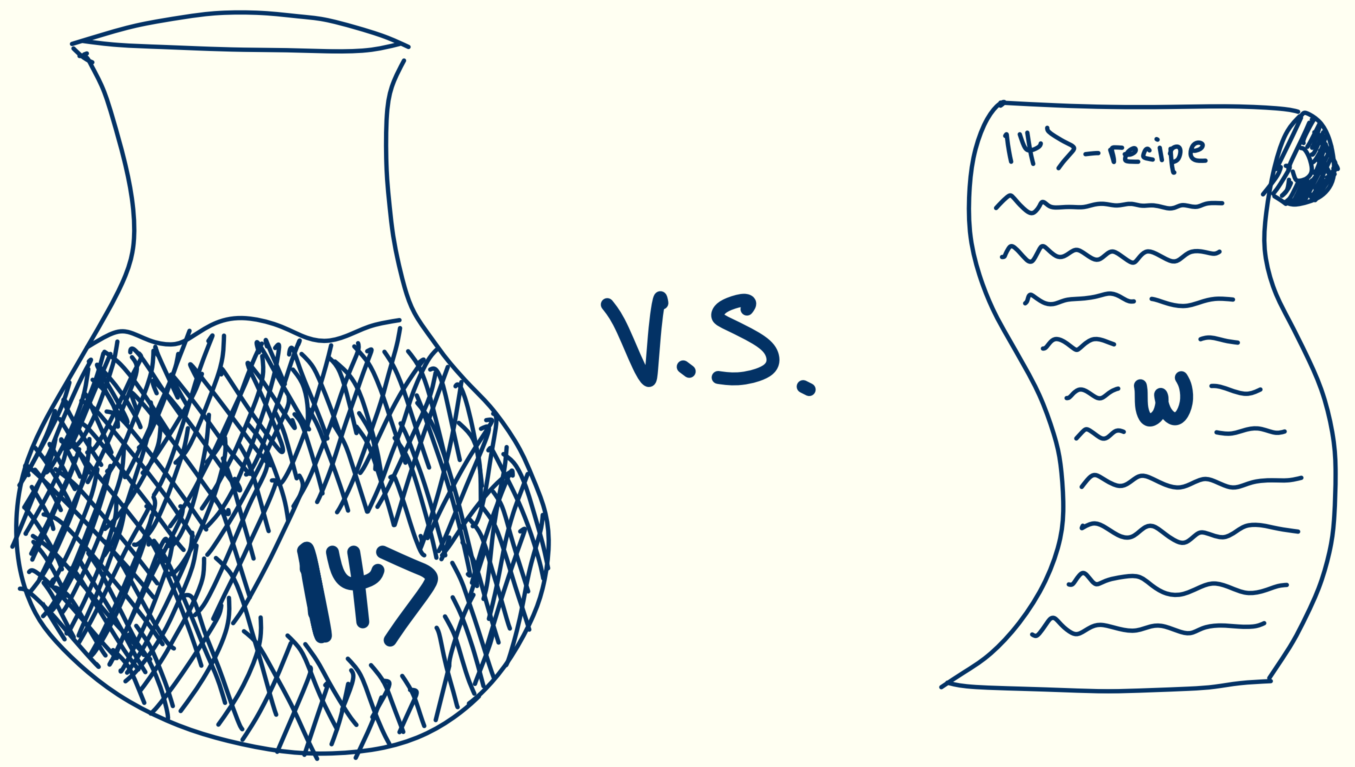
To me, the problem has been “stuck” in between two competing desires for a while.

- In any separation, the QMA must do more than just measure their quantum state
  → The oracle should have some hidden global structure that is “visible” to a quantum proof.
- But, quantum lower bound techniques usually take advantage of the randomness of the oracle.
  → Need a new technique for analyzing some kind of structured classical oracles.

Our paper bridges the gap, taking the less structured oracle of Zhandry’24, and introducing new analysis to understand Fourier-related sets.



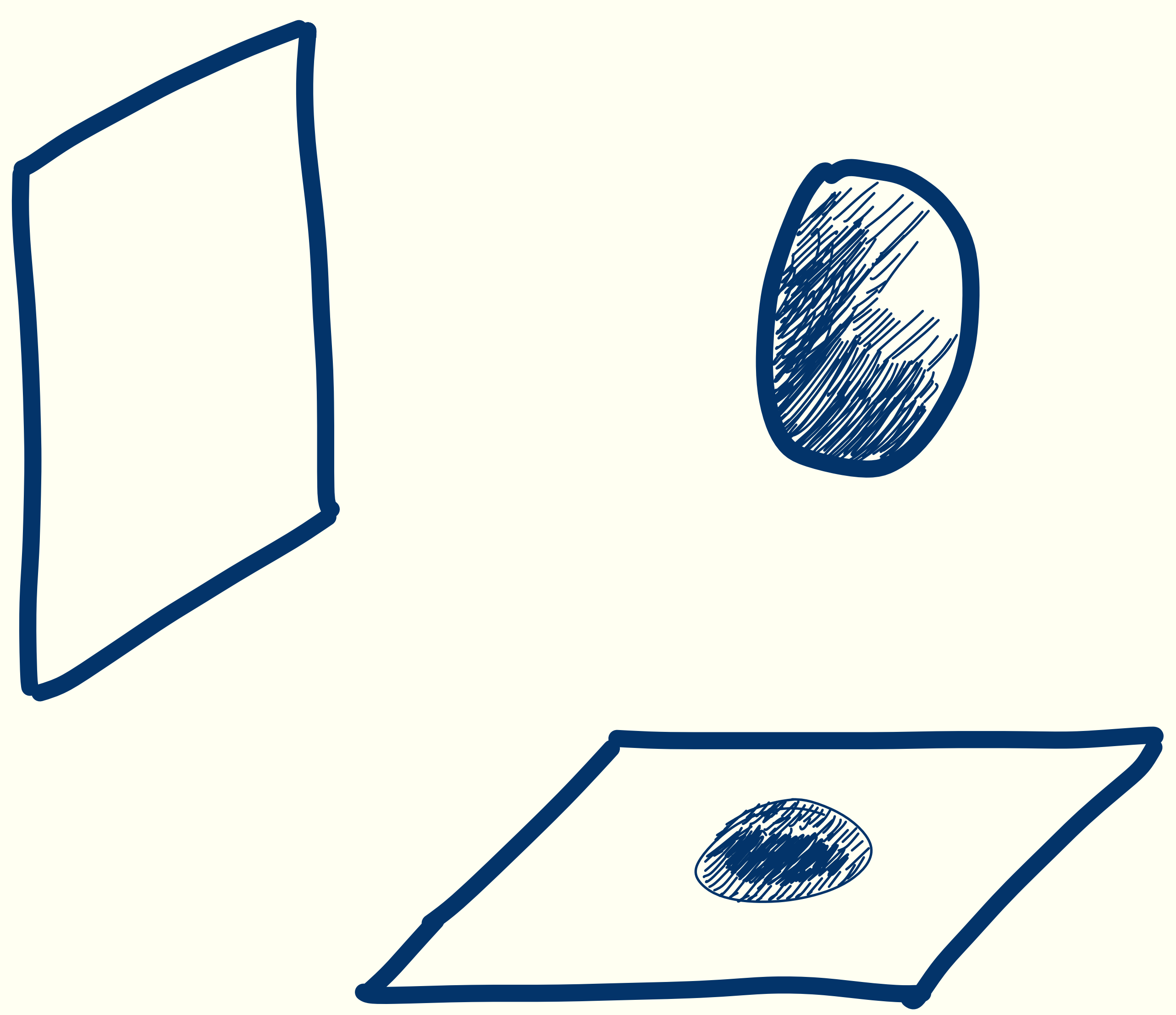
We prove that there is a classical oracle relative to which QMA $\neq$ QCMA



Computing in two bases

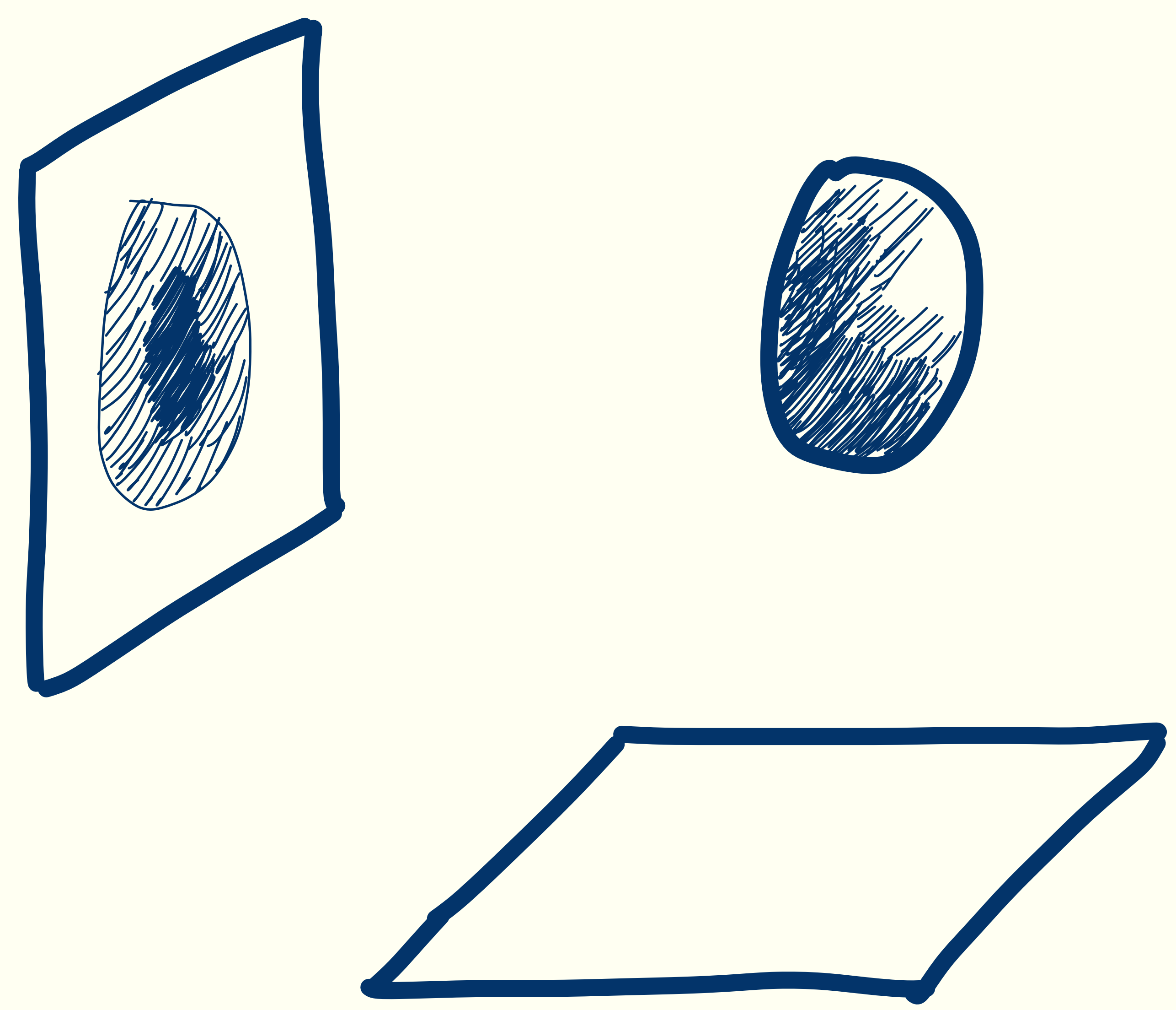
Quantum states can be viewed from one of two bases:

Position (Standard)



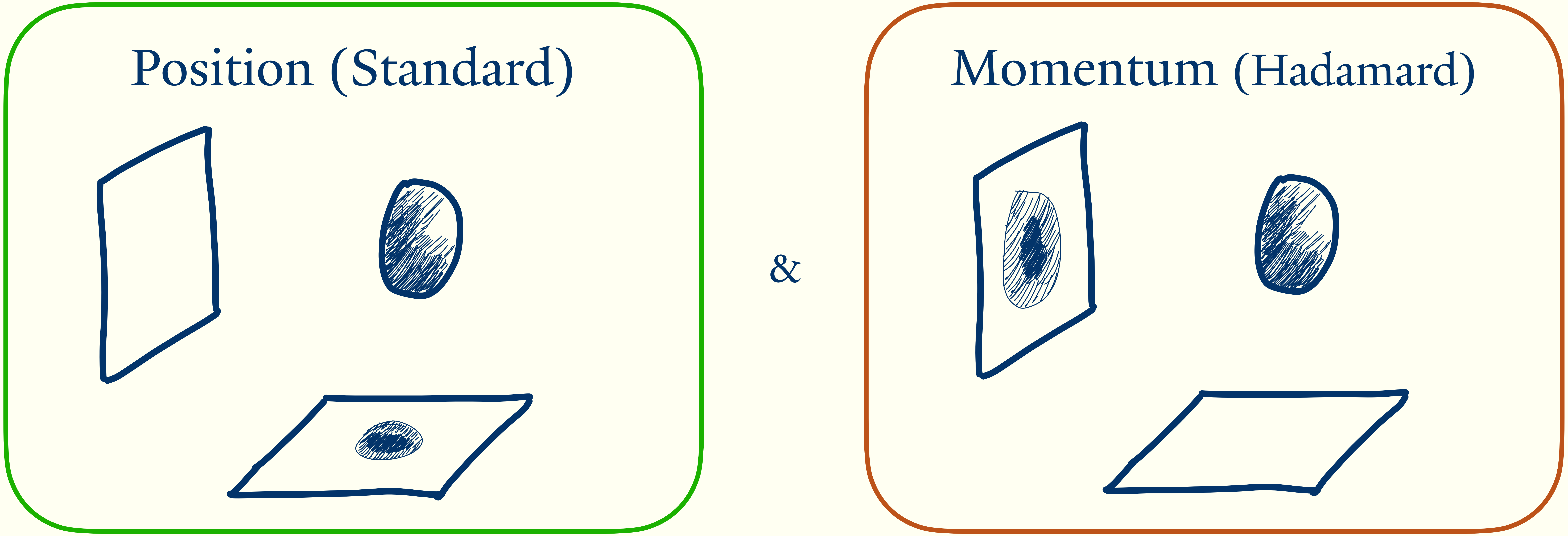
&

Momentum (Hadamard)



Computing in two bases

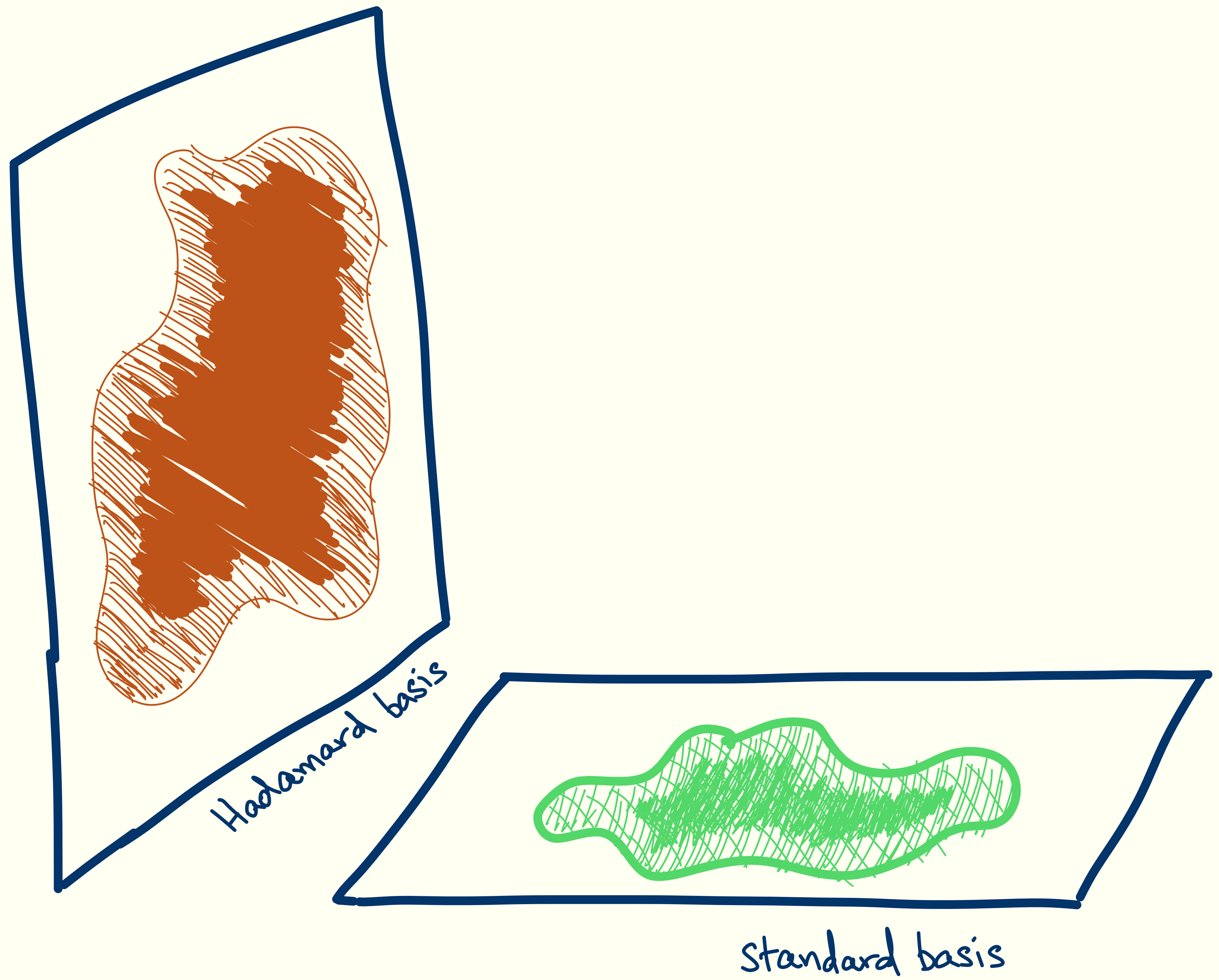
Quantum states can be viewed from one of two bases:



Rough intuition: The "size" of the shadows in the standard and Hadamard basis should multiply to a fixed number for all n-qubit states ($\sim 2^n$).

The spectral Forrelation problem

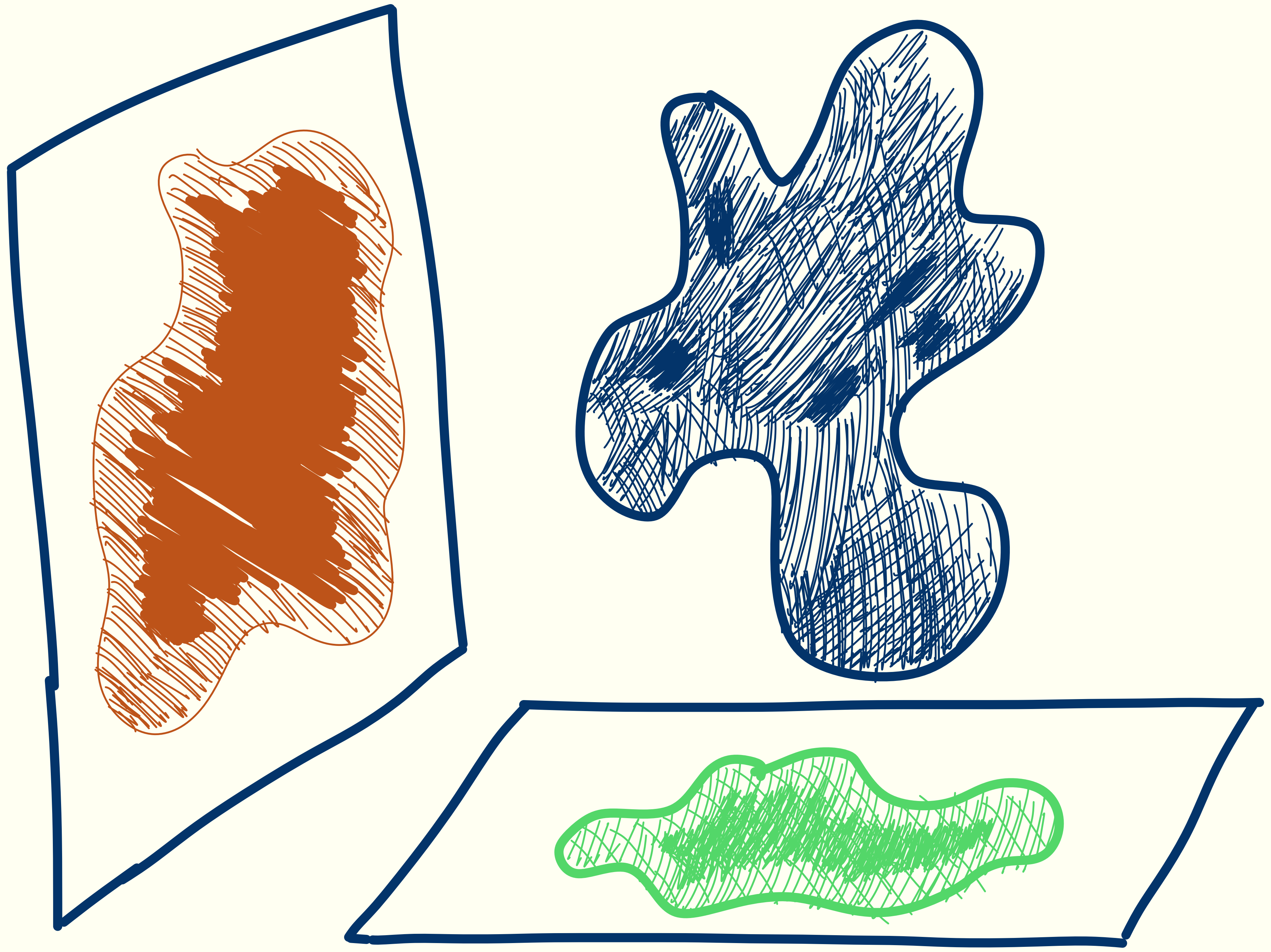
The spectral Forrelation problem is a problem about pairs of sets (S, U), which we treat as oracles through the set membership functions. S~positions, and U~momentums.



The spectral Forrelation problem

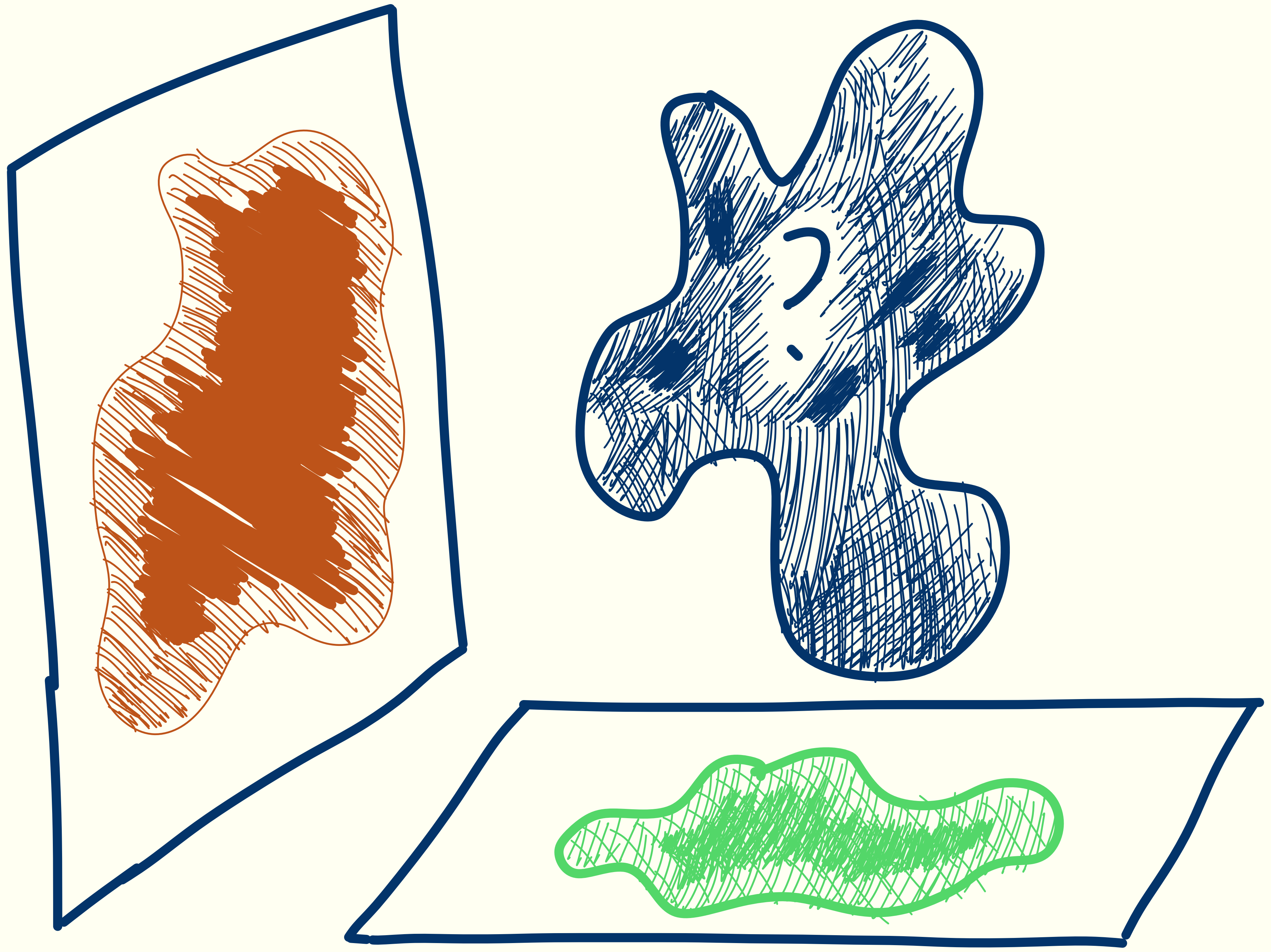
We say that two sets (S, U) are α-spectrally Forrelated if there is a state $|\psi\rangle$ such that

$$\|\Pi_U \cdot H^{\otimes n} \cdot \Pi_S |\psi\rangle\|^2 \geq \alpha$$



The spectral Forrelation problem

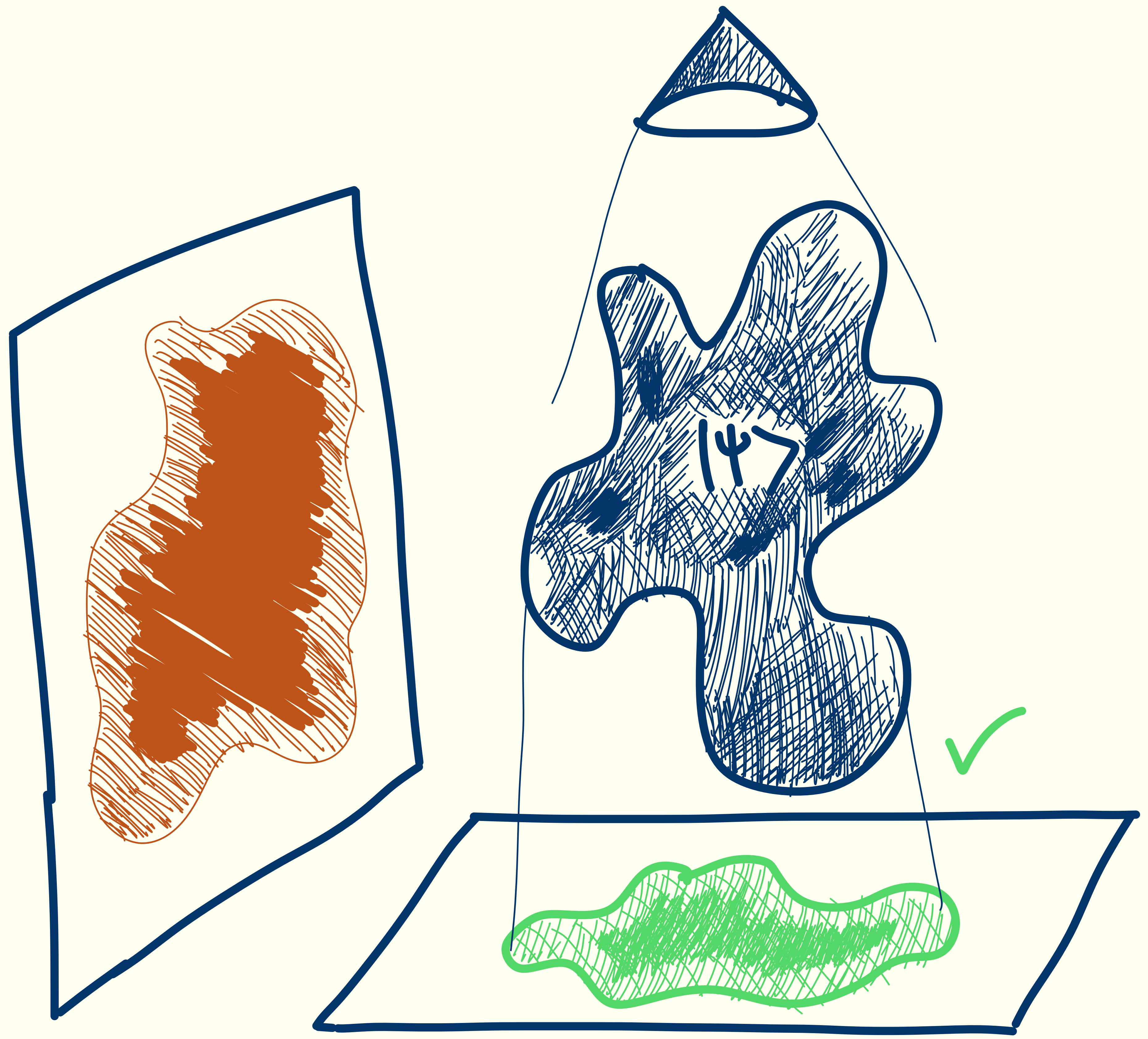
Given oracle access to two sets (S, U) (via set membership functions), determine if there is a state $|\psi\rangle$ such that $\|\Pi_U \cdot H^{\otimes n} \cdot \Pi_S |\psi\rangle\|^2$ is large ($\geq 59/100$) or small ($\leq 57/100$), promised that one of the two is the case.



Spectral Forrelation is in QMA

Given a copy of a state $|\psi\rangle$:

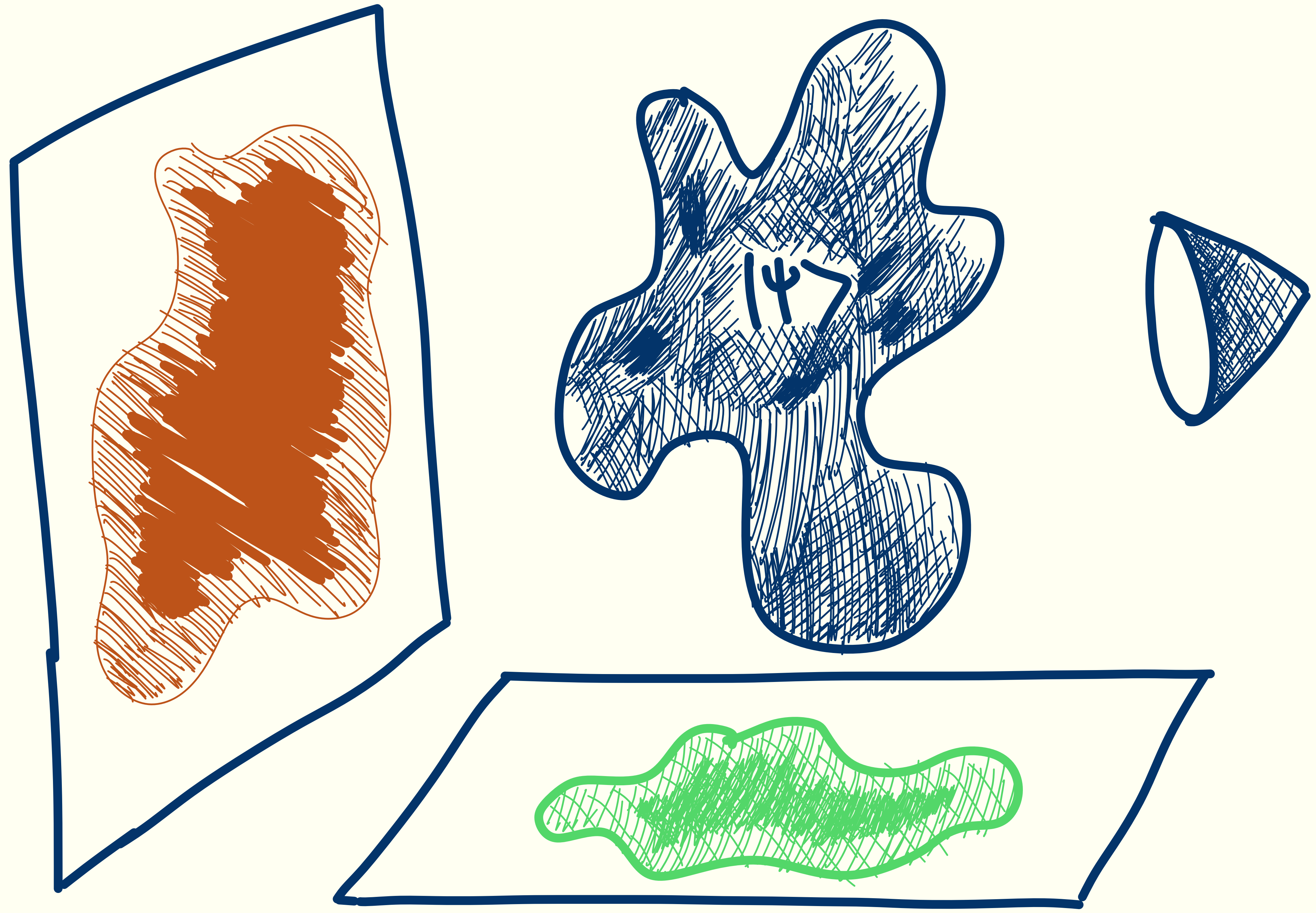
- Use S oracle to measure the POVM $\{\Pi_S, \text{id} - \Pi_S\}$, reject if the outcome is $\text{id} - \Pi_S$.



Spectral Forrelation is in QMA

Given a copy of a state $|\psi\rangle$:

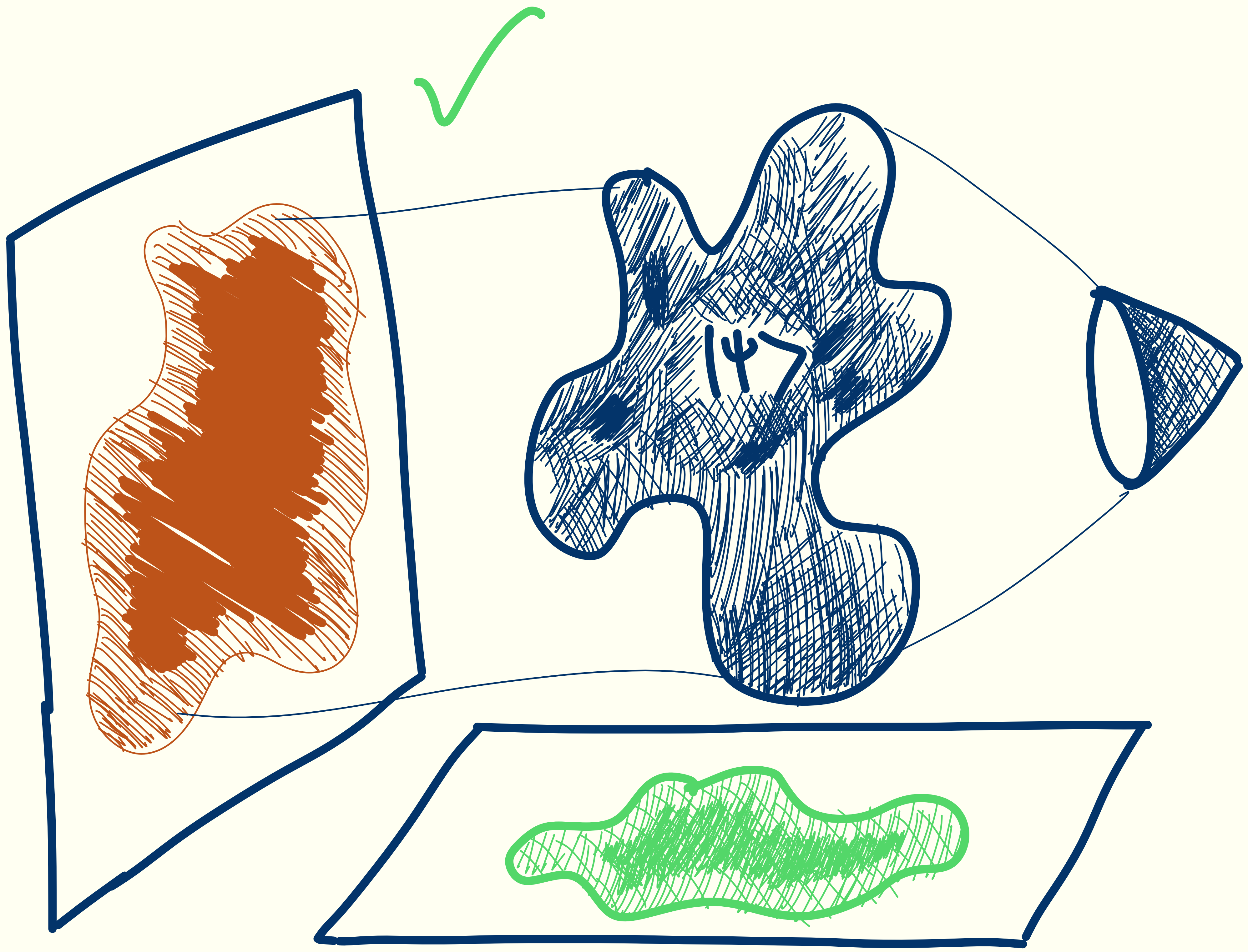
- Use S oracle to measure the POVM $\{\Pi_S, \mathrm{id} - \Pi_S\}$, reject if the outcome is $\mathrm{id} - \Pi_S$.
- Apply $H^{\otimes n}$ to the resulting state.



Spectral Forrelation is in QMA

Given a copy of a state $|\psi\rangle$:

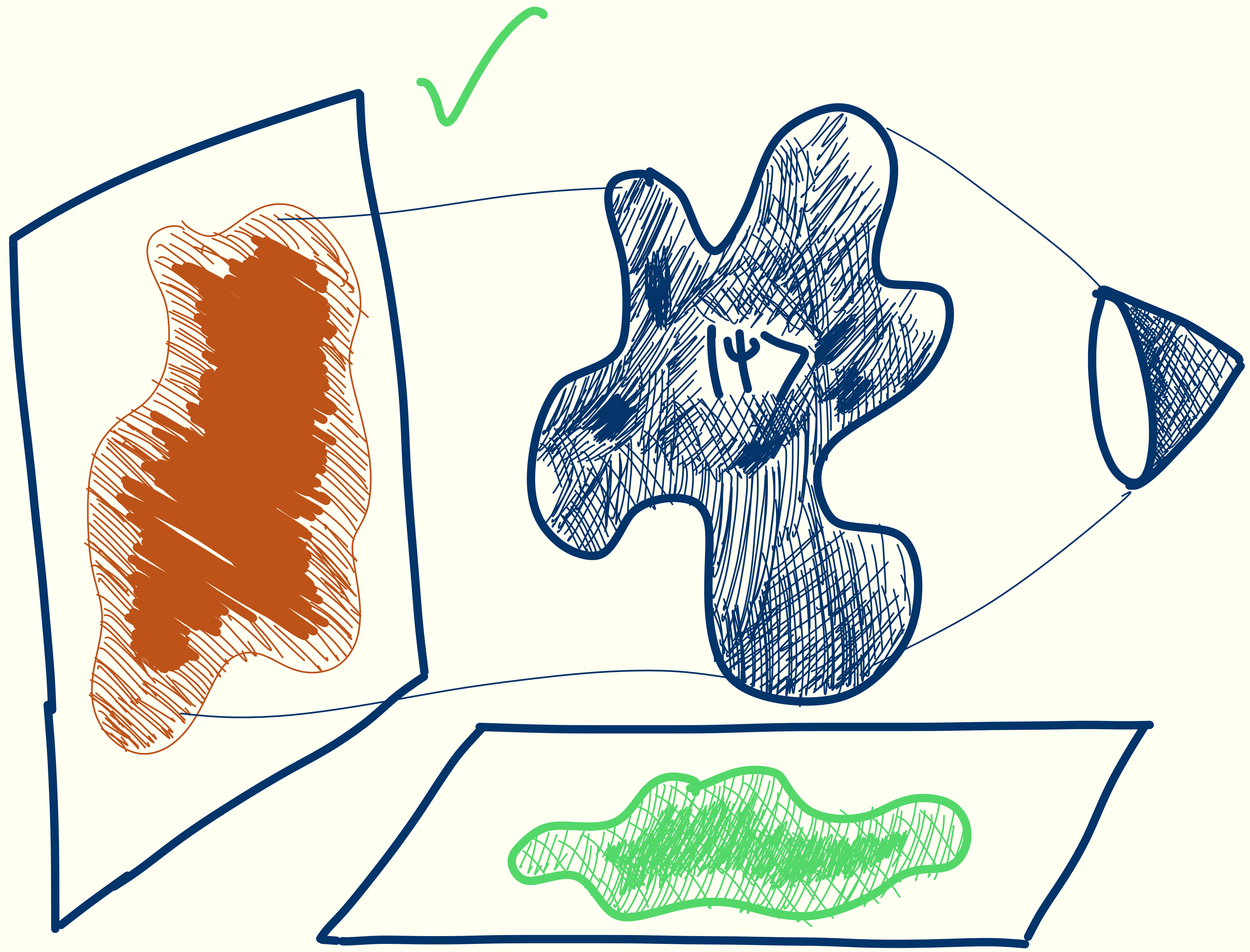
- Use S oracle to measure the POVM $\{\Pi_S, \mathrm{id} - \Pi_S\}$, reject if the outcome is $\mathrm{id} - \Pi_S$.
- Apply $H^{\otimes n}$ to the resulting state.
- Use U oracle to measure the POVM $\{\Pi_U, \mathrm{id} - \Pi_U\}$, reject it the outcome is $\mathrm{id} - \Pi_U$.
- Accept.



Spectral Forrelation is in QMA

Given a copy of a state $|\psi\rangle$:

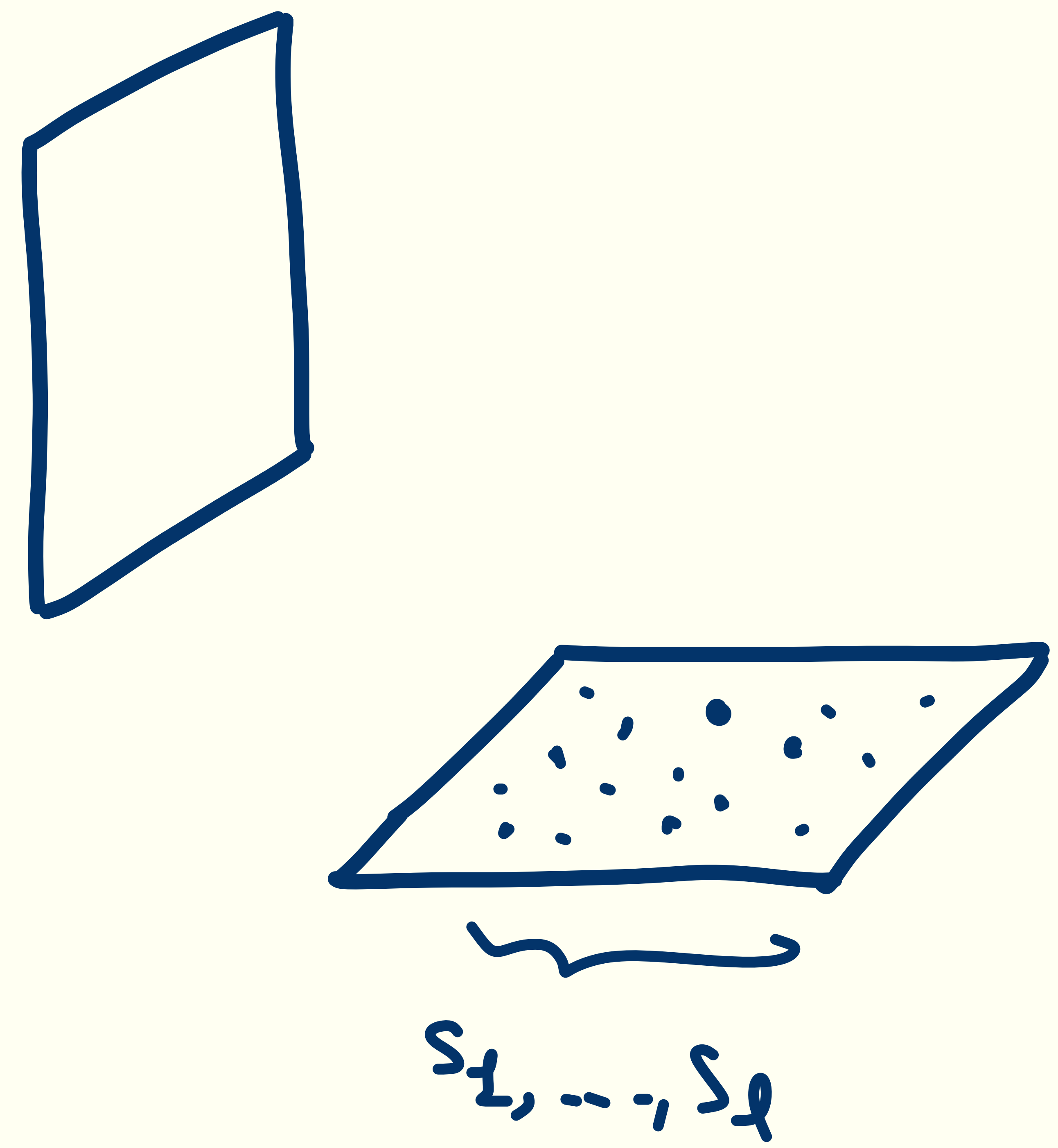
- Use S oracle to measure the POVM $\{\Pi_S, \mathrm{id} - \Pi_S\}$, reject if the outcome is $\mathrm{id} - \Pi_S$.
- Apply $H^{\otimes n}$ to the resulting state.
- Use U oracle to measure the POVM $\{\Pi_U, \mathrm{id} - \Pi_U\}$, reject it the outcome is $\mathrm{id} - \Pi_U$.
- Accept.



Claim: This verifier accepts with probability: $\| \Pi_U \cdot H^{\otimes n} \cdot \Pi_S |\psi\rangle \|^2$.
Sequential amplification can bring this to the standard 2/3 or 1/3.

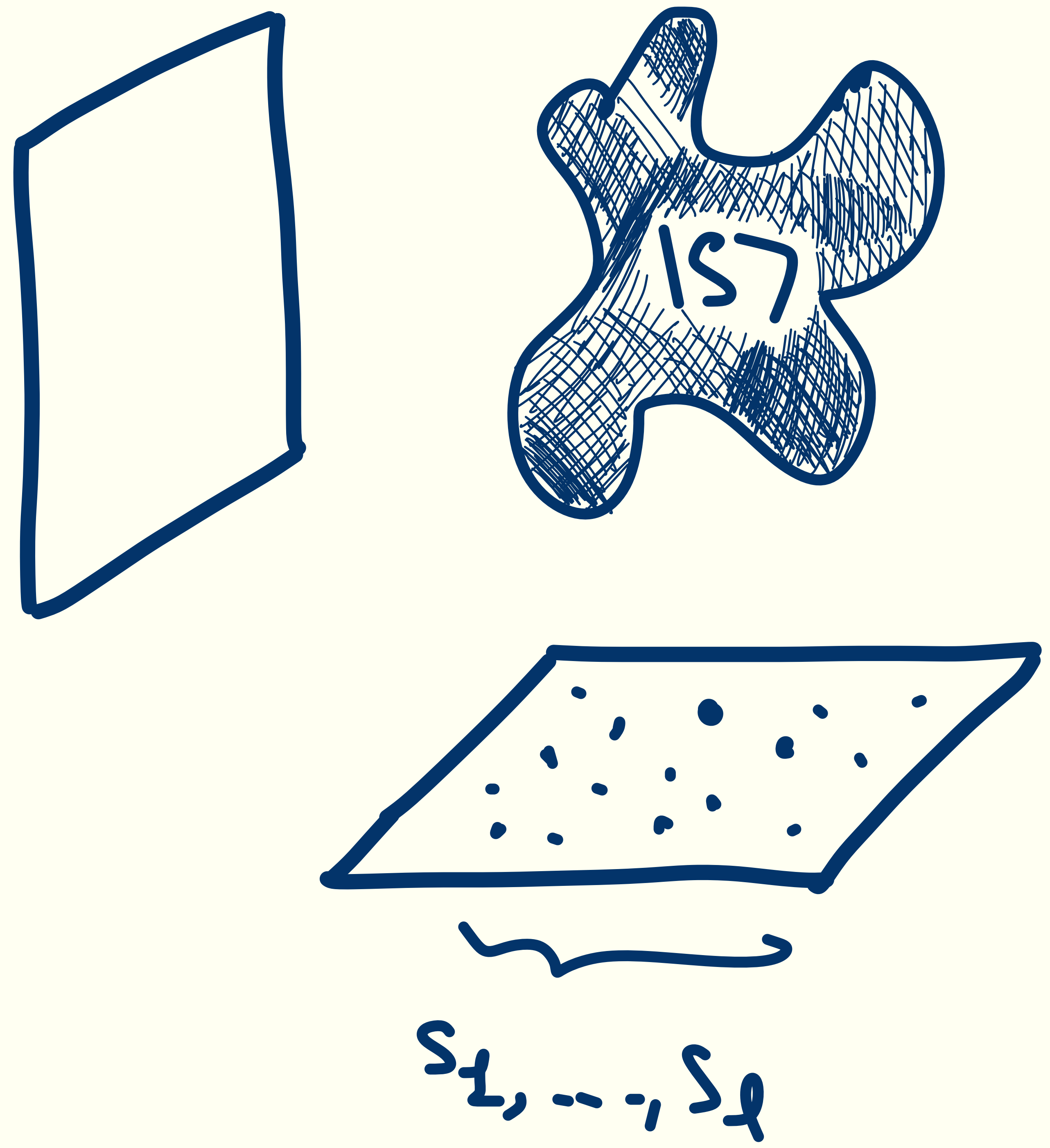
Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$.



Classicalizing a random quantum state

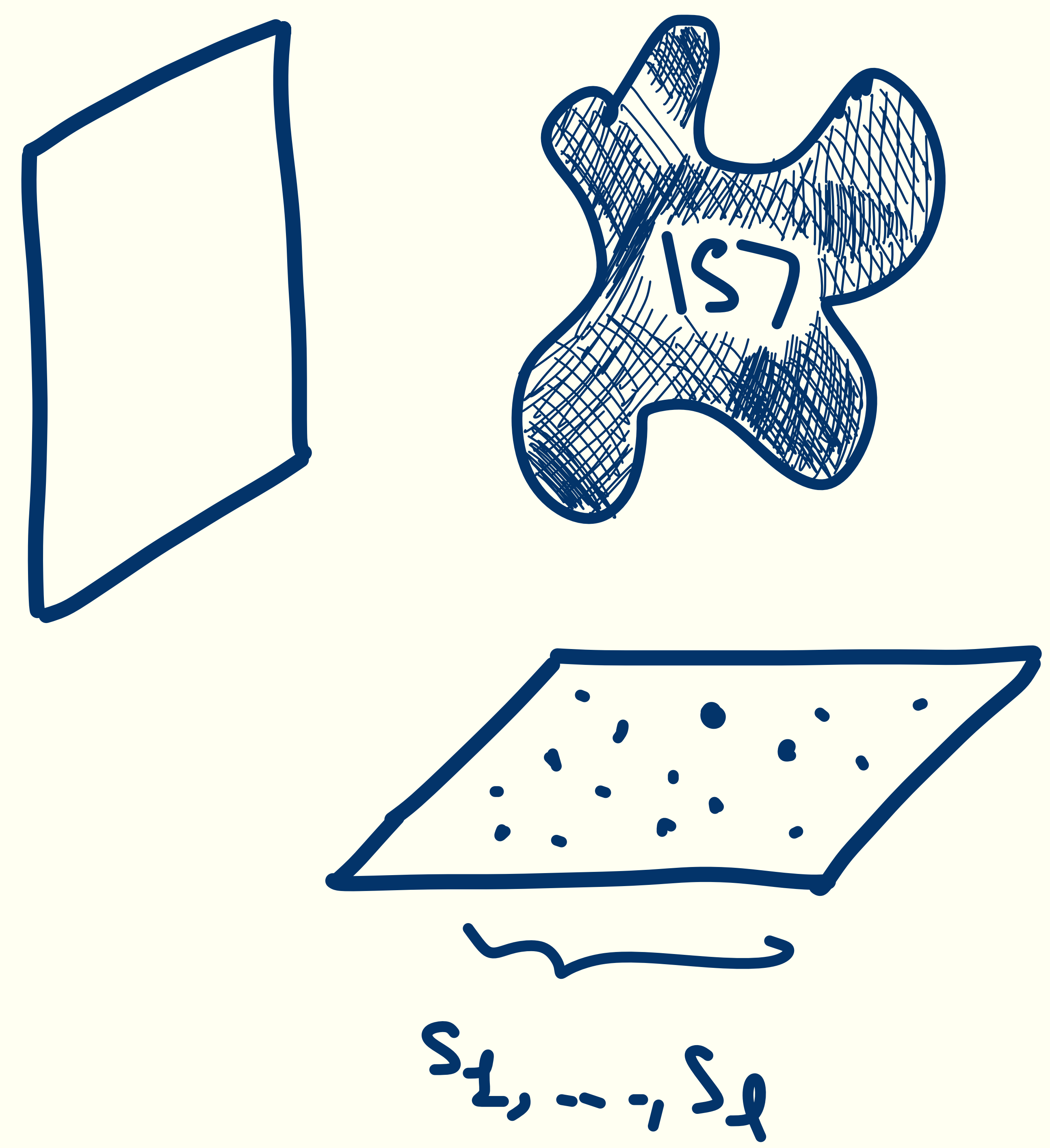
- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.



Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.

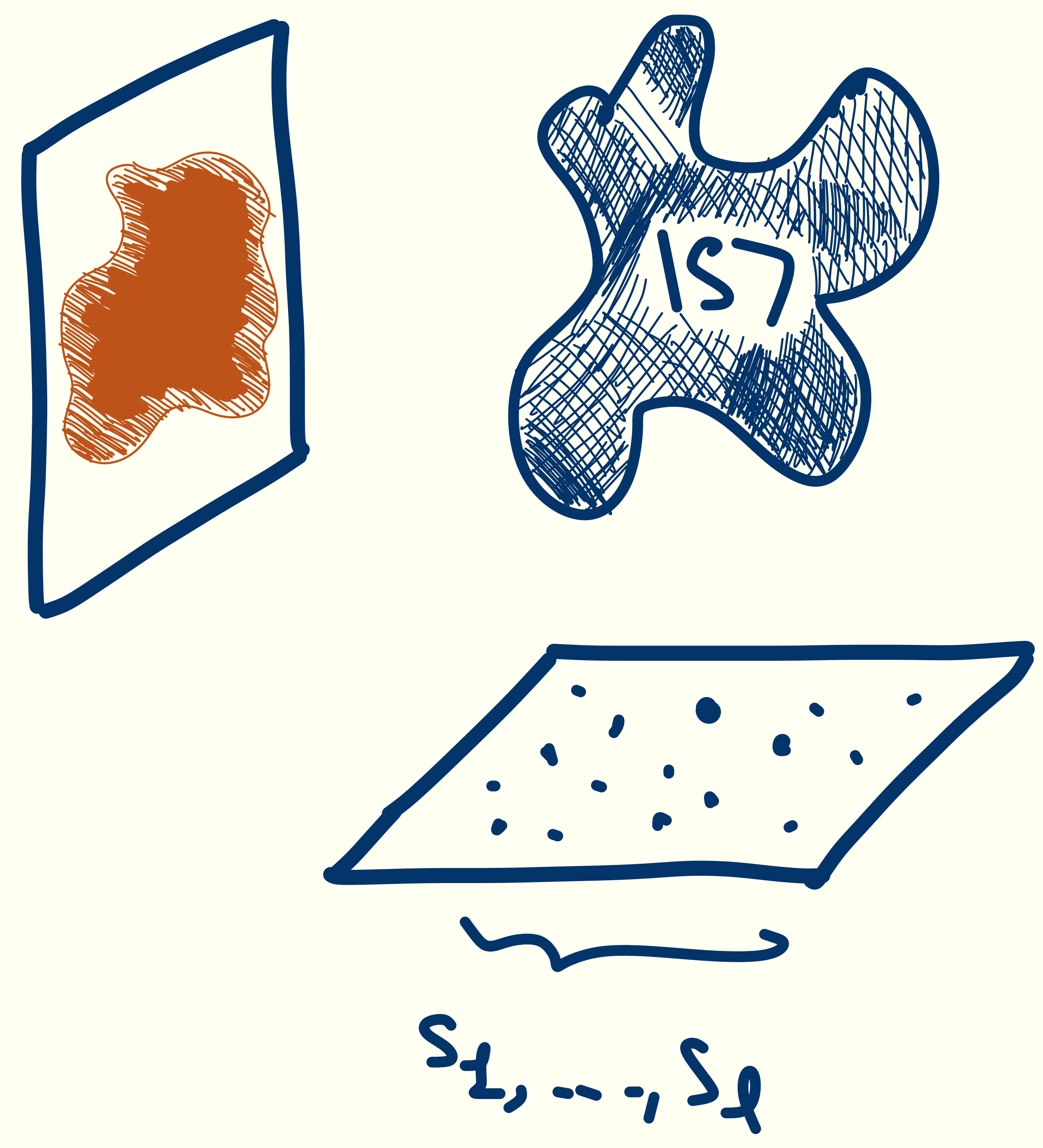
- We take U to be the heavy points of $H^{\otimes n}|S\rangle$, the Hadamard transform of $|S\rangle$.



Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.

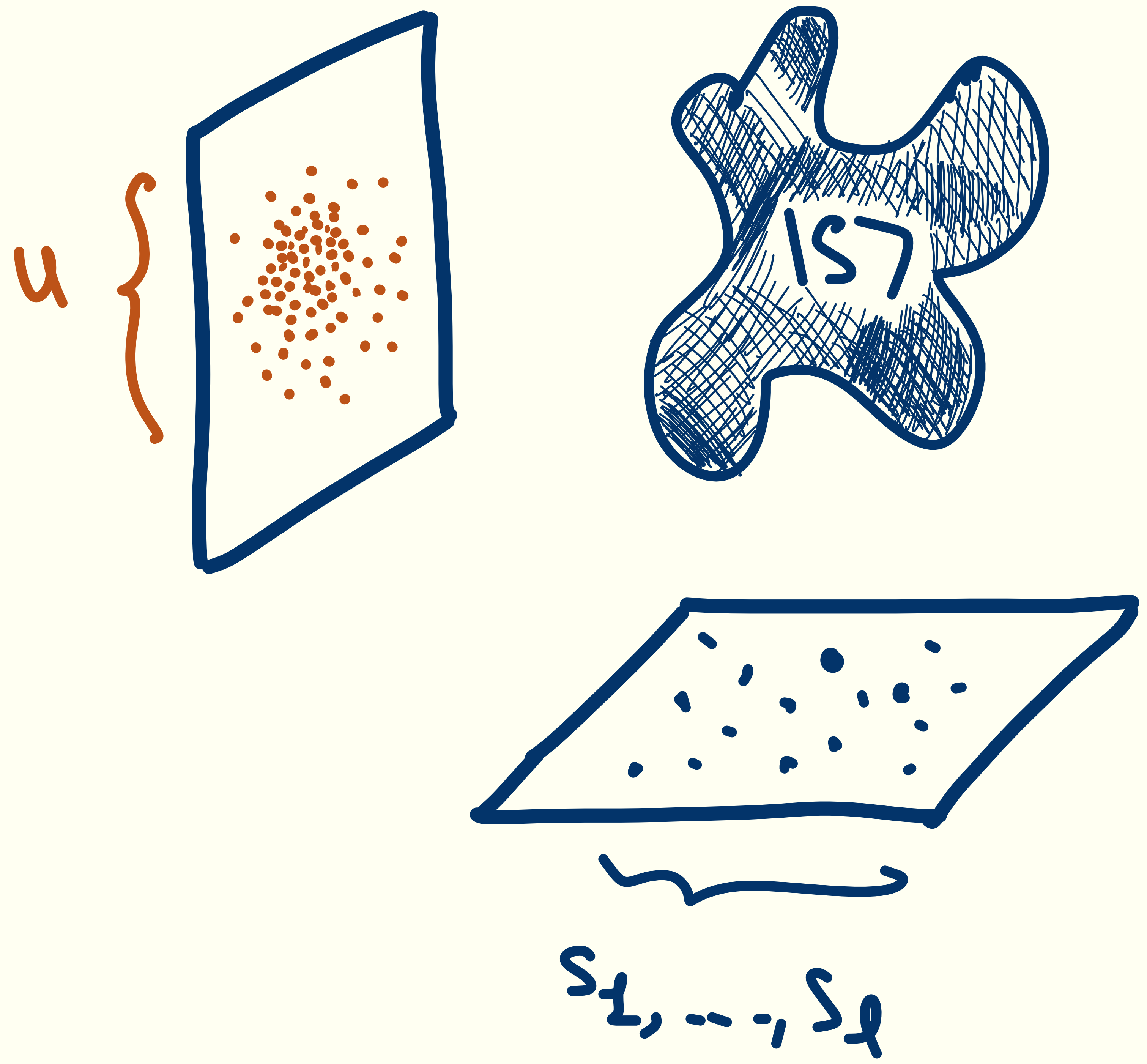
- We take U to be the heavy points of $H^{\otimes n}|S\rangle$, the Hadamard transform of $|S\rangle$.



Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.

- We take U to be the heavy points of $H^{\otimes n}|S\rangle$, the Hadamard transform of $|S\rangle$.

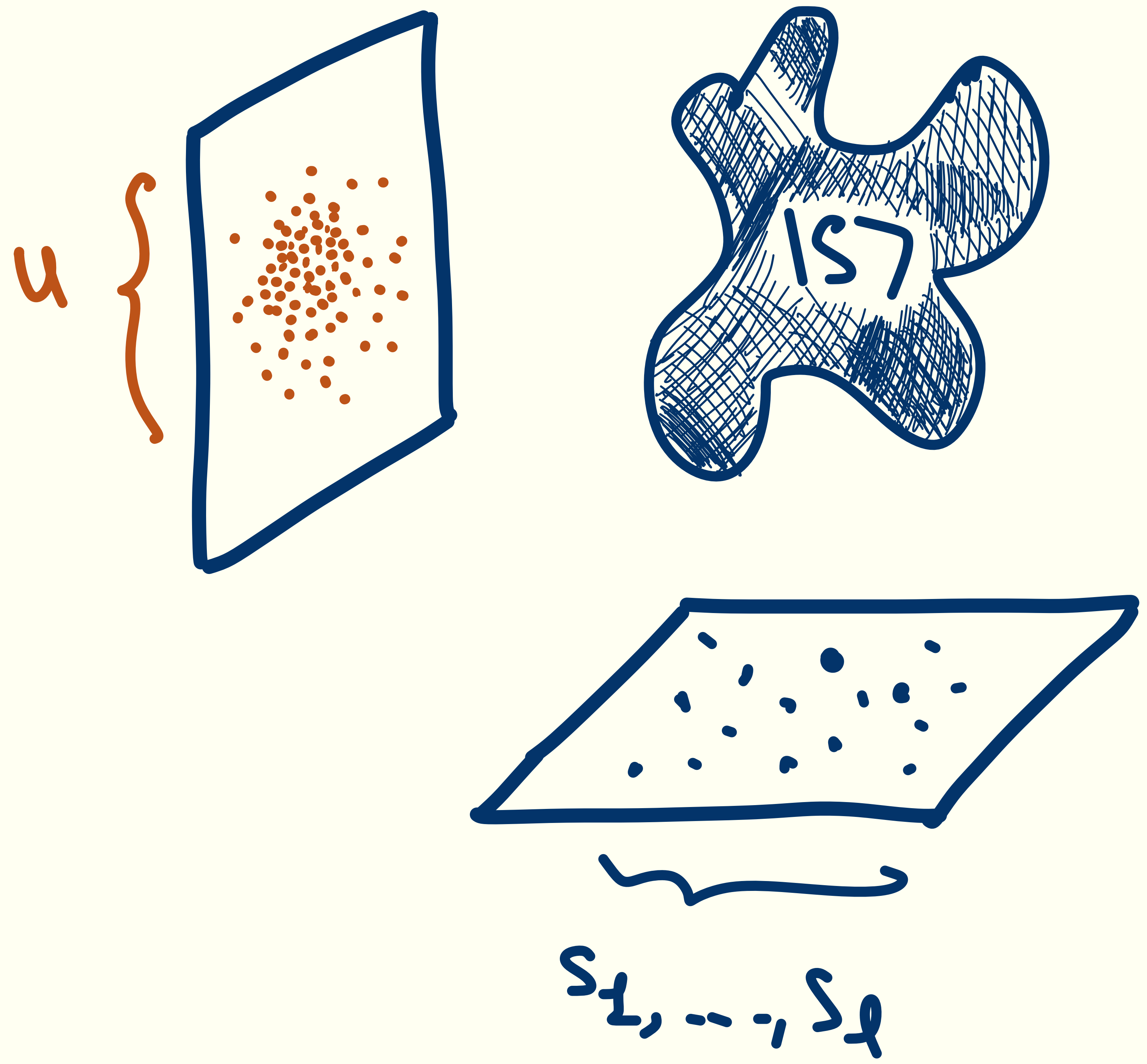


Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.

- We take U to be the heavy points of $H^{\otimes n}|S\rangle$, the Hadamard transform of $|S\rangle$.

We call this distribution over oracles the Strong distribution.



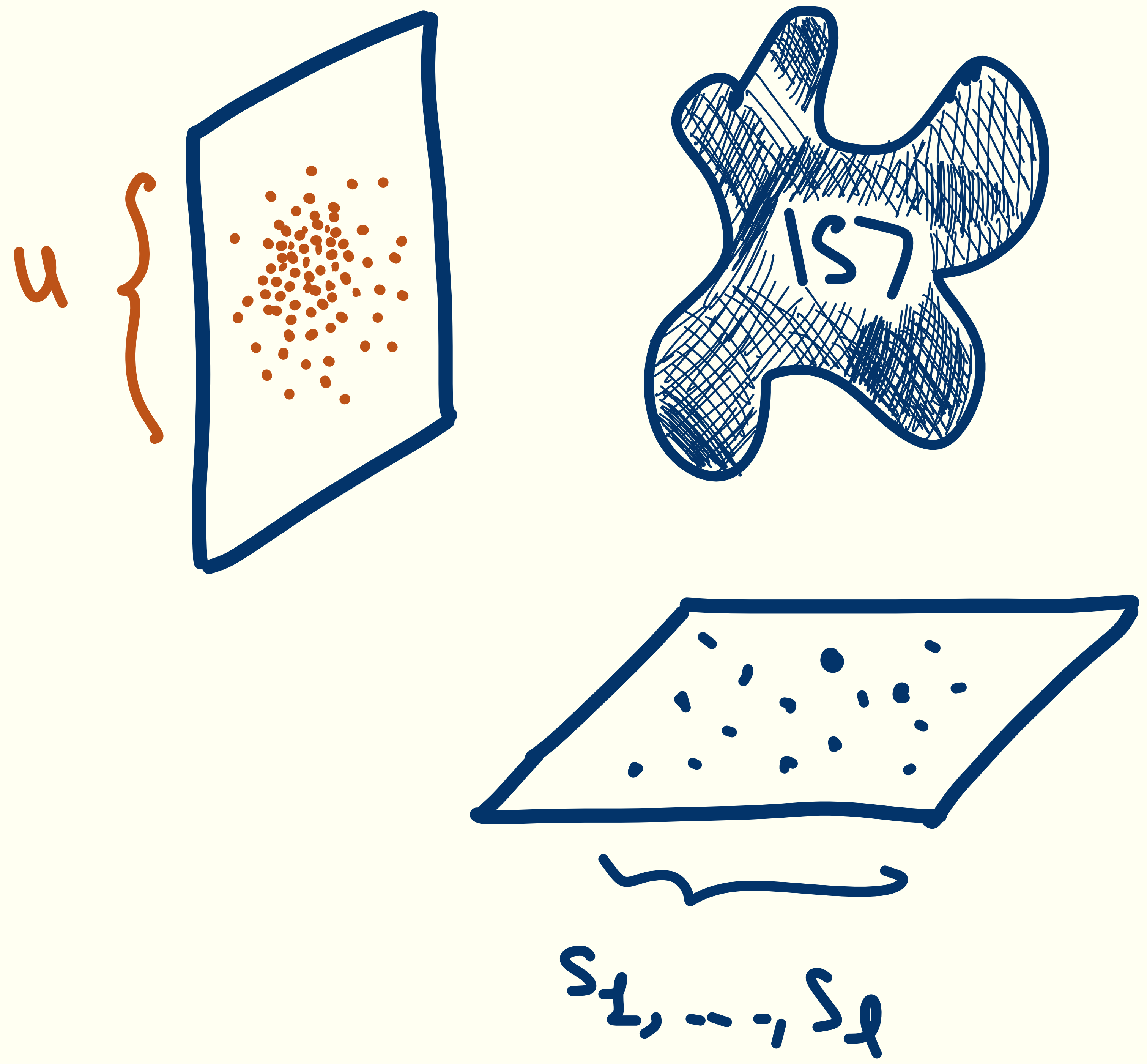
Classicalizing a random quantum state

- We will first sample $\ell = 2^{n/10}$ many random elements $s_1, \ldots, s_\ell$. Let $|S\rangle$ be the uniform superposition over the points.
- We take U to be the heavy points of $H^{\otimes n}|S\rangle$, the Hadamard transform of $|S\rangle$.

We call this distribution over oracles the Strong distribution.

Claim (Informal): For $(S, U) \sim$ Strong, the following holds:

$$\mathbb{E}_U \left[\Pi_S \cdot H^{\otimes n} \cdot \Pi_U \cdot H^{\otimes n} \cdot \Pi_S\right] \approx \frac{1}{10}|S\rangle\langle S| + \frac{1}{2}\mathrm{id}$$



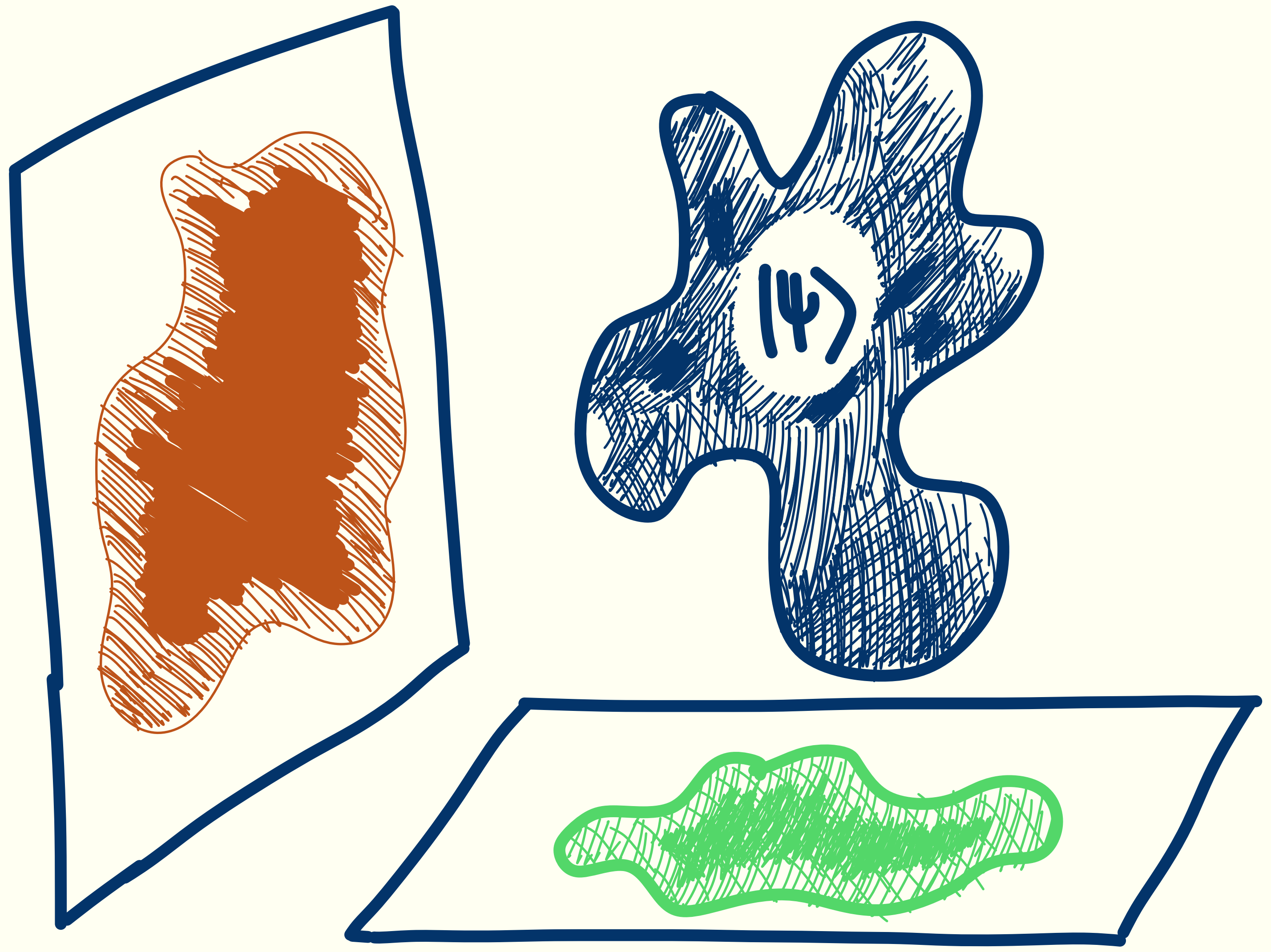
Strong yes instances

A pair (S, U) is a strong yes instance if:

Strong yes instances

A pair (S, U) is a strong yes instance if:

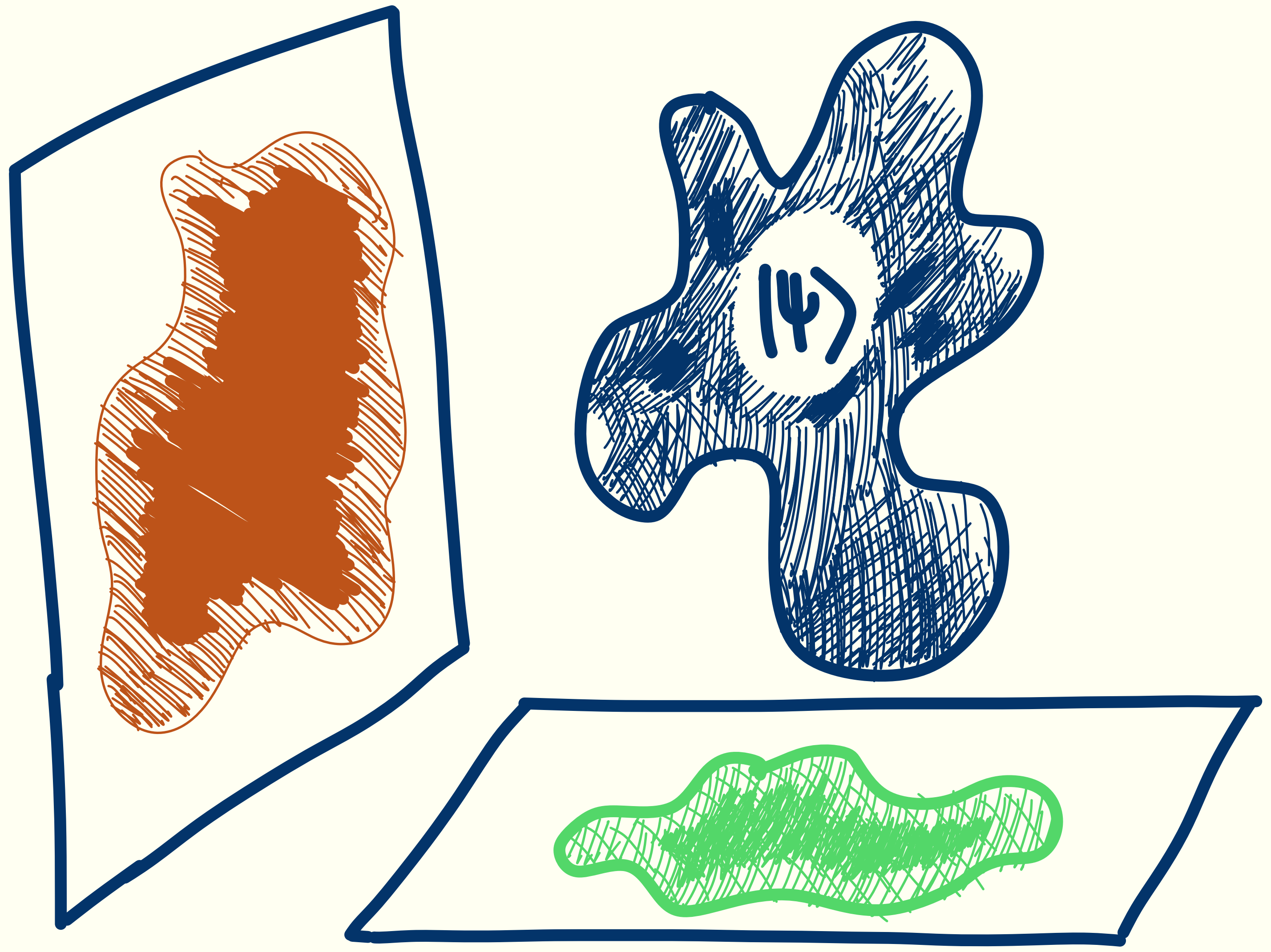
- (S, U) is a yes instance of spectral Forrelation (i.e., $\geq 59/100$ spectrally Forrelated).

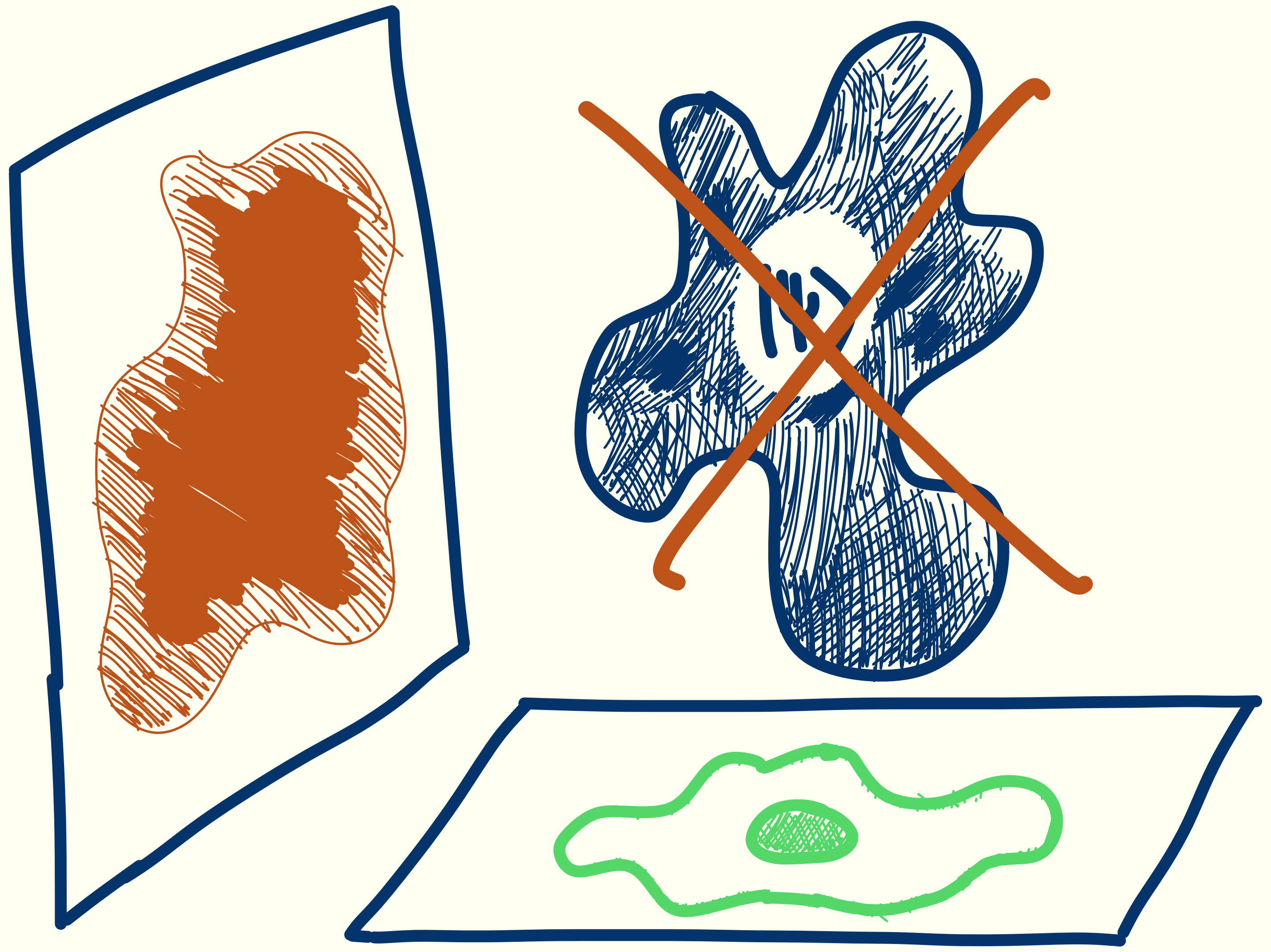


Strong yes instances

A pair (S, U) is a strong yes instance if:

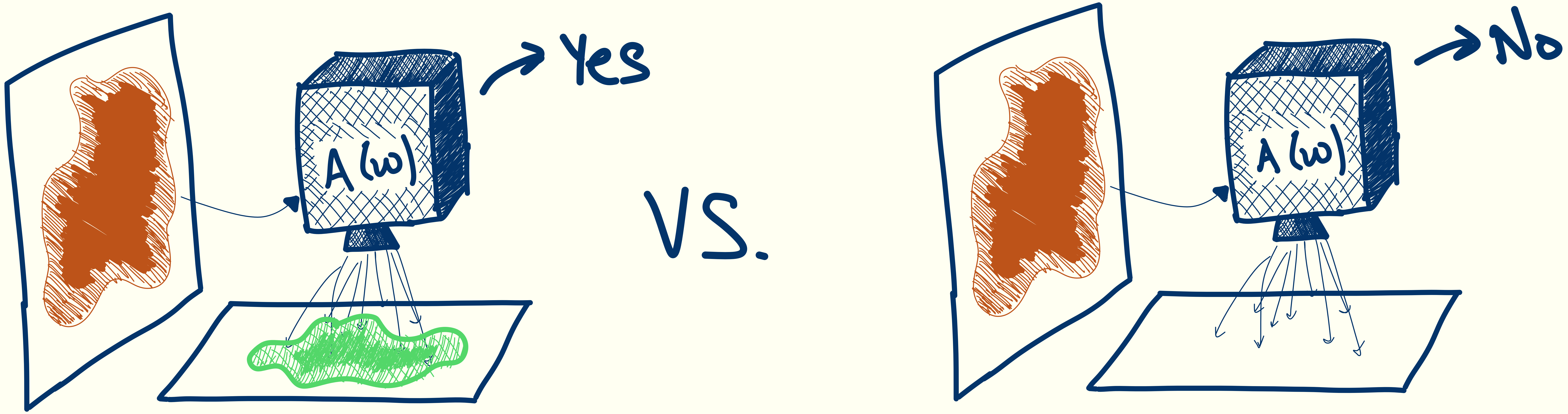
- (S, U) is a yes instance of spectral Forrelation (i.e., $\geq 59/100$ spectrally Forrelated).
- For all $\Delta \subset S$ with $|\Delta| \leq \ell/100$, (Δ, U) is a no instance of spectral Forrelation (i.e., $\leq 57/100$ spectrally Forrelated).





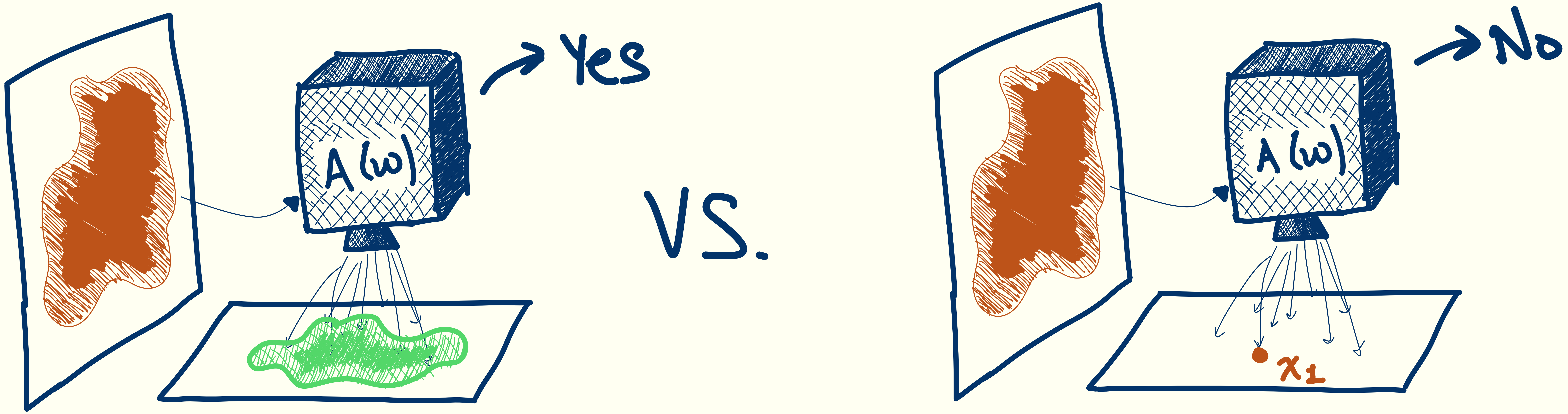
Strong yes instances can be sampled from

Any quantum query algorithm that distinguishes between (S, U) and $(\varnothing, U)$ must query a point in S pretty often ($\geq 1/3t$ chance per query), since otherwise the action of the oracles is identical.



Strong yes instances can be sampled from

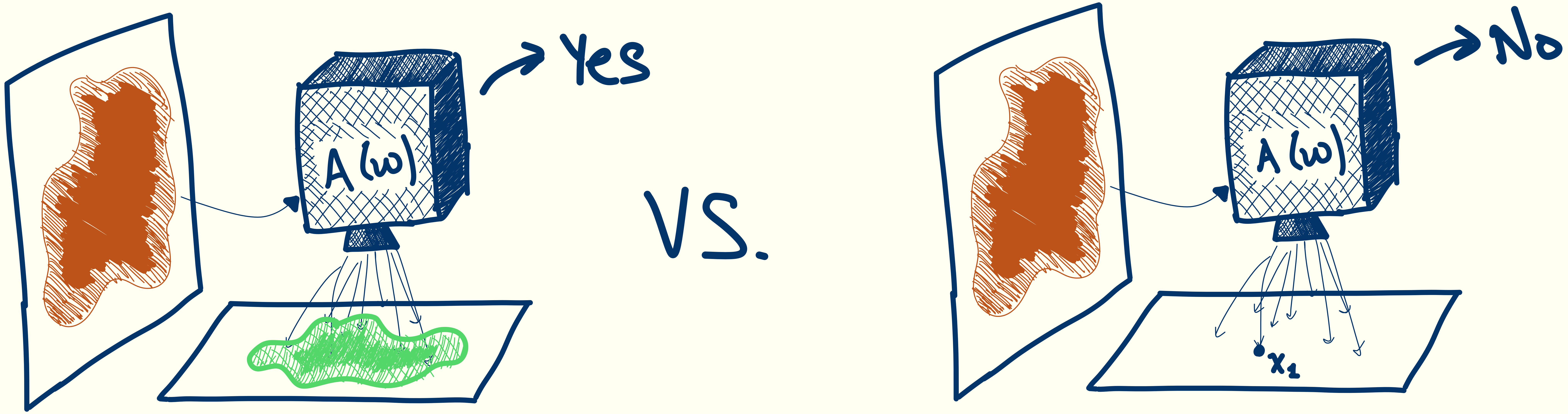
Any quantum query algorithm that distinguishes between (S, U) and $(\emptyset, U)$ must query a point in S pretty often ($\geq 1/3t$ chance per query), since otherwise the action of the oracles is identical.



Therefore, measuring a random query of the algorithm will yield a point in S with good probability, x_1.

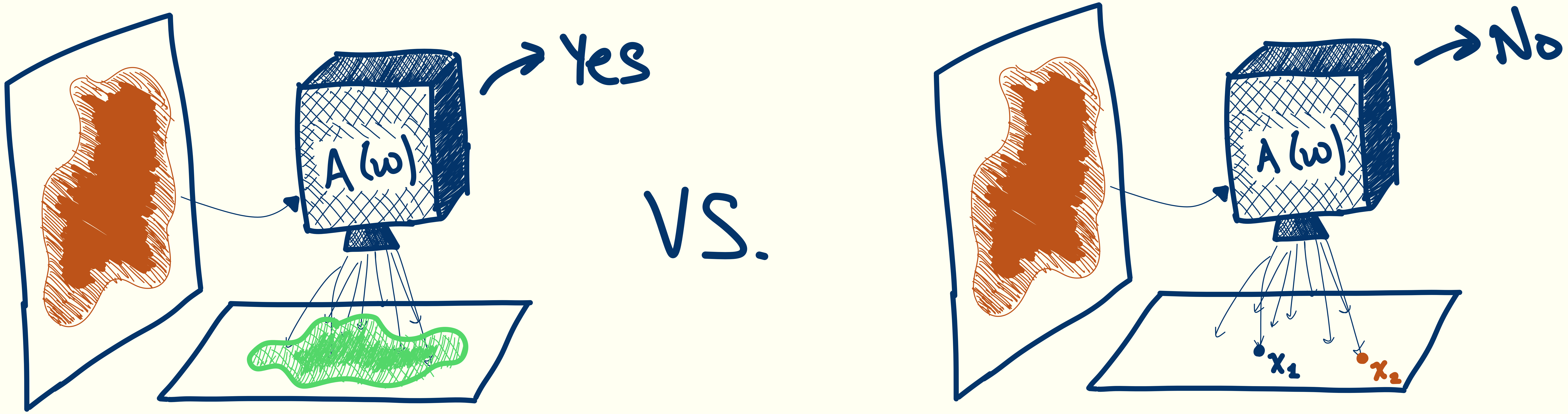
Strong yes instances can be sampled from

Any quantum query algorithm that distinguishes between (S, U) and $(\{x_1\}, U)$ must query a point in S pretty often ($\geq 1/3t$ chance per query), since otherwise the action of the oracles is identical.



Strong yes instances can be sampled from

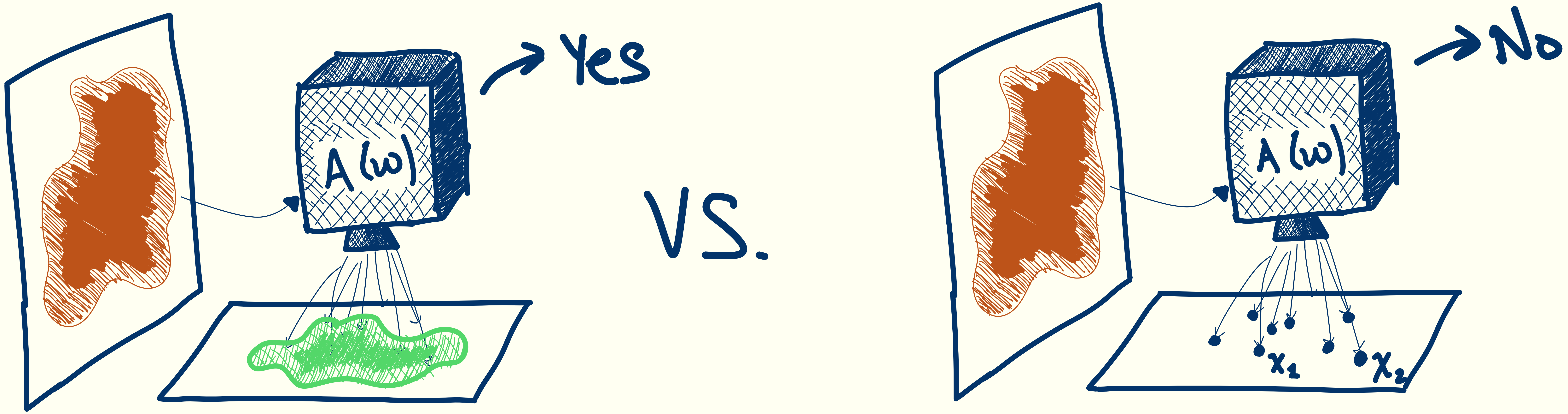
Any quantum query algorithm that distinguishes between (S, U) and $(\{x_1\}, U)$ must query a point in S pretty often ($\geq 1/3t$ chance per query), since otherwise the action of the oracles is identical.



Therefore, measuring a random query of the algorithm will yield a point in S with good probability, x_2.

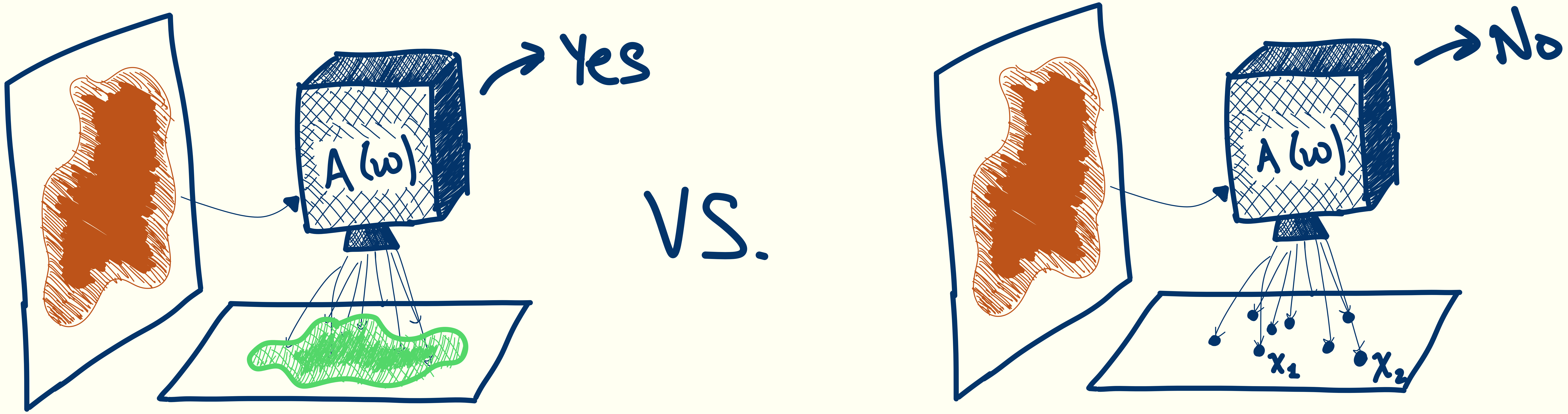
Strong yes instances can be sampled from

Because of the strong yes property, we can keep going until $\ell/100$ points have been sampled! This is the part that uses the fact that the witness is classical.



Strong yes instances can be sampled from

Because of the strong yes property, we can keep going until $\ell/100$ points have been sampled! This is the part that uses the fact that the witness is classical.



Given a QCMA algorithm, we can guess the classical witness and be correct with probability 2^{-q}.

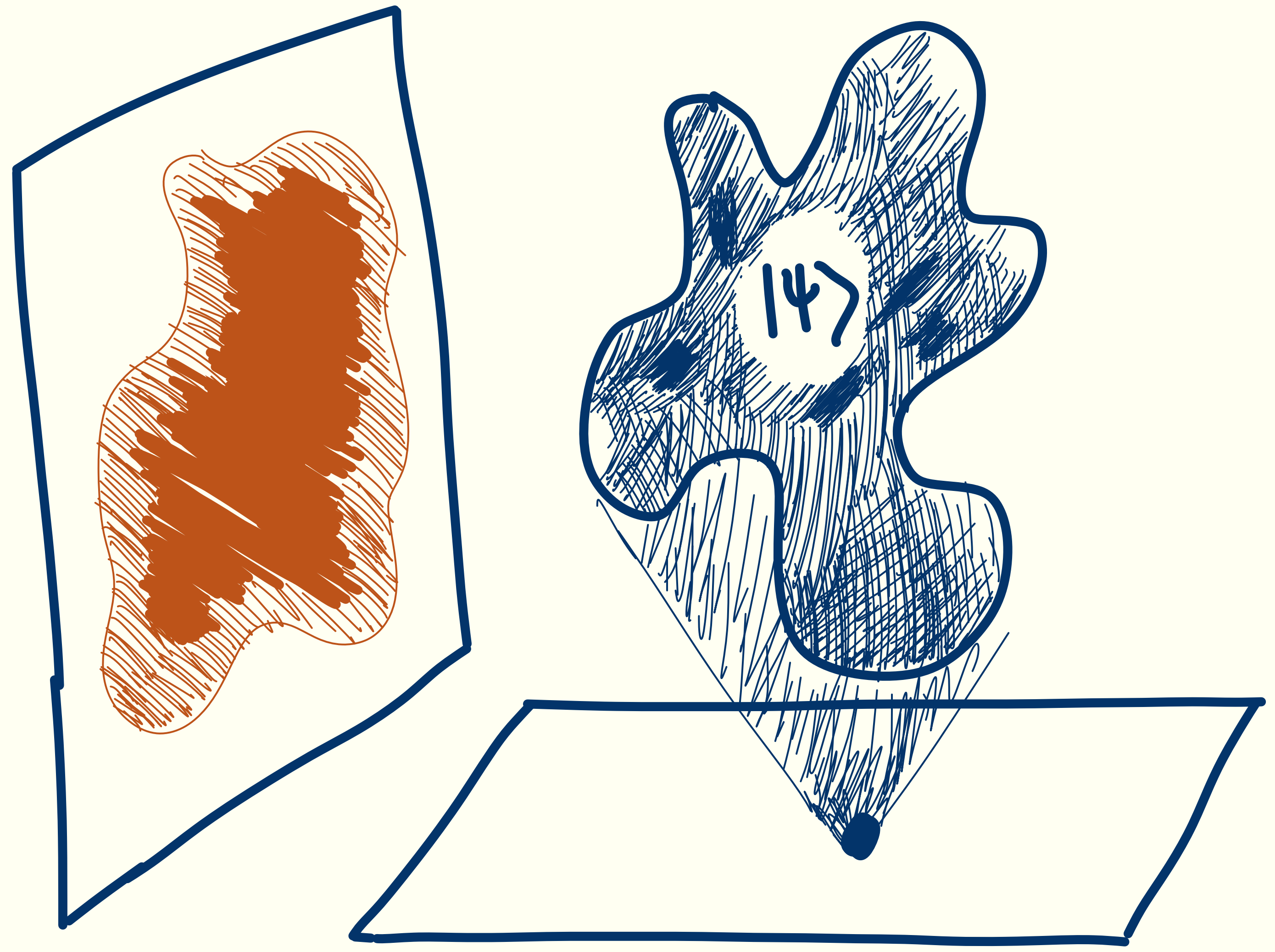
Why should spectral Forrelation be hard?

- S is sparse → guessing a single point of S seems like it should be hard.

Why should spectral Forrelation be hard?

- S is sparse → guessing a single point of S seems like it should be hard.

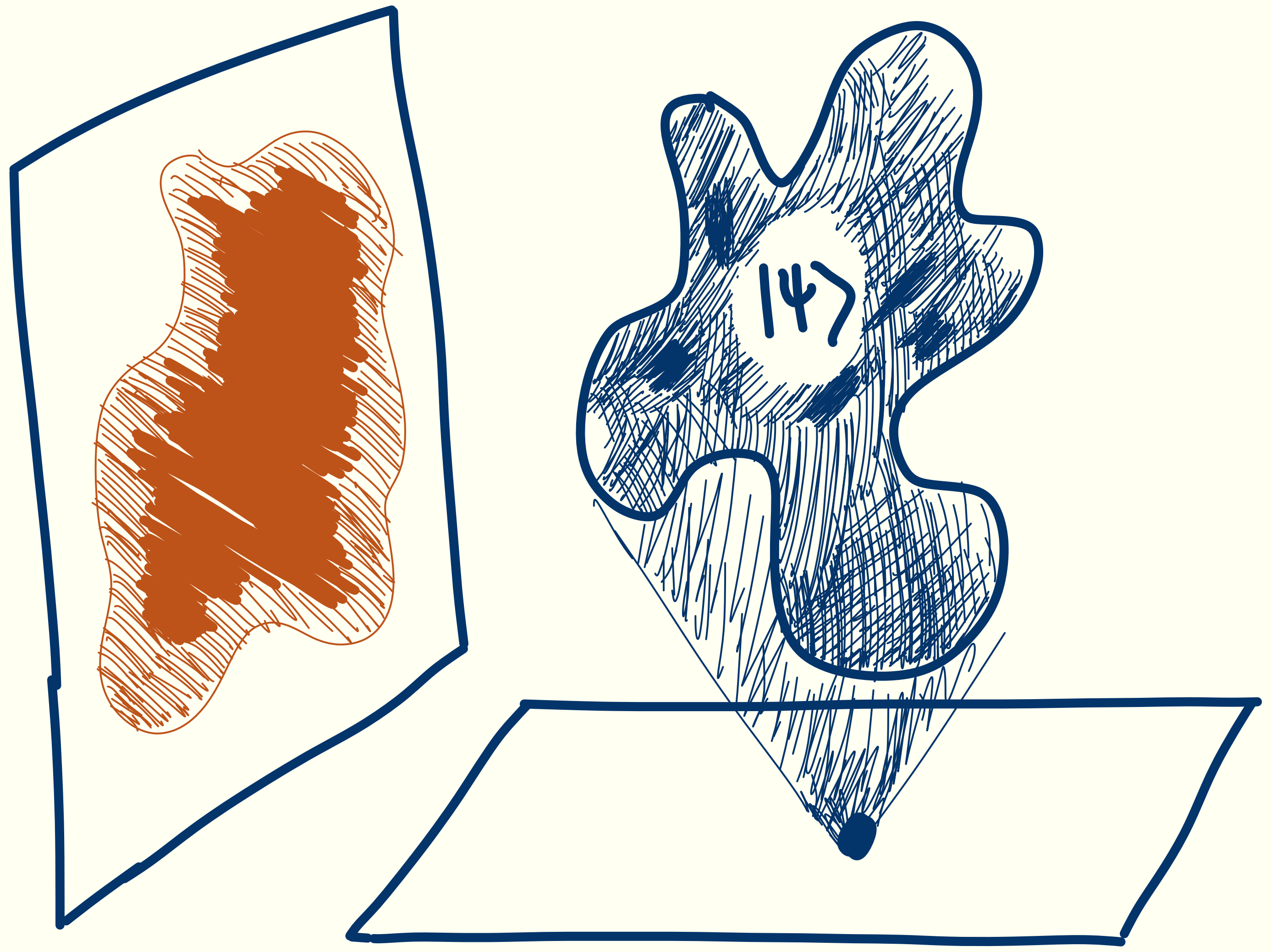
A quantum witness helps you verify spectral Forrelation, but only gives you a single point from S.



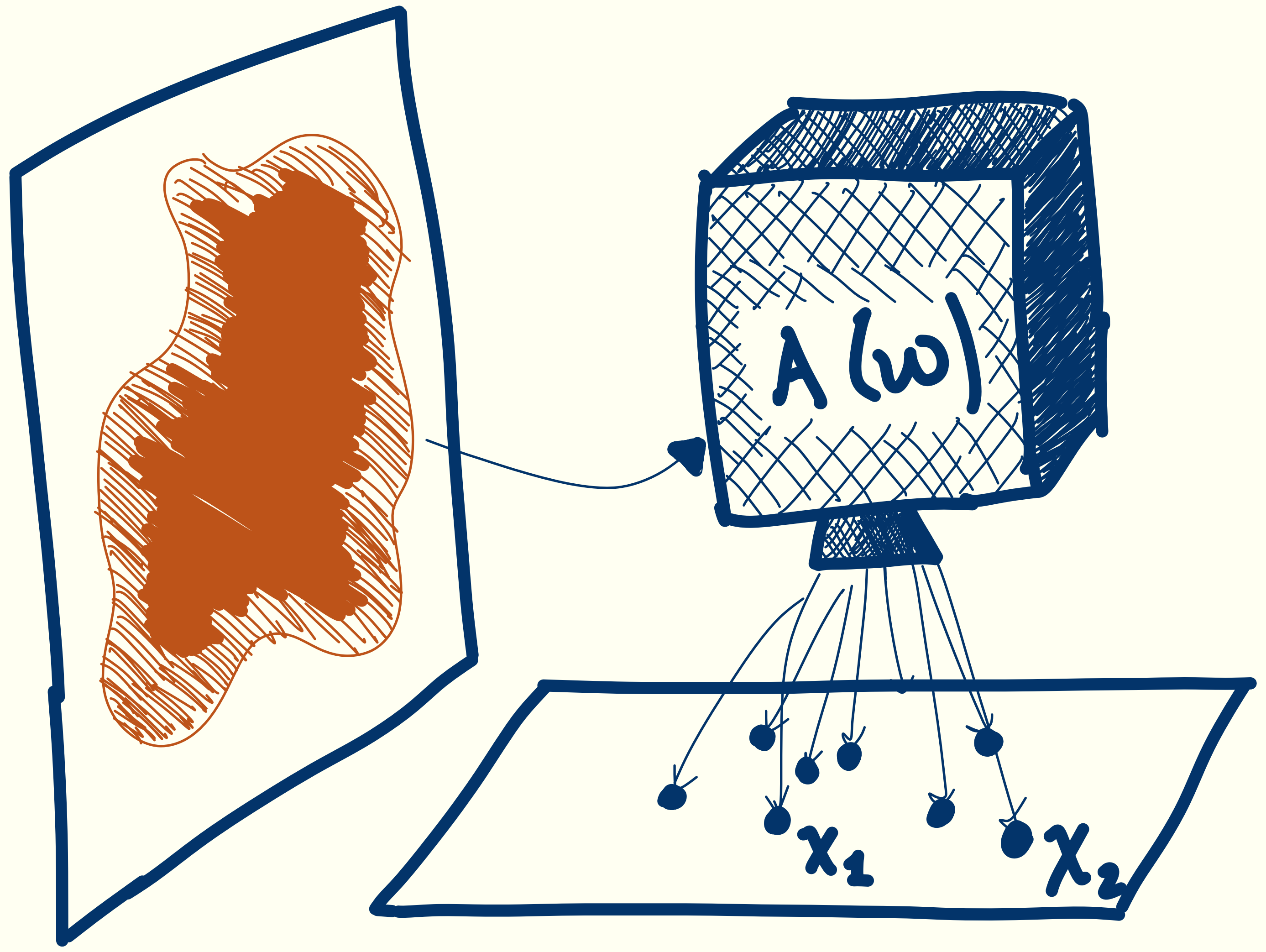
Why should spectral Forrelation be hard?

- S is sparse → guessing a single point of S seems like it should be hard.

A quantum witness helps you verify spectral Forrelation, but only gives you a single point from S.



A classical witness that help you verify spectral Forrelation can be re-used, must actually specify $\ell/10$ points from S, somehow!



Main theorems

Main theorems

Theorem 1: For all $v > 0$, and all quantum query algorithms making $T = T(n)$ queries to a set membership oracle for U, the probability, over Strong, that the algorithm outputs v distinct points from S is at most

$$\leq \left(\frac{\mathrm{poly}(v, T)}{\mathrm{poly}(2^n)}\right)^v.$$

Main theorems

Theorem 1: For all $v > 0$, and all quantum query algorithms making $T = T(n)$ queries to a set membership oracle for U, the probability, over Strong, that the algorithm outputs v distinct points from S is at most

$$\leq \left(\frac{\mathrm{poly}(v, T)}{\mathrm{poly}(2^n)}\right)^v.$$

Theorem 2: If there exists a QCMA algorithm, making $t = t(n)$ queries to (S, U) and taking a witness of length $q = q(n)$, then for all $0 < v < \ell/100$, there is a query algorithm making vt queries to U that outputs v distinct points from S with probability

$$\geq 2^{-q}\left(\frac{1}{36t^2}\right)^v$$

Takeaways

Takeaways

- **Quantum proofs are really powerful!**
→ That power is what we think makes them not reusable!
→ Our proof finds a task (sampling) that should be really hard, and shows that a reusable proof would be too good to be true.

Takeaways

- **Quantum proofs are really powerful!**
  → That power is what we think makes them not reusable!
  → Our proof finds a task (sampling) that should be really hard, and shows that a reusable proof would be too good to be true.
- **Small structural changes can have a huge impact!**
  → Our analysis (the bosonic compressed oracle) is possible because we allow S to be a multi-set with independent elements instead of a set with exactly ℓ elements.
  → This removal of structure allowed us to understand queries to the Fourier transform of an oracle way better than we could before!

Takeaways

- **Quantum proofs are really powerful!**
→ That power is what we think makes them not reusable!
→ Our proof finds a task (sampling) that should be really hard, and shows that a reusable proof would be too good to be true.
- **Small structural changes can have a huge impact!**
→ Our analysis (the bosonic compressed oracle) is possible because we allow S to be a multi-set with independent elements instead of a set with exactly ℓ elements.
→ This removal of structure allowed us to understand queries to the Fourier transform of an oracle way better than we could before!
- **Much more work is needed!**
→ Understanding oracles with structure seems to require an understanding that structure, seem to be annoying to deal with using general methods.
→ To understand other oracles (expander mixing problem, Yamakawa-Zhandry, etc.), we will need more specific tools, or a big leap in understanding of quantum algorithms.

Open questions

Open questions

- **Can we find new constructions/security proofs for quantum money?**
  → Our ideas lie in the intersection of ideas used for quantum money (subset states ↔ subspace states, Fourier transform of S ↔ Fourier transform for group actions).
  → We also prove a separation between UnclonableQMA and QMA, feels like we should be able to say something about quantum money, but what?

Open questions

- **Can we find new constructions/security proofs for quantum money?**
  → Our ideas lie in the intersection of ideas used for quantum money (subset states ↔ subspace states, Fourier transform of S ↔ Fourier transform for group actions).
  → We also prove a separation between UnclonableQMA and QMA, feels like we should be able to say something about quantum money, but what?

- **Can we use our oracle/techniques to solve other problems in query complexity?**
  → BQP/qpoly versus BQP/poly?
  → QMA search-to-decision?

Open questions

- **Can we find new constructions/security proofs for quantum money?**
  → Our ideas lie in the intersection of ideas used for quantum money (subset states ↔ subspace states, Fourier transform of S ↔ Fourier transform for group actions).
  → We also prove a separation between UnclonableQMA and QMA, feels like we should be able to say something about quantum money, but what?

- **Can we use our oracle/techniques to solve other problems in query complexity?**
  → BQP/qpoly versus BQP/poly?
  → QMA search-to-decision?

- **Is there a connection to the Aaronson-Ambainis conjecture?**
  → Both Liu-Mutreja-Yuen'24 and Zhandry'24 showed that there is a connection between QCMA versus QMA and pseudorandomness against quantum algorithms.
  → Our proof didn't say anything about this, but could you use our techniques?

Thanks for listening!