On the power of a unique quantum witness

Shengyu Zhang

The Chinese University of Hong Kong

(Joint work with Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattash)

Role of # of witnesses in NP

- NP: Problems that can be verified in poly. time.
- Obs: # of witnesses for positive instances can be widely varying from 1 to exponentially high.
- *Question: Is hardness of NP due to this variation?*

- [Theorem*1] $NP \subseteq RP^{UP}$
  - RP: like BPP, but without error on negative instances.
  - UP: problems in NP with promise that each positive instance has a unique witness

*1: Valiant, Vazirani, TCS, 1986.

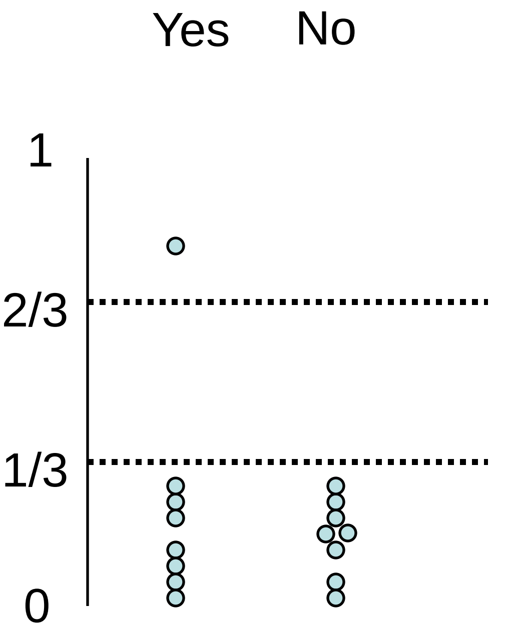
Proof of V-V

- Main idea: Set a filter to let each potential witness pass w.p. $\Theta(1/D)$.
  - D: # of witnesses.
- Then w.c.p. exactly one witness passes

- Other issues:
  - # of witnesses: Guess it. Double the guess.
  - Efficiency of the filter: 2 universal-hashing

The case for MA

- UMA: A yes instance has
  - a unique witness with accepting prob. > 2/3,
  - all other witnesses with accepting prob. < 1/3.



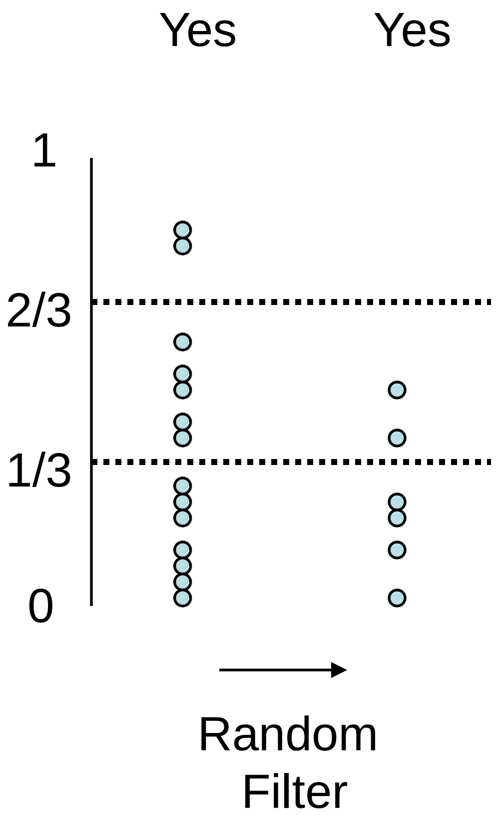
- *Question*[1]*: Can we reduce MA to UMA?*

*1. Aharonov, Ben-Or, Brandao, Sattath, arXiv/0810.4840, *2008*.

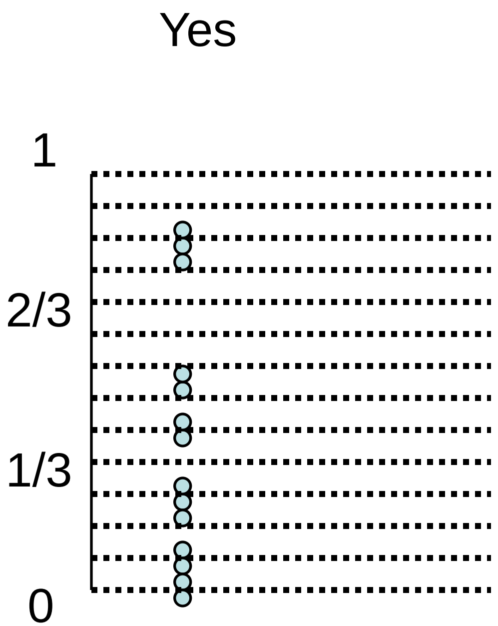
The difficulty for MA

- Difficulty: A yes instance of MA may have many “grey” witnesses with accepting prob. in (1/3, 2/3).

- Still random filter? Kills all good witnesses before killing all grey ones.



The idea for MA*[1]



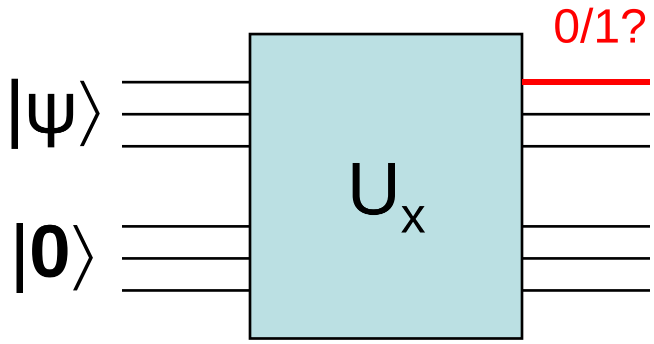
- Evenly cut [0,1] into m subintervals.
  - m=poly(n): length of witness
- One of them has

$$\frac{\#\text{ good witnesses}}{\#\text{ grey witnesses}} \geq 1/2$$

- Observe that constant fraction is enough to make VV work.

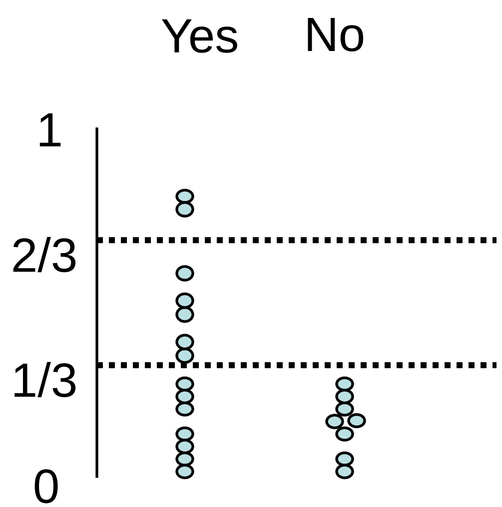
*1. Aharonov, Ben-Or, Brandao, Sattath, arXiv/0810.4840, *2008*.

QMA



$x \in L$: $\exists |\psi\rangle$, $\|U_x|\psi\mathbf{0}\rangle\|^2 > 2/3$.

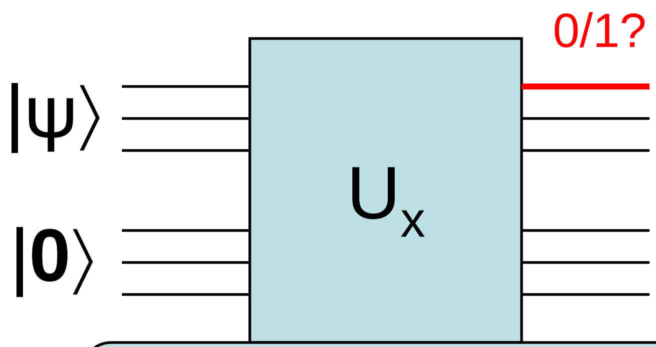
$x \notin L$: $\forall |\psi\rangle$, $\|U_x|\psi\mathbf{0}\rangle\|^2 < 1/3$.



[Fact] There are 2^m orthonormal vectors $|\psi_i\rangle$, s.t. $\forall |\psi\rangle = \sum \alpha_i |\psi_i\rangle$,

$$\|U_x|\psi\mathbf{0}\rangle\|^2 = \sum |\alpha_i|^2 \cdot \|U_x|\psi_i\mathbf{0}\rangle\|^2$$

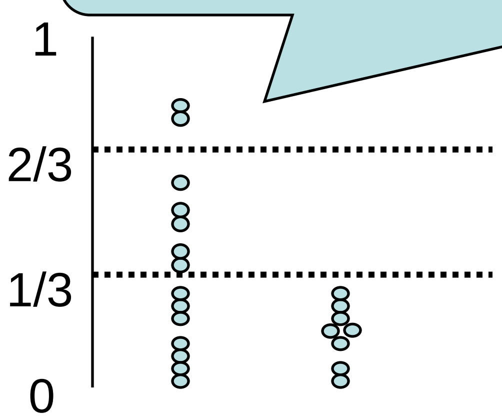
Unique QMA



$x \in L$: $\exists |\psi\rangle$, $\| U_x |\psi \mathbf{0}\rangle \|^2 > 2/3$.

$x \notin L$: $\forall |\psi\rangle$, $\| U_x |\psi \mathbf{0}\rangle \|^2 < 1/3$.

Question[*1]*:* $\mathrm{QMA} \subseteq \mathrm{BQP}^{\mathrm{UQMA}}$?



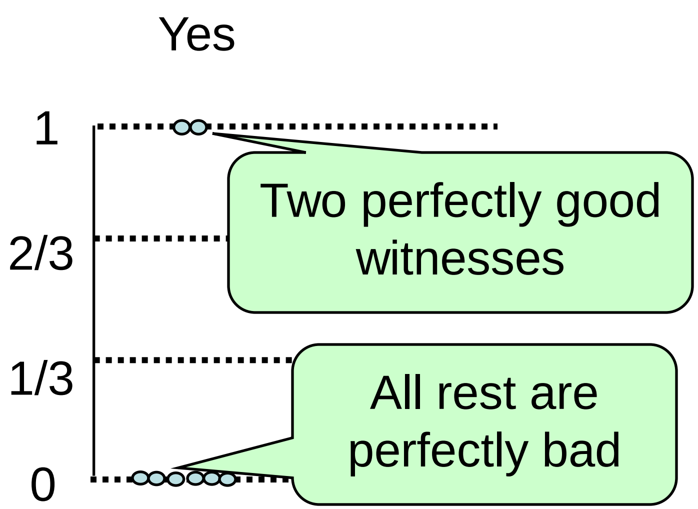
[Fact] There are 2^m orthonormal vectors $|\psi_i\rangle$, s.t. $\forall |\psi\rangle = \sum \alpha_i |\psi_i\rangle$,

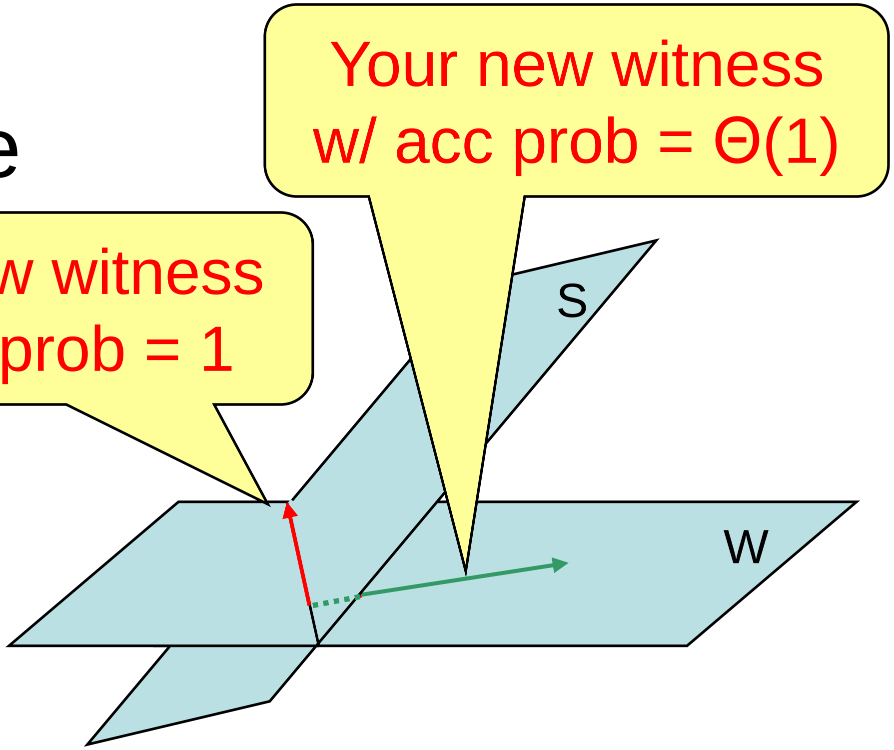
$$\| U_x |\psi \mathbf{0}\rangle \|^2 = \sum |\alpha_i|^2 \cdot \| U_x |\psi_i \mathbf{0}\rangle \|^2$$

*1. Aharonov, Ben-Or, Brandao, Sattath, arXiv/0810.4840, *2008*.

Difficulty for QMA

- Consider the simple set of Yes instances*1:





If the universe of witnesses is 3-dim …
Natural analog of random selection
--- Random Projection

*1. Aharonov, Ben-Or, Brandao, Sattath, arXiv/0810.4840, *2008*.

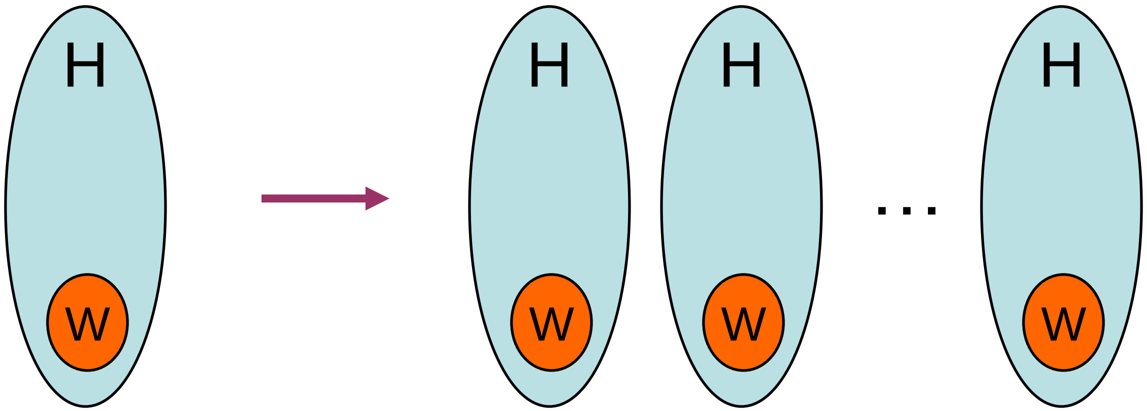
Difficulty for QMA

- Unfortunately dim(H) = 2^m = exp(n).
- Random Projection fails: The whole 2-dim subspace W gets projected onto the random subspace S almost uniformly
  - Largest and smallest scales are esp. close

"… which we believe captures the difficulty of the problem."
"A new idea seems to be required."

--- Aharonov, Ben-Or, Brandao, Sattath, arXiv/0810.4840, *2008*.

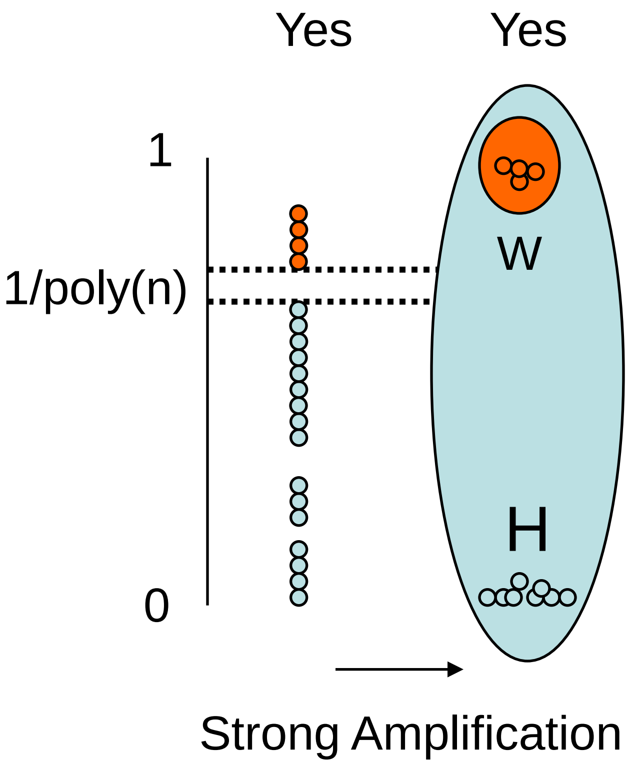
1st step: "Think out of the box", literally



Check all

Suicidal: $d \rightarrow d^d$

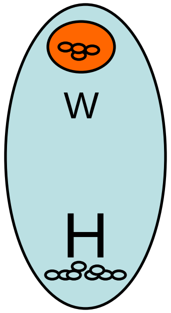
2^{nd} step: Adding proper constraints



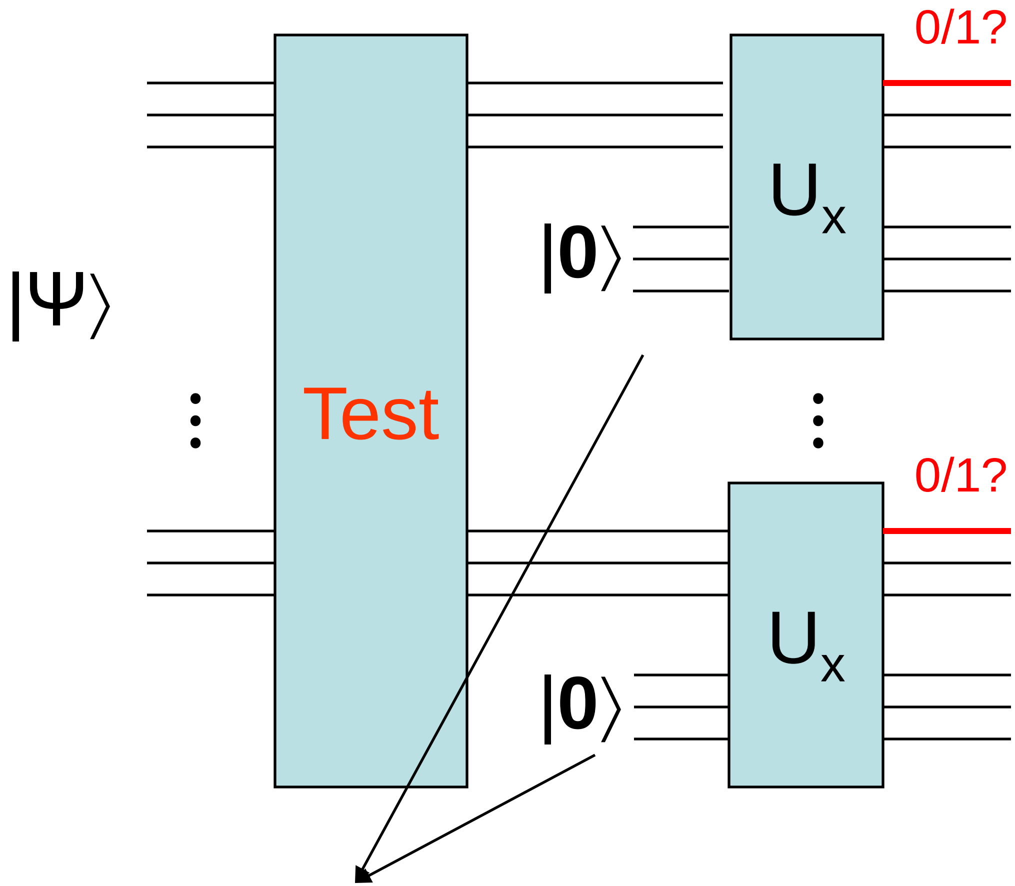
[Fact] There are 2^m orthonormal vectors $|\psi_i\rangle$, s.t. $\forall|\psi\rangle=\sum\alpha_i|\psi_i\rangle$,

$$\|U_x|\psi\mathbf{0}\rangle\|^2 = \sum|\alpha_i|^2\cdot\|U_x|\psi_i\mathbf{0}\rangle\|^2$$

2nd Step: Adding proper constraints



d = dim(W)



d copies of original circuit

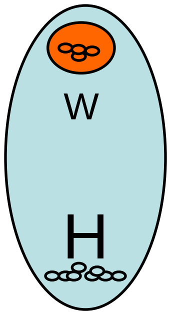
- ∃ a unique vector $|\Psi^*\rangle \in W^{\otimes d}$ passing Test w.p. 1. And it's still $|\Psi^*\rangle$.

- Any other $|\Phi\rangle \perp |\Psi^*\rangle$: after passing Test the state has one component in $W^{\perp}$.

Reminder of symmetric and alternating subspaces

In $H^{\otimes d}$ where $\dim(H) = n$:

- $S_{ij} = \{|\psi\rangle \in H^d : \pi_{ij}|\psi\rangle = |\psi\rangle\}$,
- $A_{ij} = \{|\psi\rangle \in H^d : \pi_{ij}|\psi\rangle = -|\psi\rangle\}$
- [Fact] $H^{\otimes d} = S_{ij} \oplus A_{ij}$
- $\mathrm{Alt}(H^{\otimes d}) = \cap_{i\neq j} A_{ij}$,
  - $\dim(\mathrm{Alt}(H^{\otimes d})) = \binom{n}{d}$
  - A basis: $\{\sum_\pi \mathrm{sign}(\pi)|i_{\pi(1)}\rangle|i_{\pi(2)}\rangle \ldots |i_{\pi(d)}\rangle : \text{distinct } i_1, \ldots, i_d \in [n]\}$



$d = \dim(W)$

$\dim(\mathrm{Alt}(W^{\otimes d})) = 1$

[Fact] $\mathrm{Alt}(H^{\otimes d}) \cap W^{\otimes d} = \mathrm{Alt}(W^{\otimes d})$

Alternating Test

On potential witness ρ in $H^{\otimes d}$:

ρ

- Attach $\sum_{\pi \in S\_d} |\pi\rangle$ *1 $\rightarrow \sum_\pi |\pi\rangle\, \rho$
- Permute ρ according to π (in superposition) $\rightarrow \sum_\pi |\pi\rangle\, \pi(\rho)$
- Accept if the attached reg is $\sum_\pi \mathrm{sign}(\pi) |\pi\rangle$ $= (\sum_\pi \mathrm{sign}(\pi) |\pi\rangle) \otimes \rho'$?

  by $|0\rangle \rightarrow \sum_\pi |\pi\rangle$

  $\rightarrow \sum_\pi \mathrm{sign}(\pi) |\pi\rangle$

*1: A normalization factor of $(d!)^{-1/2}$ is omitted.

For alternating states

Recall: $|\psi\rangle \in \mathrm{Alt}(H^{\otimes d})$ means $\pi_{ij}\,|\psi\rangle = -\,|\psi\rangle$

On ρ in $H^{\otimes d}$

- Attach $\sum_\pi |\pi\rangle$
- Permute ρ according to π (in superposition)
- Accept if the attached reg is $\sum_\pi \mathrm{sign}(\pi)|\pi\rangle$

$$|\psi\rangle$$

$$\to \sum_\pi |\pi\rangle\, |\psi\rangle$$

$$\to \sum_\pi |\pi\rangle\, \pi(|\psi\rangle)$$

$$= \sum_\pi |\pi\rangle\, \mathrm{sign}(\pi)|\psi\rangle$$

$$= \left(\sum_\pi \mathrm{sign}(\pi)|\pi\rangle\right) \otimes |\psi\rangle$$

For $\mathrm{Alt}(H^{\otimes d})^{\perp}$

- Recall that $H^{\otimes d} = S_{ij} \oplus A_{ij}$
- So $(\bigcap_{i\neq j} A_{ij})^{\perp} = \sum A_{ij}^{\perp} = \sum S_{ij}$
  - i.e. any state in $(\bigcap_{i\neq j} A_{ij})^{\perp}$ is $|\psi\rangle = \sum|\psi_{ij}\rangle$, where $|\psi_{ij}\rangle \in S_{ij}$.

On ρ in $H^{\otimes d}$ $\qquad |\psi_{ij}\rangle$

- Attach $\sum_{\pi}|\pi\rangle$ $\qquad \rightarrow \sum_{\pi}|\pi\rangle\,|\psi_{ij}\rangle$
- Permute ρ according to π (in superposition) $\qquad \rightarrow \sum_{\pi}|\pi\rangle\,\pi(|\psi_{ij}\rangle)$
- Accept if the attached reg is $\sum_{\pi}\mathrm{sign}(\pi)|\pi\rangle$

[Fact] The attached reg is orthogonal to $\sum_{\pi}\mathrm{sign}(\pi)|\pi\rangle$

$$\sum_\pi |\pi\rangle\, \pi(|\psi_{ij}\rangle) \quad \perp \quad \sum_\pi \mathrm{sign}(\pi)|\pi\rangle$$

- $\sum_\pi |\pi\rangle\, \pi(|\psi_{ij}\rangle)$ projected on $\sum_\sigma \mathrm{sign}(\sigma)|\sigma\rangle \otimes H^{\otimes d}$

$= \left(\sum_\sigma \mathrm{sign}(\sigma)|\sigma\rangle\right) \left(\sum_\sigma \mathrm{sign}(\sigma)\langle\sigma|\right) \sum_\pi |\pi\rangle\, \pi(|\psi_{ij}\rangle)$

$= \sum_{\sigma,\pi} \mathrm{sign}(\sigma)\, \mathrm{sign}(\pi)\, |\sigma\rangle \pi(|\psi_{ij}\rangle) \equiv a$

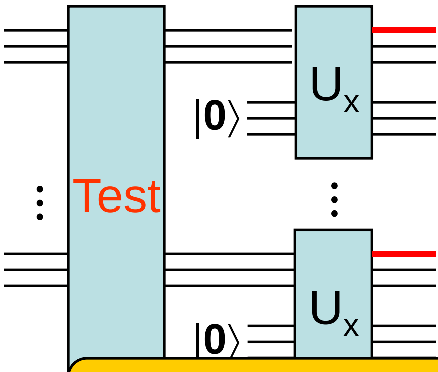
- Let $\pi = \pi' \circ \pi_{ij}$, then

$$a = \sum_{\sigma,\pi} \mathrm{sign}(\sigma)\, \underbrace{\mathrm{sign}(\pi)}_{= -\,\mathrm{sign}(\pi')}\, |\sigma\rangle \pi' \circ \underbrace{\pi_{ij}(|\psi_{ij}\rangle)}_{= |\psi_{ij}\rangle}$$

$= -\sum_{\sigma,\pi'} \mathrm{sign}(\sigma)\, \mathrm{sign}(\pi')\, |\sigma\rangle \pi'(|\psi_{ij}\rangle) = -a$

- So $a = 0$.

What we have shown?



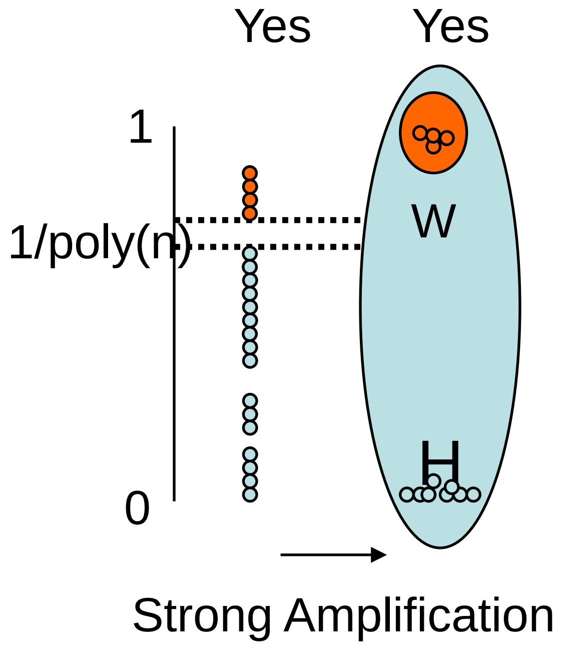
Our unique witness!

- All states in $\mathrm{Alt}(H^{\otimes d})$ pass AltTest w.p. 1.
- All states in $\mathrm{Alt}(H^{\otimes d})^{\perp}$ pass AltTest w.p. 0.
- … after AltTest, only states in $\mathrm{Alt}(H^{\otimes d})$ remain.
- But $\mathrm{Alt}(H^{\otimes d}) \cap W^{\otimes d} = \mathrm{Alt}(W^{\otimes d})$,
  - which has dim = 1 if d = dim(W).

Recall: $\mathrm{Alt}(H^{\otimes d}) = \mathrm{span}\{\sum_{\pi} \mathrm{sign}(\pi) |i_{\pi(1)}\rangle |i_{\pi(2)}\rangle \ldots |i_{\pi(d)}\rangle$: distinct $i_1, \ldots, i_d \in [2^m]\}$

Concluding remarks

- This paper reduces FewQMA to UQMA.
  - Idea of using 1-dim alternating subspace is quite different than the classical V-V.



- Open:
  - General (exp.) case?
  - Gap generation?

Thanks!