On the power of a unique quantum witness

Iordanis Kerenidis
CNRS
LRI, Univ Paris 11

Joint work with Rahul Jain, Greg Kuperberg, Miklos Santha, Or Sattath, Shengyu Zhang

The class NP

NP: Is this boolean formula satisfiable?

Send Satisfying Assignment

A promise problem $L = (L_{yes}, L_{no})$ is in NP if there exists a verification procedure V_x such that

- $x \in L_{yes}$
  there exists a witness w, st. V_x always accepts x
- $x \in L_{no}$
  for all witnesses w, V_x always rejects x.

- Verification procedure: family of circuits uniformly generated in polynomial-time

The hardness of NP

- Why are NP-complete problems so HARD?
  - The number of witnesses varies from 1 to exponential.
  - Is this variation behind their difficulty?

Valiant-Vazirani Theorem

UP: the set of promise problems in NP where in addition on positive instances there exists a unique witness

Any problem in NP can be reduced in randomized polynomial-time to a promise problem in UP, i.e.

$$NP \subseteq RP^{UP}$$

Or, if UP is "easy" then NP is "easy"

What about Quantum witnesses?

- QMA: the quantum equivalent of NP
  - Not many natural QMA-complete problems
    - Local Hamiltonians, Consistency of Density Matrices
  - Is Graph Non-Isomorphism in QMA?
    - There exists a quantum witness. How do I check it?
  - Is Perfect completeness possible?
    - Reasons to believe that it's hard to prove

What about Quantum witnesses?

- QMA: the quantum equivalent of NP
  - Not many natural QMA-complete problems
    - Local Hamiltonians, Consistency of Density Matrices
  - Is Graph Non-Isomorphism in QMA?
    - There exists a quantum witness. How do I check it?
  - Is Perfect completeness possible?
    - Reasons to believe that it's hard to prove
  - Is there a quantum Valiant-Vazirani theorem?
    [Aharonov, Ben-Or, Brandao, Sattah 2008]
    - The "Number" of witnesses can be infinite
    - Unique witnesses?

Valiant-Vazirani Theorem

- SAT: NP-complete
- Unique-SAT: UP-complete

- Valiant-Vazirani (restated)

  If there exists an efficient algorithm to solve Unique-SAT, then there exists an efficient algorithm to solve SAT

Valiant-Vazirani Theorem

- SAT: NP-complete
- Unique-SAT: UP-complete

- Valiant-Vazirani (restated)

  If there exists an efficient algorithm to solve Unique-SAT, then there exists an efficient algorithm to solve SAT

- Main tool: Family of pairwise independent hash functions

Definition

$\mathcal{H}$ is a family of pairw. ind. hash functions $h:\{0,1\}^n \to \{0,1\}^m$

if $\forall (x,y) \in \{0,1\}^n, \forall (a,b) \in \{0,1\}^m \quad \Pr_{h\in\mathcal{H}}[h(x)=a \wedge h(y)=b] = \frac{1}{2^{2m}}$

Valiant-Vazirani continued

- Let $\varphi(x_1,\ldots,x_n)$ a boolean formula
- Assume that φ has 2^k < #witnesses < 2^{k+1}

Valiant-Vazirani continued

- Let $\varphi(x_1,\ldots,x_n)$ a boolean formula
- Assume that φ has 2^k < #witnesses < 2^{k+1}

- Then, pick a random hash function $h:\{0,1\}^n \rightarrow \{0,1\}^{k+2}$ and consider the formula $\psi_k = \varphi(x_1,\ldots x_n) \wedge (h(x_1,\ldots x_n) = 0)$

Valiant-Vazirani continued

- Let $\varphi(x_1,\ldots,x_n)$ a boolean formula
- Assume that φ has 2^k < #witnesses < 2^{k+1}

- Then, pick a random hash function $h:\{0,1\}^n \to \{0,1\}^{k+2}$ and consider the formula $\psi_k = \varphi(x_1,\ldots x_n) \wedge (h(x_1,\ldots x_n) = 0)$

Claim: ψ_k has a unique witness with constant prob.

Proof: $$\Pr ob[\exists w : h(w) = 0 \wedge \forall w'\ h(w') \neq 0]$$
$$= \Pr ob[\exists w : h(w) = 0] \cdot \Pr ob[\forall w'\ h(w') \neq 0 \mid \exists w : h(w) = 0]$$
$$\geq \frac{2^k}{2^{k+2}} \cdot \left(1 - \frac{2^{k+1}}{2^{k+2}}\right) = \frac{1}{8}$$

Valiant-Vazirani algorithm

- Let $\varphi(x_1,\ldots,x_n)$ a boolean formula

Repeat t times

For k=0,…,n-1

- Pick hash function $h:\{0,1\}^n \to \{0,1\}^{k+2}$
- Construct $\psi_k = \varphi(x_1,\ldots x_n) \wedge (h(x_1,\ldots x_n) = 0)$
- Use Unique-SAT algorithm with input ψ_k
- If Unique-SAT accepts then accept and exit

Otherwise Reject

Remark

- If φ unsatisfiable, then ALL ψ_k are unsatisfiable
- If φ sat., then with prob. $1-(7/8)^t$ we accept

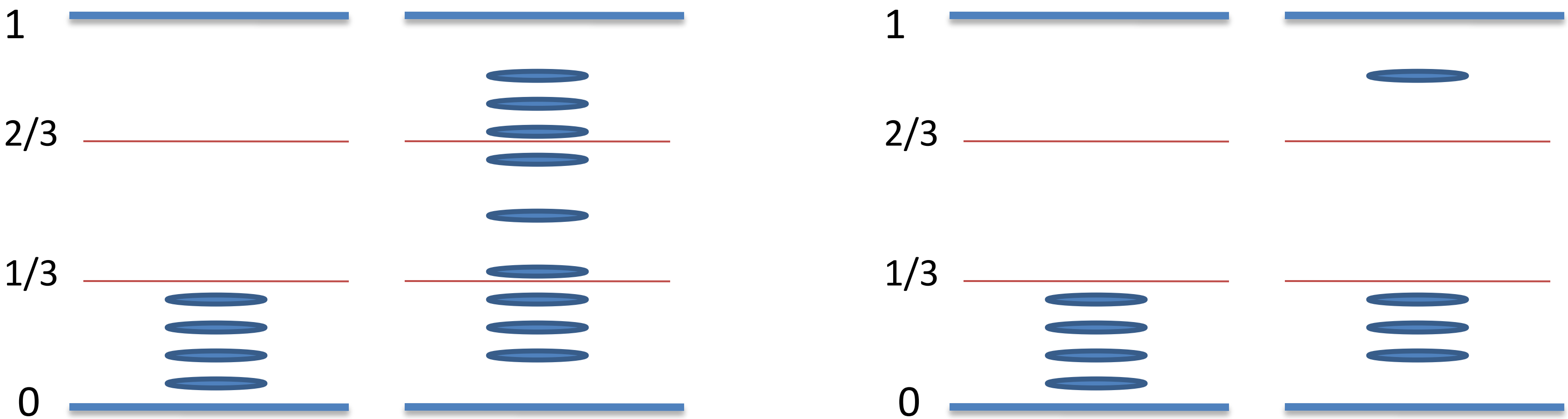
Probabilistic NP

MA: Merlin-Arthur (probabilistic NP)

$L = (L_{yes}, L_{no})$ is in MA if there exists a probabilistic verification procedure V_x st.

- $x \in L_{yes}$
  there exists a witness w, st. V_x accepts x with prob >2/3
- $x \in L_{no}$
  for all witnesses w, V_x accepts x with prob <1/3

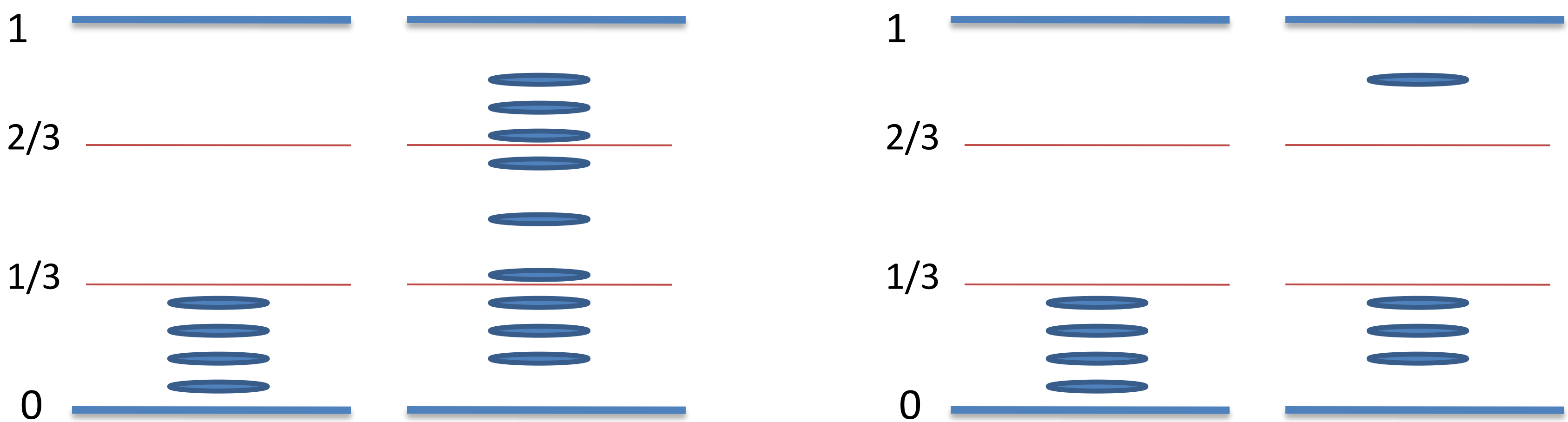
Unique MA



No and Yes instances in MA

No and Unique-Yes instances in UMA

Unique MA



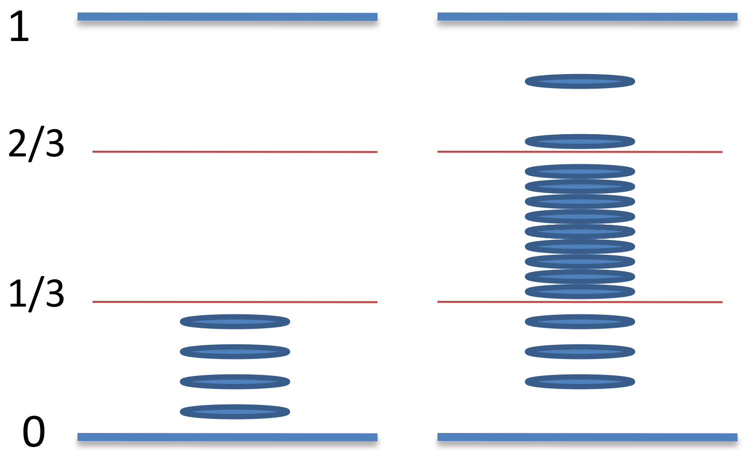
No and Yes instances in MA

No and Unique-Yes instances in UMA

L = (L_{yes},L_{no}) is in UMA if there exists a V_x st.

- $x \in L_{yes}$
  there exists a witness w, st. V_x accepts x with prob >2/3
  and for all other w', V_x accepts x with prob <1/3
- $x \in L_{no}$
  for all witnesses w, V_x accepts x w. prob. <1/3

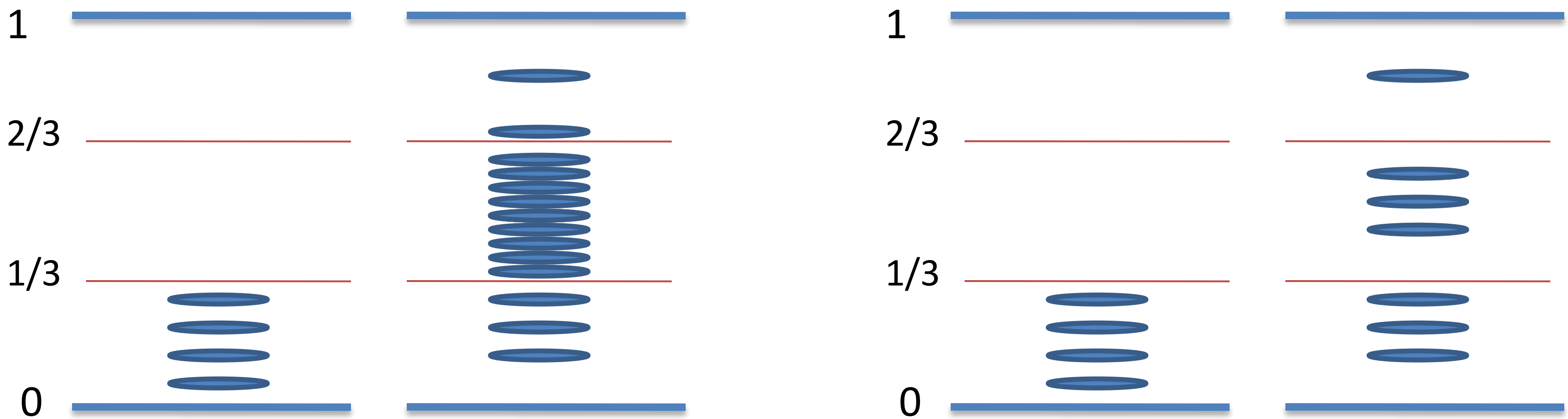
Problem with Valiant-Vazirani



No and Yes instances in MA

- Two many pseudo-witnesses compared to the real witnesses

Problem with Valiant-Vazirani

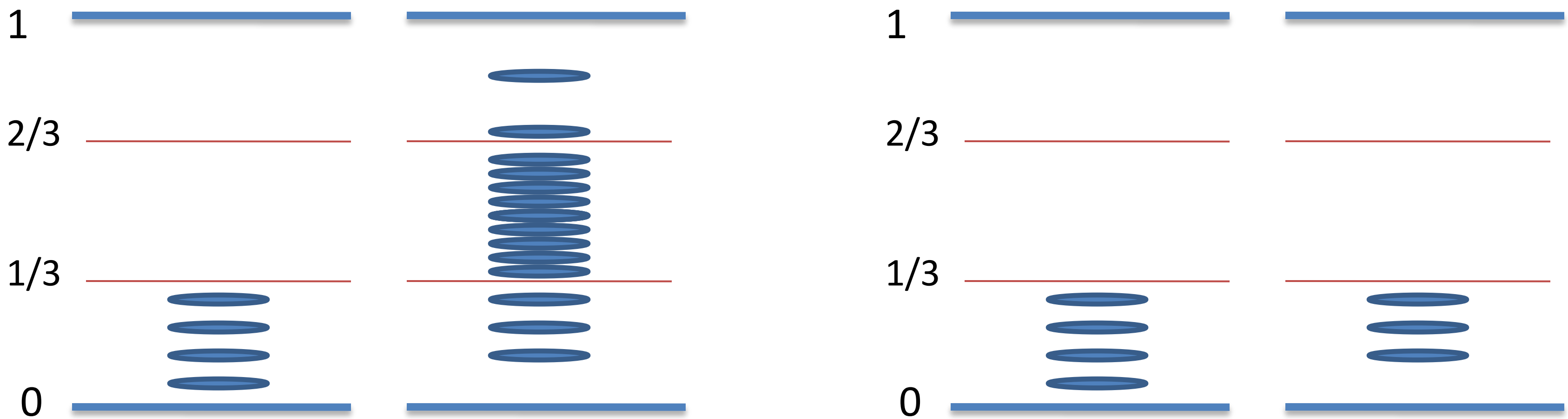


No and Yes instances in MA

No and Unique-Yes instances in UMA

- Two many pseudo-witnesses compared to the real witnesses
- If the hashing leaves one witness, then many pseudo-witnesses survive!

Problem with Valiant-Vazirani

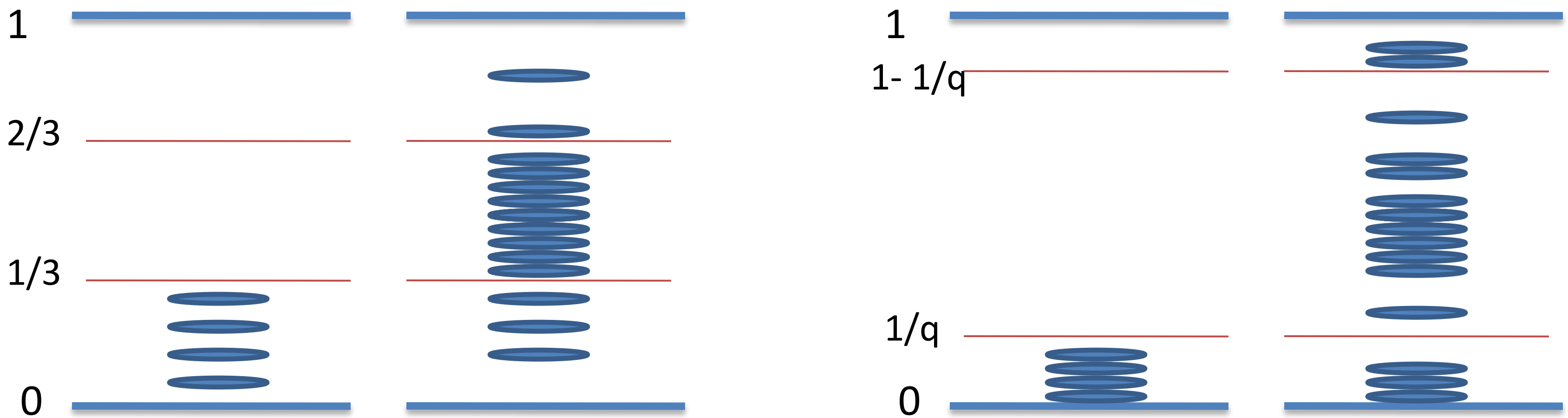


No and Yes instances in MA

No and Unique-Yes instances in UMA

- Two many pseudo-witnesses compared to the real witnesses
- If the hashing leaves one witness, then many pseudo-witnesses survive!
- If the hashing kills all pseudo-witnesses, then no witness survives

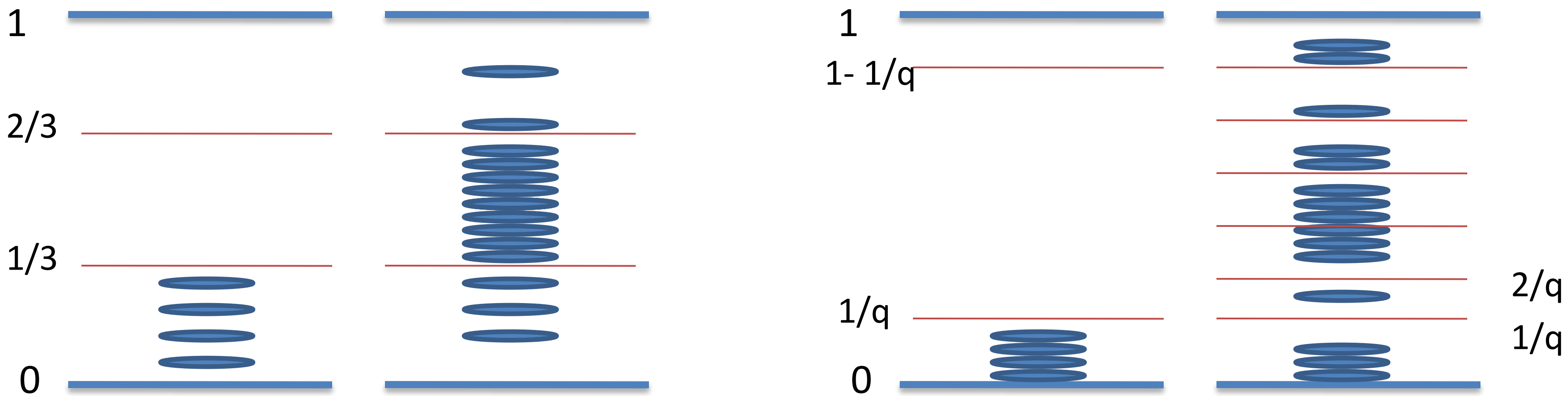
Aharonov et al. solution



No and Yes instances in MA

No and Unique-Yes instances in UMA

Aharonov et al. solution

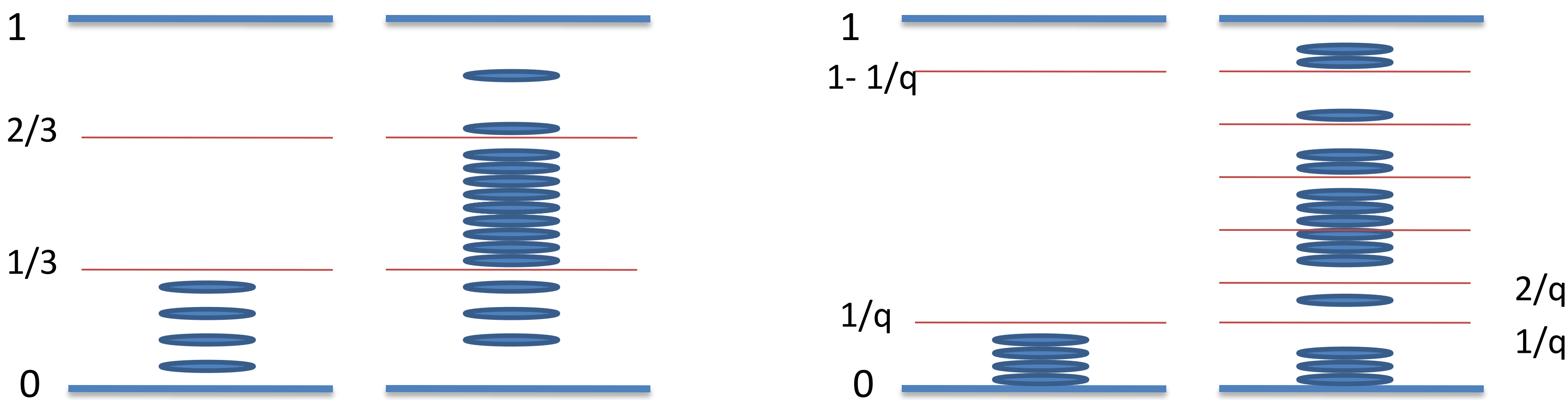


No and Yes instances in MA

No and Unique-Yes instances in UMA

Claim: There exists at least one interval where the pseudo-witnesses are no more than triple the witnesses

Aharonov et al. solution



No and Yes instances in MA

No and Unique-Yes instances in UMA

Claim: There exists at least one interval where the pseudo-witnesses are no more than triple the witnesses

V-V works with constant probability for this interval!

Quantum NP

QMA: Quantum Merlin-Arthur (probabilistic NP)

Quantum witness

$L = (L_{yes}, L_{no})$ is in QMA if there exists a quantum verification procedure V_x st.

- $x \in L_{yes}$

  there exists a quantum witness $|w\rangle$, such that V_x accepts x with prob >2/3.

- $x \in L_{no}$

  for all witnesses $|w\rangle$, V_x accepts x with prob <1/3

QMA and number of witnesses

- Infinite number of witnesses
  - Any $|w'\rangle \cong |w\rangle$ is still a witness
  - The right "number": Dimension of witness subspace

QMA and number of witnesses

- Infinite number of witnesses
  - Any $|w'\rangle \cong |w\rangle$ is still a witness
  - The right "number": Dimension of witness subspace

QMA

$L = (L_{yes}, L_{no})$ is in QMA if there exists V_x st.

- $x \in L_{yes}$

  there exists witness $|w\rangle$, st. V_x accepts x with prob >2/3
- $x \in L_{no}$

  for all witnesses $|w\rangle$, V_x accepts x with prob. <1/3

QMA and number of witnesses

- Infinite number of witnesses
  - Any $|w'\rangle \cong |w\rangle$ is still a witness
  - The right "number": Dimension of witness subspace

QMA

$L = (L_{yes}, L_{no})$ is in QMA if there exists V_x st.

- $x \in L_{yes}$

  there exists a subspace W_x of dimension at least 1, st.
  for all $|w\rangle$ in W_x, V_x accepts x with prob >2/3
- $x \in L_{no}$

  for all witnesses $|w\rangle$, V_x accepts x with prob. <1/3

QMA and number of witnesses

QMA

$L = (L_{yes}, L_{no})$ is in QMA if there exists V_x st.

- $x \in L_{yes}$

  there exists a subspace W_x of dimension at least 1, st.

  for all $|w\rangle$ in W_x, V_x accepts x with prob >2/3
- $x \in L_{no}$

  for all witnesses $|w\rangle$, V_x accepts x with prob. <1/3

QMA and number of witnesses

QMA

$L = (L_{yes}, L_{no})$ is in QMA if there exists V_x st.

- $x \in L_{yes}$
  there exists a subspace W_x of dimension at least 1, st.
  for all $|w\rangle$ in W_x, V_x accepts x with prob >2/3
- $x \in L_{no}$
  for all witnesses $|w\rangle$, V_x accepts x with prob. <1/3

UQMA

$L = (L_{yes}, L_{no})$ is in UQMA if there exists V_x st.

- $x \in L_{yes}$
  there exists a subspace W_x of dimension EXACTLY 1, st.
  for all $|w\rangle$ in W_x, V_x accepts x with prob >2/3 and
  for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3
- $x \in L_{no}$
  for all witnesses $|w\rangle$, V_x accepts x with prob. <1/3

Quantum Valiant-Vazirani

- Is there a quantum Valiant-Vazirani theorem?

  [Aharonov, Ben-Or, Brandao, Sattah 2008]

<u>Quantum Valiant-Vazirani</u> Efficient algorithm for UQMA $\Longrightarrow$ Efficient algorithm for QMA

Remark: [ABBS08]

- Extended Valiant-Vazirani theorem for MA and QCMA.
  - Hashing
  - Taking care of the promise

Our result

QMA: dimension(Witness subspace W_x) $\geq$ 1

UQMA: dimension(Witness subspace W_x) = 1

for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3

Our result

QMA: dimension(Witness subspace W_x) $\geq$ 1

UQMA: dimension(Witness subspace W_x) = 1

for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3

FewQMA

- Poly(input size) $\geq$ dimension(Witness subspace W_x) $\geq$ 1
- for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3

Our result

QMA: dimension(Witness subspace W_x) $\geq$ 1

UQMA: dimension(Witness subspace W_x) = 1

for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3

FewQMA

- Poly(input size) $\geq$ dimension(Witness subspace W_x) $\geq$ 1
- for all $|w\rangle$ in $W_x^{\perp}$, V_x accepts x with prob <1/3

Theorem

Efficient algorithm for UQMA

$\Rightarrow$ Efficient algorithm for FewQMA

or

Any problem in FewQMA can be reduced in deterministic polytime to a promise problem in UQMA, i.e. FewQMA $\subseteq$ P^{UQMA}

The 2-dimensional case

- QMA problem (open question in [ABBS08])
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^{\perp}$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

The 2-dimensional case

- QMA problem (open question in [ABBS08])
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^{\perp}$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

- Quantum analog of Valiant-Vazirani
  - Pick a random subspace R
  - New witnesses: old witnesses + Projection on R

  - It doesn't work!!! [ABBS08]
  - The projections of any two vectors on a random subspace of dimension K has expectation K/N and variance $\sqrt{K}/N$

The 2-dimensional case

- QMA problem
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^{\perp}$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

The 2-dimensional case

- QMA problem
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^{\perp}$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

- Two orthogonal witnesses $|w_1\rangle$, $|w_2\rangle$

The 2-dimensional case

- QMA problem
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^\perp$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

- Two orthogonal witnesses $|w_1\rangle$, $|w_2\rangle$

- Give both witnesses: $|w_1\rangle|w_2\rangle$ (But also $|w_2\rangle|w_1\rangle$)

The 2-dimensional case

- QMA problem
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^{\perp}$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

- Two orthogonal witnesses $|w_1\rangle$, $|w_2\rangle$

- Give both witnesses: $|w_1\rangle|w_2\rangle$ (But also $|w_2\rangle|w_1\rangle$)

- How about a superposition of the two witnesses?
  - $|w_1\rangle|w_2\rangle+|w_2\rangle|w_1\rangle$
    Symmetric. But $|w_1\rangle|w_1\rangle+|w_2\rangle|w_2\rangle$ and $|w_1\rangle|w_1\rangle-|w_2\rangle|w_2\rangle$

The 2-dimensional case

- QMA problem
  - Yes: a 2-dimensional subspace W_x st. V_x accepts w.p. 1
    for any $|w\rangle$ in $W_x^\perp$ V_x accepts w.p. 0
  - No: for any $|w\rangle$, V_x accepts w.p. 0

- Two orthogonal witnesses $|w_1\rangle$, $|w_2\rangle$

- Give both witnesses: $|w_1\rangle|w_2\rangle$ (But also $|w_2\rangle|w_1\rangle$)

- How about a superposition of the two witnesses?
  - $|w_1\rangle|w_2\rangle+|w_2\rangle|w_1\rangle$
    Symmetric. But $|w_1\rangle|w_1\rangle+|w_2\rangle|w_2\rangle$ and $|w_1\rangle|w_1\rangle-|w_2\rangle|w_2\rangle$
  - Et voila: $|w_1\rangle|w_2\rangle-|w_2\rangle|w_1\rangle$

    The only alternating state that is also a witness!

Proof sketch for FewQMA

- Let L a problem in FewQMA and $W \subseteq H$ the witness subspace ($1 \leq \dim(W) = d \leq q(|x|)$, $\dim(H) = K$)

Proof sketch for FewQMA

- Let L a problem in FewQMA and $W \subseteq H$ the witness subspace ($1 \leq \dim(W) = d \leq q(|x|)$, $\dim(H) = K$)
- We need to describe a one-dimensional subspace st.
  1. It should be easy to perform the projection onto it
  2. Everything orthogonal should be rejected

Proof sketch for FewQMA

- Let L a problem in FewQMA and $W \subseteq H$ the witness subspace $(1 \leq \dim(W) = d \leq q(|x|)$, $\dim(H) = K)$

- We need to describe a one-dimensional subspace st.
  1. It should be easy to perform the projection onto it
  2. Everything orthogonal should be rejected

- First, we look at $H^{\otimes t}$
  - This seems bad, since the dimension of $W^{\otimes t}$ grows as d^t

Proof sketch for FewQMA

- Let L a problem in FewQMA and $W \subseteq H$ the witness subspace ($1 \leq \dim(W) = d \leq q(|x|)$, $\dim(H) = K$)

- We need to describe a one-dimensional subspace st.
  1. It should be easy to perform the projection onto it
  2. Everything orthogonal should be rejected

- First, we look at $H^{\otimes t}$
  - This seems bad, since the dimension of $W^{\otimes t}$ grows as d^t

- Then, look at the Alternating subspace of $H^{\otimes t}$, $Alt_{H^{\otimes t}}$

$$\dim(Alt_{H^{\otimes t}}) = \binom{K}{t}$$

Proof sketch for FewQMA

- Let L a problem in FewQMA and $W \subseteq H$ the witness subspace ($1 \leq \dim(W) = d \leq q(|x|)$, $\dim(H) = K$)

- We need to describe a one-dimensional subspace st.
  1. It should be easy to perform the projection onto it
  2. Everything orthogonal should be rejected

- First, we look at $H^{\otimes t}$
  - This seems bad, since the dimension of $W^{\otimes t}$ grows as d^t

- Then, look at the Alternating subspace of $H^{\otimes t}$, $Alt_{H^{\otimes t}}$

$$\dim(Alt_{H^{\otimes t}}) = \binom{K}{t}$$

- What is the intersection of $Alt_{H^{\otimes t}}$ and $W^{\otimes t}$?

The unique quantum witness

- $Alt_{H^{\otimes t}} \cap W^{\otimes t} = Alt_{W^{\otimes t}}$ and $\dim(Alt_{W^{\otimes t}}) = \binom{\dim(W)}{t} = \binom{d}{t}$
- So this will be our unique witness by taking t=d!

The unique quantum witness

- $Alt_{H^{\otimes t}} \cap W^{\otimes t} = Alt_{W^{\otimes t}}$ and $\dim(Alt_{W^{\otimes t}}) = \binom{\dim(W)}{t} = \binom{d}{t}$
- So this will be our unique witness by taking t=d!

BUT

1. We don't know d. Yes, but d is a most q(|x|), so we can check all possible t's from 1 to q.

The unique quantum witness

- $Alt_{H^{\otimes t}} \cap W^{\otimes t} = Alt_{W^{\otimes t}}$ and $\dim(Alt_{W^{\otimes t}}) = \binom{\dim(W)}{t} = \binom{d}{t}$
- So this will be our unique witness by taking t=d!

BUT

1. We don't know d. Yes, but d is a most q(|x|), so we can check all possible t's from 1 to q.

2. How can the Verifier perform the projection on $Alt_{W^{\otimes t}}$?

   Claim: The projections on $Alt_{H^{\otimes t}}$ and $W^{\otimes t}$ commute.

   Hence, it suffices to perform $\prod_{W^{\otimes t}} \cdot \prod_{Alt_{H^{\otimes t}}}$

The unique quantum witness

- $Alt_{H^{\otimes t}} \cap W^{\otimes t} = Alt_{W^{\otimes t}}$ and $\dim(Alt_{W^{\otimes t}}) = \binom{\dim(W)}{t} = \binom{d}{t}$
- So this will be our unique witness by taking t=d!

BUT

1. We don't know d. Yes, but d is a most q(|x|), so we can check all possible t's from 1 to q.

2. How can the Verifier perform the projection on $Alt_{W^{\otimes t}}$?

   Claim: The projections on $Alt_{H^{\otimes t}}$ and $W^{\otimes t}$ commute.

   Hence, it suffices to perform $\prod_{W^{\otimes t}} \cdot \prod_{Alt_{H^{\otimes t}}}$

3. Are the states orthogonal to $Alt_{W^{\otimes t}}$ rejected?

Rejecting the orthogonal states

- Our unique quantum witness is $Alt_{W^{\otimes t}}$
- The Verifier performs $\Pi_{W^{\otimes t}} \cdot \Pi_{Alt_{H^{\otimes t}}}$

Rejecting the orthogonal states

- Our unique quantum witness is $Alt_{W^{\otimes t}}$
- The Verifier performs $\prod_{W^{\otimes t}} \cdot \prod_{Alt_{H^{\otimes t}}}$

  - Let $|\varphi\rangle \perp Alt_{W^{\otimes t}} = Alt_{H^{\otimes t}} \cap W^{\otimes t}$

  - Then, $|\varphi\rangle = |\varphi_1\rangle + |\varphi_2\rangle, \quad |\varphi_1\rangle \perp Alt_{H^{\otimes t}}, |\varphi_2\rangle \perp W^{\otimes t}$

Rejecting the orthogonal states

- Our unique quantum witness is $Alt_{W^{\otimes t}}$
- The Verifier performs $\prod_{W^{\otimes t}} \cdot \prod_{Alt_{H^{\otimes t}}}$

  - Let $|\varphi\rangle \perp Alt_{W^{\otimes t}} = Alt_{H^{\otimes t}} \cap W^{\otimes t}$

  - Then, $|\varphi\rangle = |\varphi_1\rangle + |\varphi_2\rangle, \quad |\varphi_1\rangle \perp Alt_{H^{\otimes t}}, |\varphi_2\rangle \perp W^{\otimes t}$

  - $|\varphi_1\rangle$ is rejected by $\prod_{Alt_{H^{\otimes t}}}$, $|\varphi_2\rangle$ is rejected by $\prod_{W^{\otimes t}}$

The Alternating Test

- $\Pi_{Alt_{H^{\otimes t}}}$
- For t=2, this is exactly the SWAP Test
- [Barenko et al.] Symmetric Test for any t.

Input: $|\psi\rangle \in H^{\otimes t}$

- Create $\frac{1}{t!}\sum_{\pi}|\pi\rangle \otimes |\psi\rangle$
- Apply Unitary $U: |\pi\rangle \otimes |\psi\rangle \rightarrow |\pi\rangle \otimes SWAP_{\pi}|\psi\rangle$
- Accept is first register is $\frac{1}{t!}\sum_{\pi}(-1)^{sign(\pi)}|\pi\rangle$

The Witness Test

- $\Pi_{W^{\otimes t}}$
- We cannot do this projection exactly. W is unknown!
- But we have the procedure V_x that almost does it

Input: $|\psi\rangle \in H^{\otimes t}$

- For all registers 1 to t
  - Apply the procedure V_x
- Output Accept iff V_x always outputs accept

- This Test doesn't Commute with the Alt Test!
- Technical claim shows that it still works

The Final Algorithm

Input: $x \in L$

Witness: $for \quad t=1,\ldots,q(|x|), \quad |\psi_t\rangle \in H^{\otimes t}$

- For all t=1,…,q(|x|)
  - Apply the Alternating Test(t)
  - Apply the Witness Test(t)
  - If both tests output Accept then Accept and Halt
- Output Reject

Conclusions

- How important is the dimension of the quantum witness?
  - Our result: FewQMA is no harder than UQMA
  - Ultimate Goal: QMA is no harder than UQMA

Remarks

- New techniques, different from Valiant-Vazirani
- Our reduction is deterministic. Quite unlikely for QMA.