The complexity of poly-gapped Hamiltonians

(Extending Valiant-Vazirani Theorem to the probabilistic and quantum settings)

Fernando G.S.L. Brandão

joint work with

Dorit Aharonov, Michael Ben-Or and Or Sattath

(Hebrew University of Jerusalem)

(arXiv:0810.4840)

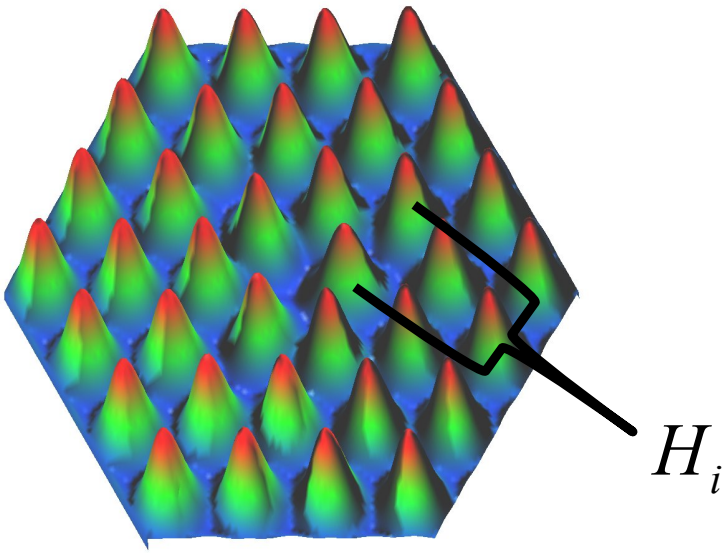
ESI, Vienna 12/08/09

Imperial College London

Institute for Mathematical Sciences

QIC

The Local Hamiltonian Problem



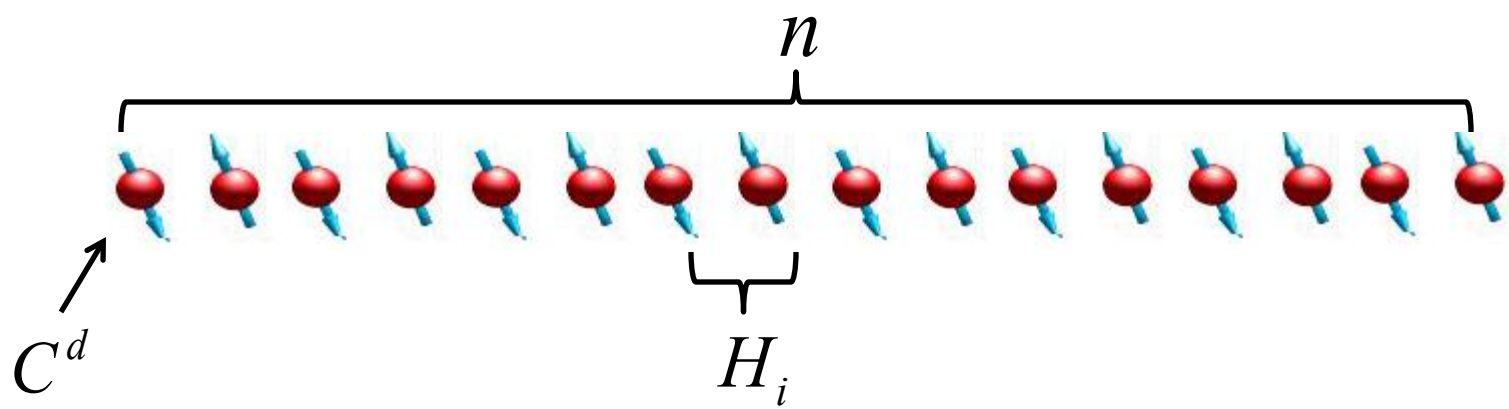
- Is the groundstate energy of

$$H = \sum_i H_i$$

below **a** or above **b** ?

$$\left(b - a \geq 1/\, poly(n)\right)$$

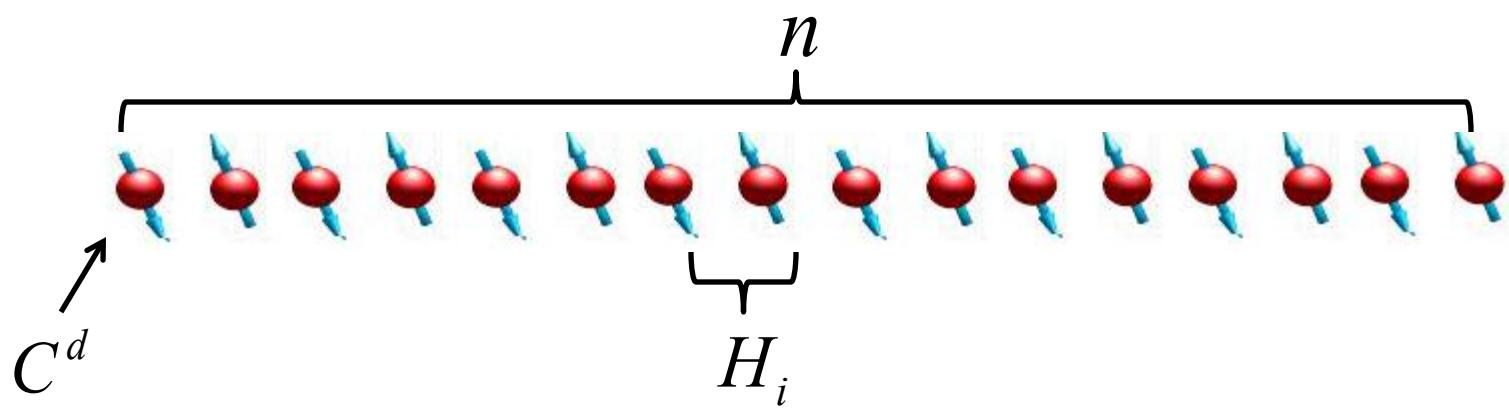
The Local Hamiltonian Problem



- One-dimensional chains are as hard as the general case (Aharonov, Gottesman, Irani, Kempe 07)

- Can we reduce it even further?
(frustration freeness, translation invariance, gap...)

The Local Hamiltonian Problem



Spectral gap: $\Delta(H) = E_1(H) - E_0(H)$

- Non-critical, *gapped* ($\Delta(H) = \Omega(1)$) 1-D models are easier (Hastings 07)

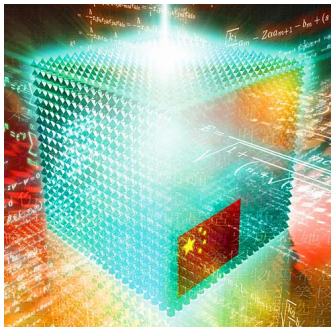
- **THIS TALK: What about for poly-gapped Hamiltonians ($\Delta(H) = 1/poly(n)$)?**

Quantum Merlin Arthur

Quantum Merlin Arthur

Quantum Merlin Arthur

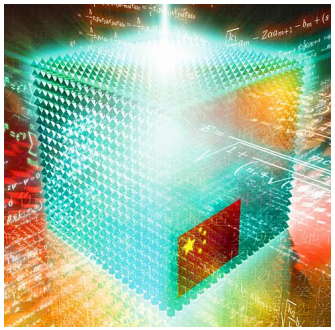
$$|\Psi\rangle$$



Quantum Computer

Quantum Merlin Arthur

$$|\Psi\rangle$$



Quantum Computer

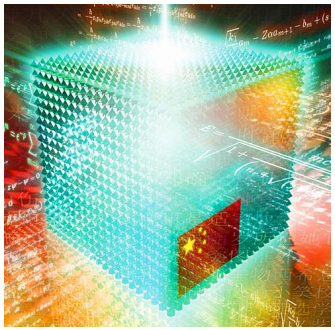
A language **L** is in QMA if for every x in **L**:

QMA:

- YES instance: Merlin can convince Arthur with probability > 2/3

Quantum Merlin Arthur

$$|\Psi\rangle$$



Quantum Computer

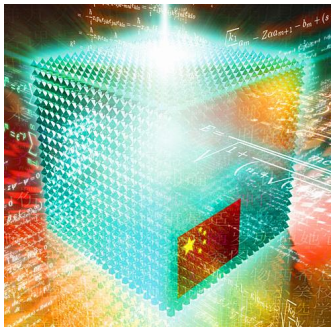
A language **L** is in QMA if for every x in **L**:

QMA:

- YES instance: Merlin can convince Arthur with probability > 2/3
- NO instance: Merlin cannot convince Arthur with probability > 1/3

Quantum Merlin Arthur

$$|0,1,0,\ldots\rangle$$



Quantum Computer

VARIANTS:

- QCMA: Merlin's proof is *classical*

Quantum Merlin Arthur

$$|0,1,0,\ldots\rangle$$

Classical Computer

VARIANTS:

- QCMA: Merlin's proof is *classical*
- MA: Merlin's proof is classical, Arthur only has a *classical* computer

Quantum Merlin Arthur

$$|0,1,0,\ldots\rangle$$

Classical Computer

VARIANTS:

- QCMA: Merlin's proof is *classical*
- MA: Merlin's proof is classical, Arthur only has a *classical* computer
- NP: Same as MA, but decisions are deterministic
  (YES instance: always accept
  NO instance: always reject)

A complex state of belief

- We conjecture that

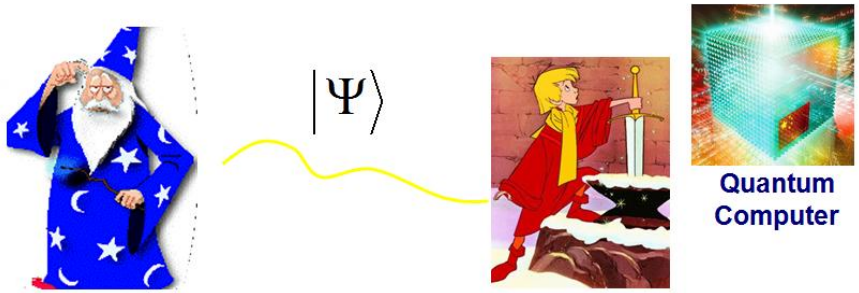
NP not equal to QMA, QCMA

(quantum helps)

- ...and that we cannot solve all the problems in NP, QCMA, QMA efficiently even on a quantum computer

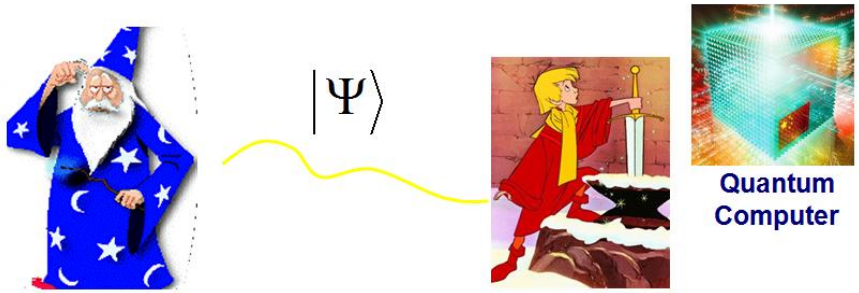
(checking is easier than solving)

The Local Hamiltonian Problem



- The LH problem is QMA-complete (Kitaev 00)
- It's QMA-complete already for 1-D Hamiltonians (Aharonov, Gottesman, Irani, Kempe 07)
- It's in NP for gapped 1-D Hamiltonians (Hastings 07)

The Local Hamiltonian Problem



- The LH problem is QMA-complete (Kitaev 00)

- It's QMA-complete already for 1-D Hamiltonians (Aharonov, Gottesman, Irani, Kempe 07)

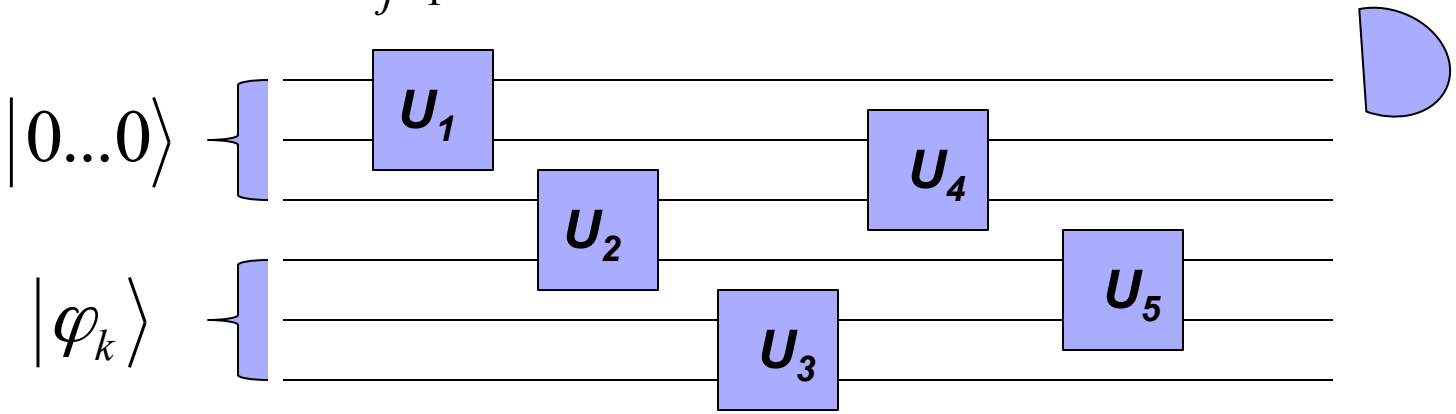
- It's in NP for gapped 1-D Hamiltonians (Hastings 07)

- For poly-gapped Hamiltonians, is it still QMA-complete, or is it perhaps in NP?

Poly-gapped Hamiltonians

- Using Kitaev construc. we can encode any QMA problem into a local Hamiltonian *H* (with ||H|| < poly(n)) whose low-lying energy space is (approx.) spanned by

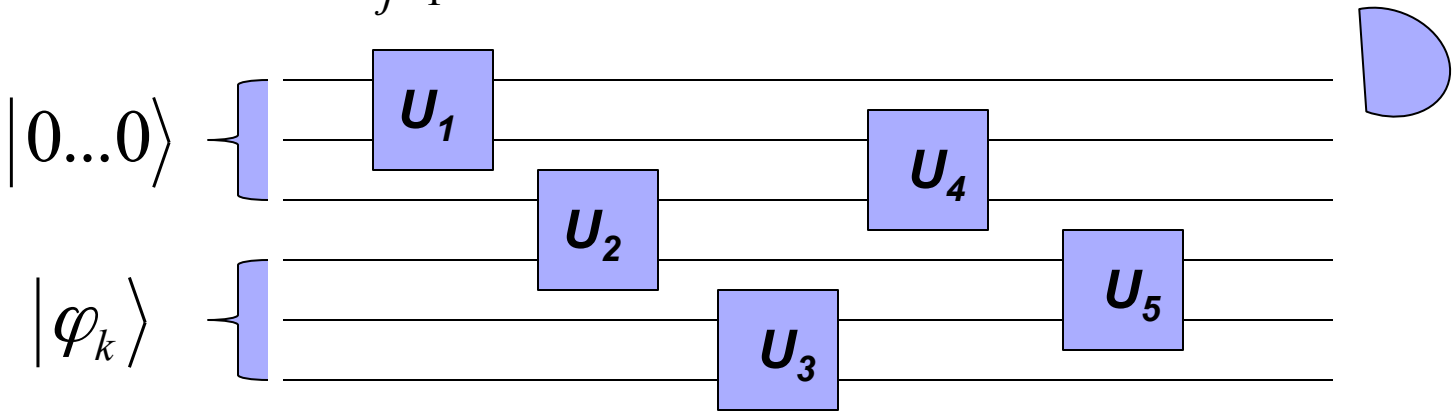
$$|\psi_k\rangle := N^{-1}\sum_{j=1} U_j U_{j-1} \ldots U_1 |\varphi_k, 0\ldots0\rangle \otimes |j\rangle$$



Poly-gapped Hamiltonians

- Using Kitaev construc. we can encode any QMA problem into a local Hamiltonian *H* (with ||H|| < poly(n)) whose low-lying energy space is (approx.) spanned by

$$|\psi_k\rangle := N^{-1}\sum_{j=1} U_j U_{j-1} \ldots U_1 |\varphi_k, 0\ldots 0\rangle \otimes |j\rangle$$

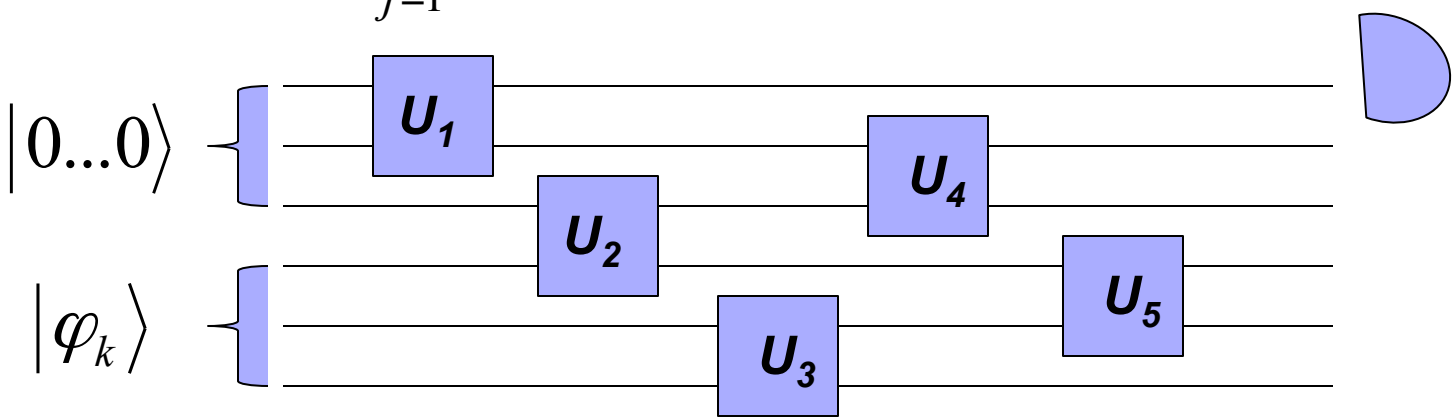


- This eigenspace is separated by 1/poly(N) from the rest of the spectrum

Poly-gapped Hamiltonians

- Using Kitaev construc. we can encode any QMA problem into a local Hamiltonian *H* (with ||H|| < poly(n)) whose low-lying energy space is (approx.) spanned by

$$|\psi_k\rangle := N^{-1}\sum_{j=1} U_j U_{j-1}\ldots U_1 |\varphi_k, 0\ldots 0\rangle \otimes |j\rangle$$



- This eigenspace is separated by 1/poly(N) from the rest of the spectrum

- $\langle\psi_k|H|\psi_k\rangle \propto 1 - \Pr(\varphi_k \ is \ accepted)$

Poly-gapped Hamiltonians

- If we want a poly-gap, we should make sure there is a quantum witness (proof) which is accepted with *higher* probability than the others

Poly-gapped Hamiltonians

- If we want a poly-gap, we should make sure there is a quantum witness (proof) which is accepted with *higher* probability than the others

- Def **UQMA** (Unique QMA):
  - NO instances: same as QMA
  - YES instances: there is a quantum state which is accepted with prob. > 2/3 and ALL states orthogonal to it are accepted with prob. at most 1/3

Poly-gapped Hamiltonians

- If we want a poly-gap, we should make sure there is a quantum witness (proof) which is accepted with higher probability than the others

- Def **UQMA** (Unique QMA):
  - NO instances: same as QMA
  - YES instances: there is a quantum state which is accepted with prob. > 2/3 and ALL states orthogonal to it are accepted with prob. at most 1/3

- Local Hamiltonians associated to UQMA are poly-gapped

- So the question is: Does UQMA = QMA ????

A classical interlude

- We can ask a similar question about NP...

- Def **UNP** (Unique NP, also called UP):
  - NO instances: same as NP
  - YES instances: there is a unique witness which is accepted

Problems wit

Are they in some s

case?

Valiant-Vazirani Theorem

+

≠

(Valiant-Vazirani 85): UNP is as hard as NP
(UNP = NP under *randomized reductions*)

- Many applications: Toda's theorem ($PH \subseteq \#P$), Braverman's proof of Linial-Nisan conjecture (a few months ago), etc...

Valiant-Vazirani Theorem

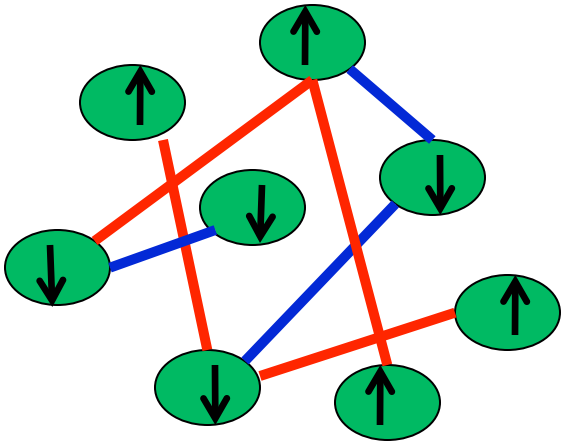
Main idea (randomized reduction): There is an efficient probabilistic mapping from e.g. 3SAT (classical Local Hamiltonians) instance C into poly many instances C_i such that

- If C is unsatisfiable (has positive energy), then all C_i are unsatisfiable (have positive energy) too

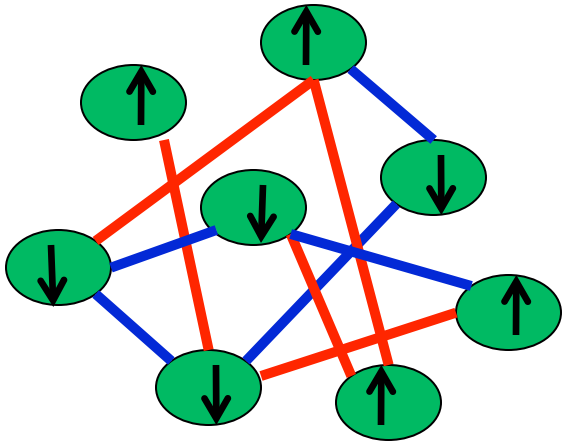
- If C satisfiable (has zero energy), then w.h.p there is at least one i such that C_i satisfiable (has zero energy) with a *unique* satisfying assignment (ground state)

Local Hamiltonian problem for classical models

Alias the Constraint Satisfaction Problem



VV
mapping



-Ferromagnetic
- Antiferromagnetic

- Tool to remove degeneracy of the groundspace!

Proof of Valiant-Vazirani Theorem

Def: (Universal Hash Functions) A family of functions $H:\{0,1\}^n \rightarrow \{0,1\}^k$ is a 2-hash function if

- $\forall a \in \{0,1\}^n, \forall b \in \{0,1\}^k,\ \Pr_{h \in H}(h(a)=b)=2^{-k}$
- $\forall a_1 \neq a_2 \in \{0,1\}^n, \forall b_1, b_2 \in \{0,1\}^k,\ \Pr_{h \in H}(h(a_2)=b_2 \mid h(a_1)=b_1)=2^{-k}$

The randomized reduction: Given a formula *C*, we build formulas C_k which are satisfiable by *x* if

- *C* is satisfiable by *x*
- $h(x)=0^k$, for a hash function from *n* to *k* bits taken at random

Proof of Valiant-Vazirani Theorem

NO instances**:** Easy, if C is not satisfiable, then neither are the C_k *!*

Proof of Valiant-Vazirani Theorem

NO instances**:** Easy, if *C* is not satisfiable, then neither are the C_k *!*

YES instances: we would like that, with some probability, there is a *k* such that C_k has *exactly one* satisfiable assignment. Let *S* be the set of witnesses and set *k* such that $2^{k-2} \leq |S| \leq 2^{k-1}$

$$\Pr_{h \in H}(|S \cap h^{-1}(0^k)| = 1)$$

$$\geq 1/8$$

Proof of Valiant-Vazirani Theorem

NO instances**:** Easy, if *C* is not satisfiable, then neither are the C_k *!*

YES instances: we would like that, with some probability, there is a *k* such that C_k has *exactly one* satisfiable assignment. Let *S* be the set of witnesses and set *k* such that $2^{k-2} \leq |S| \leq 2^{k-1}$

$$\Pr_{h\in H}(|S \cap h^{-1}(0^k)| = 1) = \sum_{x\in S} \Pr_{h\in H}(h(x) = 0^k \wedge \forall y \in S - \{x\}, h(y) \neq 0)$$

$$= \sum_{x\in S} \Pr_{h\in H}(h(x) = 0^k) \Pr_{h\in H}(\forall y \in S - \{x\}, h(y) \neq 0 \mid h(x) = 0^k)$$

$$\geq \sum_{x\in S} 2^{-k}(1 - \Pr_{h\in H}(\exists y \in S - \{x\}, h(y) \neq 0 \mid h(x) = 0^k))$$

$$\geq \sum_{x\in S} 2^{-k}(1 - \sum_{y\in S-\{x\}} \Pr_{h\in H}(h(y) \neq 0 \mid h(x) = 0^k)) \geq |S|\, 2^{-k}(1 - |S|\, 2^{-k}) \geq 1/8$$

Proof of Valiant-Vazirani Theorem

NO instances**:** Easy, if *C* is not satisfiable, then neither are the C_k *!*

YES instances: we would like that, with some probability, there is a *k* such that C_k has *exactly one* satisfiable assignment. Let *S* be the set of witnesses and set *k* such that $2^{k-2} \leq |S| \leq 2^{k-1}$

$$\Pr_{h \in H}(|S \cap h^{-1}(0^k)| = 1)$$

$$\geq 1/8$$

Valiant-Vazirani for MA and QCMA ??

NO instance

YES instance

UNIQUE YES instance

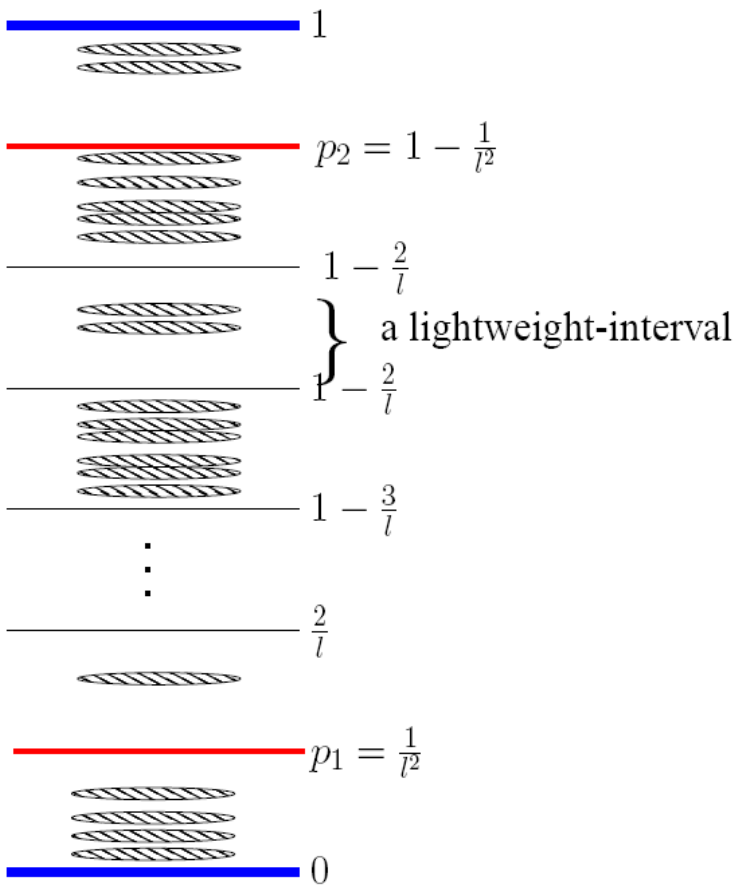
A naive application of the VV reduction might choose a witness from the “limbo” interval $[p_1, p_2]$

Main result

UQCMA = QCMA and **UMA = MA** (under randomized reductions)

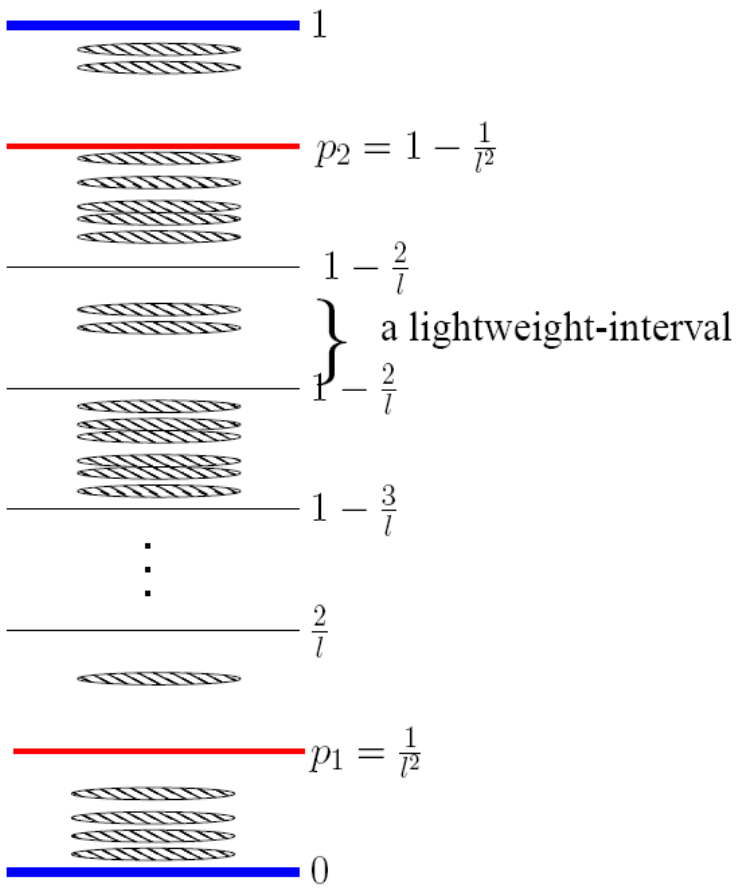
Valiant-Vazirani for MA

Solution: divide the [p_1, p_2] interval into *poly(n)* intervals (m^2 would do):



Valiant-Vazirani for MA

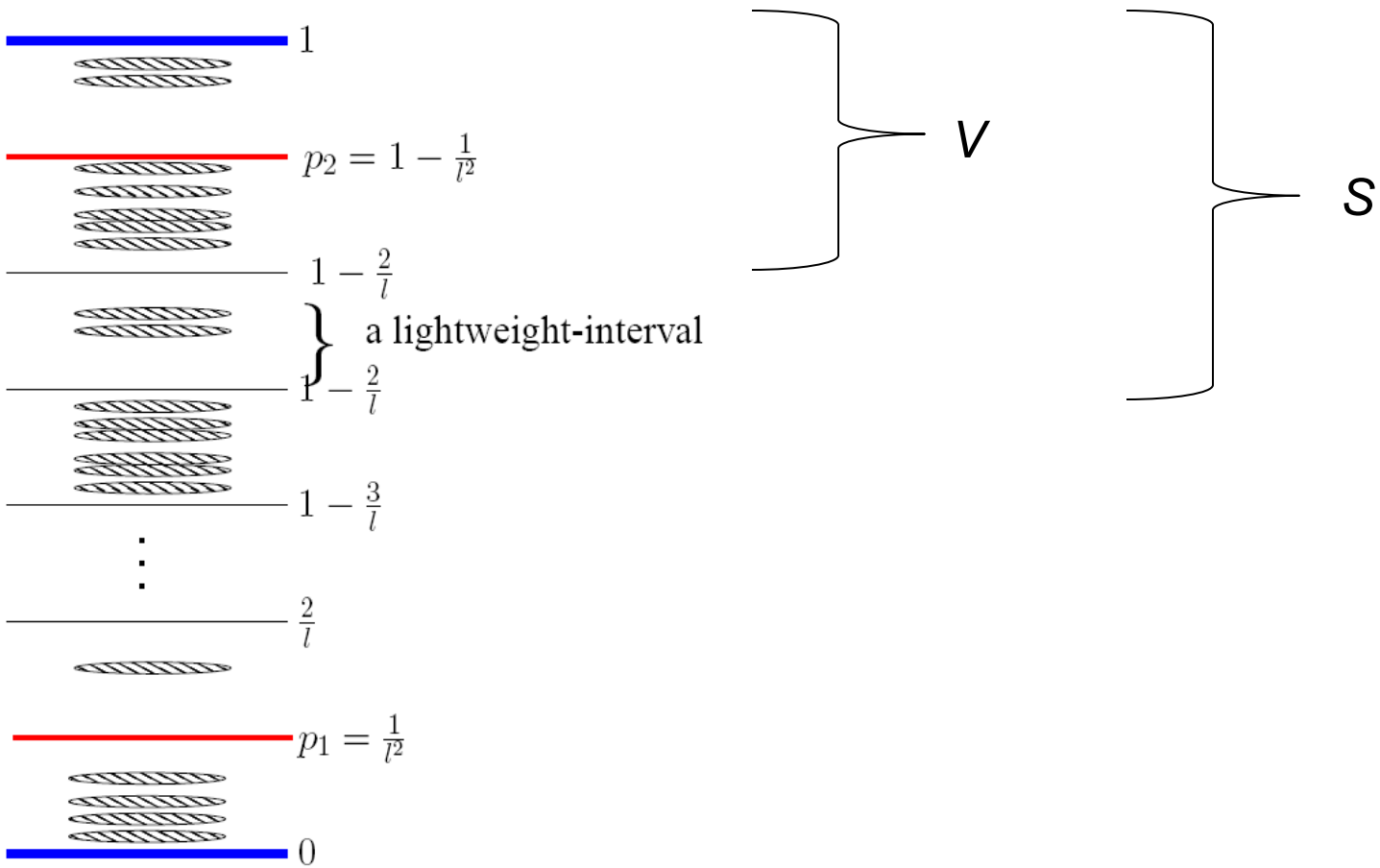
Solution: divide the $[p_1, p_2]$ interval into *poly(n)* intervals (m^2 would do):



There must be a "lightweight" interval in which the number of solutions is at most twice the number of solutions in all intervals on the top of it!

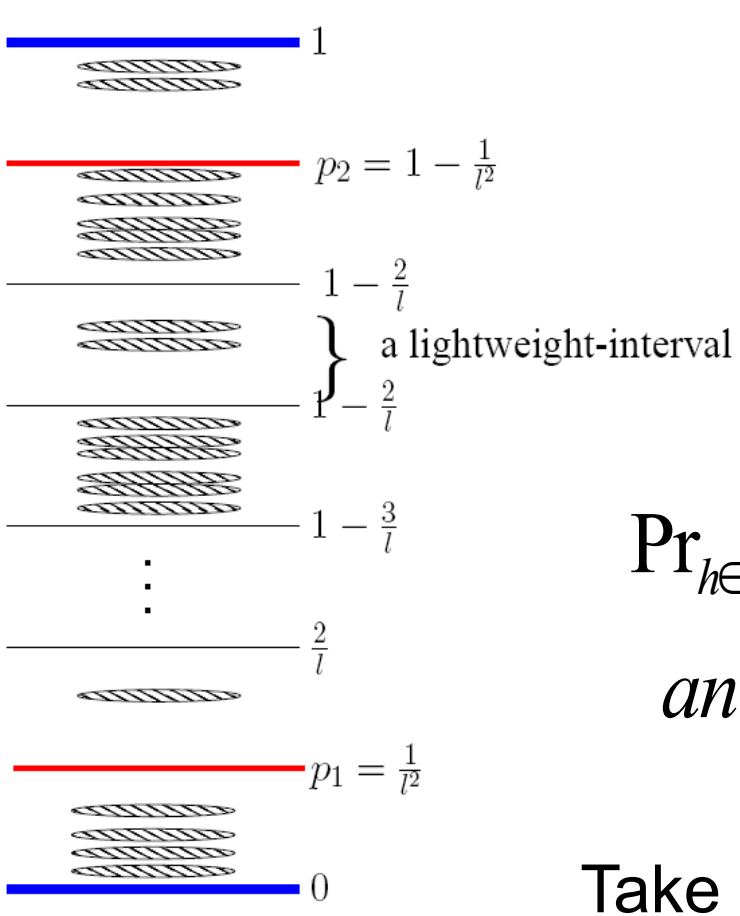
Valiant-Vazirani for MA

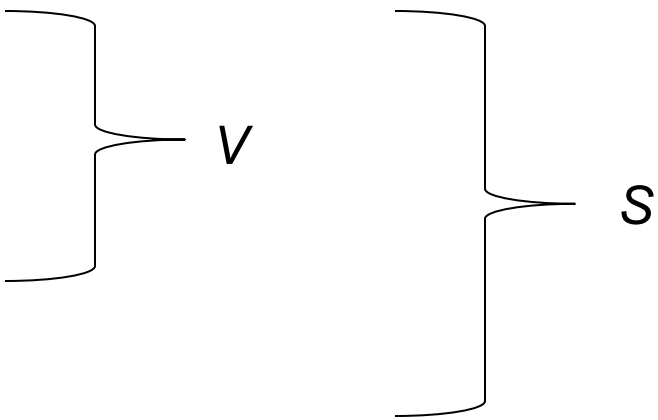
Solution: divide the $[p_1, p_2]$ interval into *poly(n)* intervals (m^2 would do)



Valiant-Vazirani for MA

Solution: divide the $[p_1, p_2]$ interval into *poly(n)* intervals (m^2 would do)





$$\Pr_{h \in H}(|S \cap h^{-1}(0^k)| = 1$$

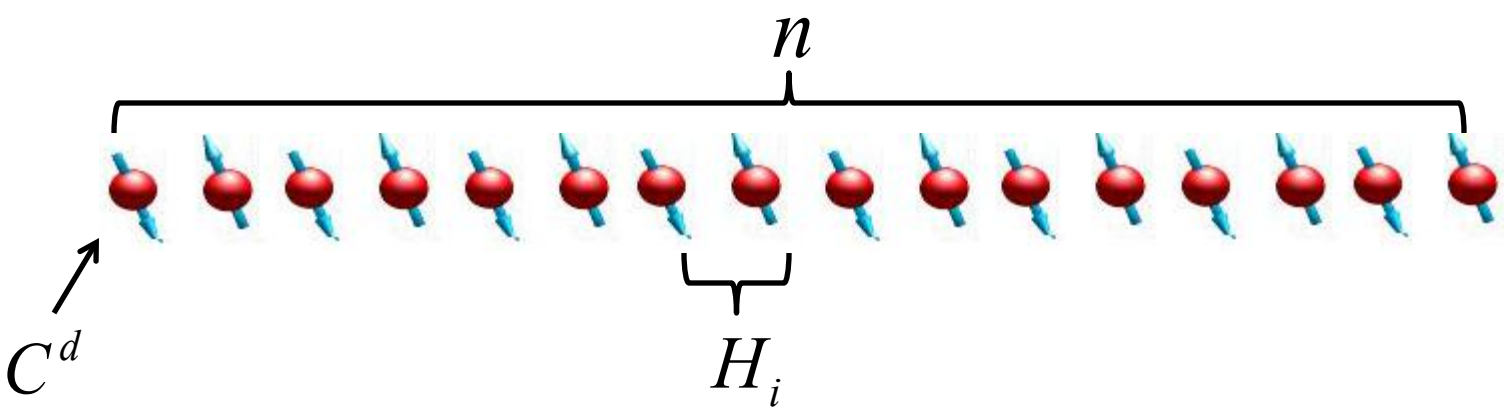
$$and\ \ S \cap h^{-1}(0^k) \in V) \geq 2^{-(k+1)}\,|V|$$

Take *k* such that $2^{k-2} \leq |S| \leq 2^{k-1}$

Valiant-Vazirani for QCMA

THE SAME

Application to Hamiltonian Complexity



- The Local Hamiltonian problem for poly-gapped 1D Hamiltonians is QCMA-hard

Application to Hamiltonian Complexity

- Why do we care about QCMA, couldn't we get a similar result just by using NP?

- Yes, but...

Application to Hamiltonian Complexity

- Why do we care about QCMA, couldn't we get a similar result just by using NP?

- Yes, but...

- Quantum hardness results tells us not only about the hardness of computing the answer, but also about the *difficulty* of providing a *classical proof* to it!

- Example: QMA-hardness (and not *merely* NP-hardness) is needed for ruling out an efficient description of a universal function in DFT (Schuch and Verstraete 07)

Cor: No class of states satisfying properties 1 and 2 can approximate the groundstate of every 1D poly-gapped Hamiltonians
(assuming NP different from QCMA)

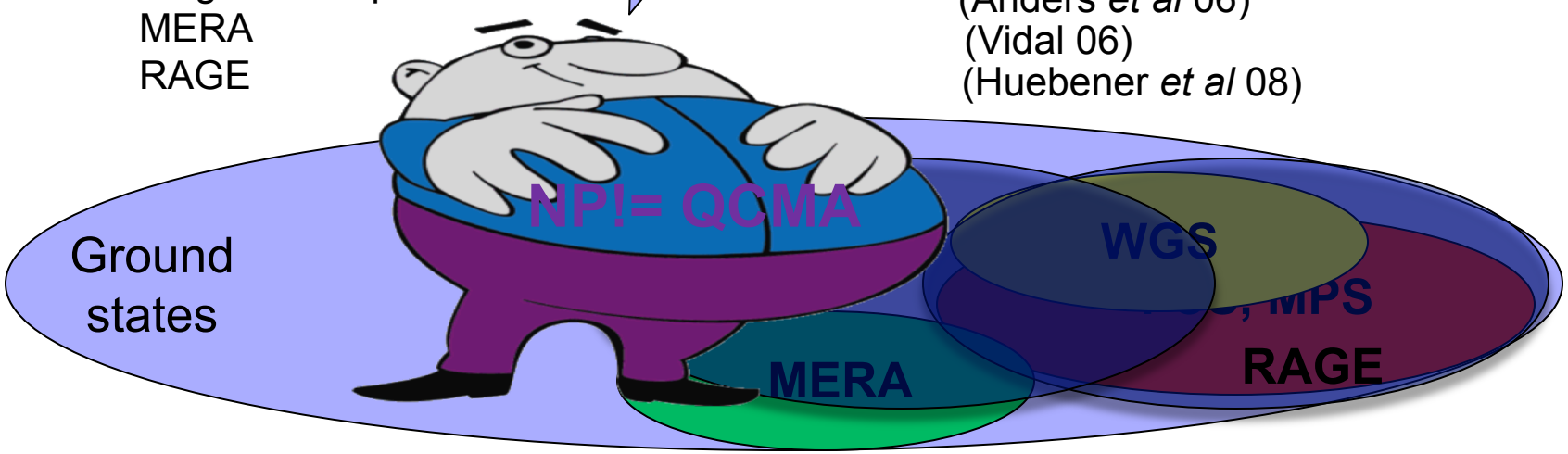
- Is there a cla
ground state c

- Consider any set of states
  1) each state is describe) parameters
  2) expectation values of l ervables can be efficiently computed (in a classica puter)

e.g. FCS, Matrix-Product-States,

(Fannes, Werner, Nachtergaele 89, Verstraete, Cirac 05)
(Anders *et al* 06)
(Vidal 06)
(Huebener *et al* 08)

Weighted Graph States
MERA
RAGE



Valiant-Vazirani for QMA??

Seems harder.... Consider the following analogous task:

- Given a set of quantum states $\{|\psi_i\rangle\}_{i=1}^{N}$, can we find a family of quantum circuits such that, w.h.p. over the choice of the circuit, it accepts a $|\psi_i\rangle$ with higher probability than the others?

Valiant-Vazirani for QMA??

- Much simpler problem: Given two *known* quantum states $\{|\psi_1\rangle, |\psi_2\rangle\}$ of *n* qubits, is there a quantum circuit of *poly(n)* gates that can distinguish them with non-negligible probability?

Valiant-Vazirani for QMA??

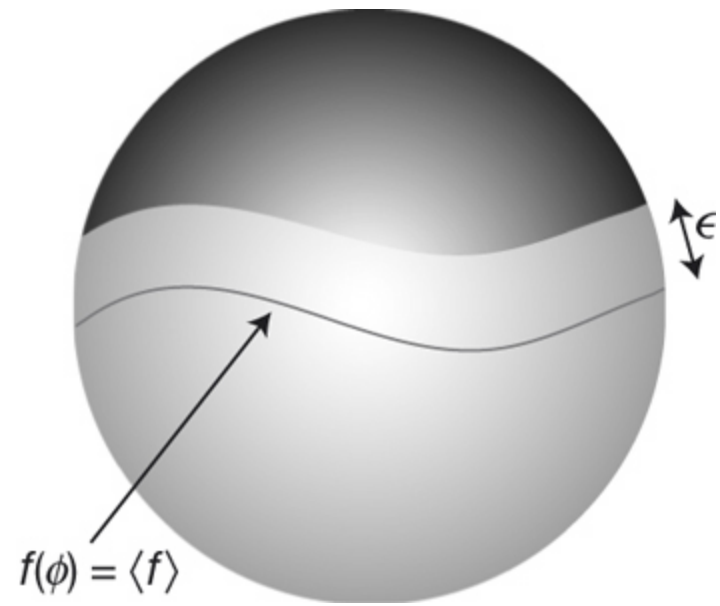
- Much simpler problem: Given two *known* quantum states $\{|\psi_1\rangle, |\psi_2\rangle\}$ of *n* qubits, is there a quantum circuit of *poly(n)* gates that can distinguish them with non-negligible probability?

NO, for the overwhelming majority of states!

Valiant-Vazirani for QMA??

Key idea: Levy's Lemma

For $f : S^d \rightarrow \Re$ with Lipschitz constant η and a point $x \in S^n$ chosen uniformly at random



$$\Pr\left(|f(x) - \mathrm{E}(f)| \geq \alpha\right) \leq \exp\left(-cd\alpha^2/\eta^2\right)$$

Valiant-Vazirani for QMA??

By Levy's Lemma, for every POVM element $0<A<I$ acting on n qubits,

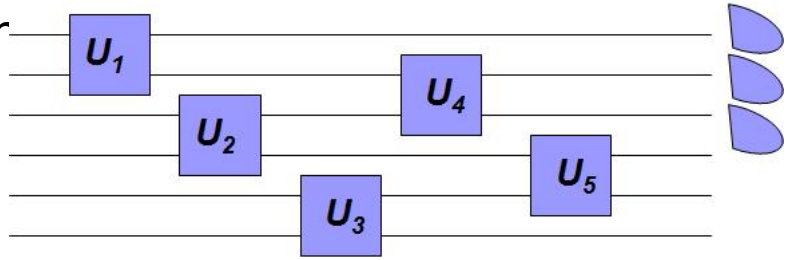
$$\Pr_{|\psi\rangle \sim Haar}\left(\left|\langle\psi|A|\psi\rangle - 2^{-n} tr(A)\right| \geq \varepsilon\right) \leq e^{-c\varepsilon^2 2^n}$$

Valiant-Vazirani for QMA??

By Levy's Lemma, for every POVM element $0<A<I$ acting on n qubits,

$$\Pr_{|\psi\rangle\sim Haar}\left(\left|\langle\psi|A|\psi\rangle - 2^{-n}tr(A)\right| \geq \varepsilon\right) \leq e^{-c\varepsilon^2 2^n}$$

There are less than $2^{n^{\log(n)}}$ different POVMs that can be implemented by a poly(n) quantum circuit com universal set.

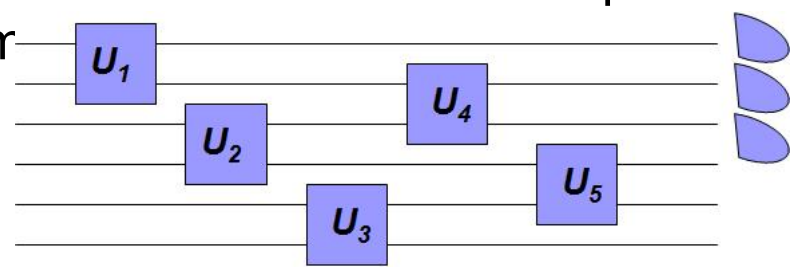


Valiant-Vazirani for QMA??

By Levy's Lemma, for every POVM element 0<*A*<*I* acting on *n* qubits,

$$\Pr_{|\psi\rangle \sim Haar}\left(\left|\langle\psi|A|\psi\rangle - 2^{-n} tr(A)\right| \geq \varepsilon\right) \leq e^{-c\varepsilon^2 2^n}$$

There are less than $2^{n^{\log(n)}}$ different POVMs that can be implemented by a poly(n) quantum circuit com
universal set.



Hence, by the union bound

$$\Pr_{|\psi\rangle \sim Haar}\left(\max_{A \in QC(poly(n))} \left|\langle\psi|A|\psi\rangle - 2^{-n} tr(A)\right| \geq \varepsilon\right) \leq 2^{n^{\log(n)}} e^{-c\varepsilon^2 2^n}$$

Where QC(poly(n)) is the set of all POVMs implementable by a

Valiant-Vazirani for QMA??

- Nice counterpart to the fact that most quantum states need an exponential number of gates to be created: the majority of states also cannot be distinguished from the maximally mixed state by polynomial quantum computation!

- Same ideas were applied recently to the impossibility of measurement based quantum computing with generic states (Gross, Flamia, Eisert 08, Bremner, Mora, Winter 08)

Valiant-Vazirani for QMA??

- But ground states of local Hamiltonians are far from generic, so this obstruction doesn't apply

- The argument before nonetheless shows that we have to use something about the *structure* of ground states (or analogously of quantum proofs) to have a chance to follow VV strategy in the quantum case.

Fighting entanglement with entanglement

- Recently, Jain, Kuperberg, Kerenidis, Santha, Sattath, Zhang managed to overcome the previous difficulty by using a *quantum trick*:

Fighting entanglement with entanglement

- Recently, Jain, Kuperberg, Kerenidis, Santha, Sattath, Zhang managed to overcome the previous difficulty by using a *quantum trick*:

- Suppose there are only two witnesses $\{|\psi_1\rangle, |\psi_2\rangle\}$ with acceptance probability bigger than 2/3 (all other having acceptance prob. < 1/3)

Fighting entanglement with entanglement

- Recently, Jain, Kuperberg, Kerenidis, Santha, Sattath, Zhang managed to overcome the previous difficulty by using a *quantum trick*:

- Suppose there are only two witnesses $\{|\psi_1\rangle, |\psi_2\rangle\}$ with acceptance probability bigger than 2/3 (all other having acceptance prob. < 1/3)

- Then we can reduce the problem to a unique witness:

The verifier simply asks for a new proof consisting of two registers, which should be antisymmetric and each register should be accepted by the original verification circuit.

$$|\psi\rangle = (|\psi_1\rangle \otimes |\psi_2\rangle - |\psi_2\rangle \otimes |\psi_1\rangle) / \sqrt{2}$$

Fighting entanglement with entanglement

- Same argument applies if we have a polynomial number of witnesses
- It doesn't work for the general case....
- In fact, the reduction is deterministic, so it's unlikely that something similar would work
- Can we rule out such possibility? It boils down to proving a *quantum oracle separation* of UQMA and QMA

QMA versus QCMA

- We would be done if QCMA = QMA

QMA versus QCMA

- We would be done if QCMA = QMA

- Could they be the same? There is an oracle separation (Aaronson, Kuperberg 06), but nothing much else is known...

QMA versus QCMA

- We would be done if QCMA = QMA

- Could they be the same? There is an quantum oracle separation (Aaronson, Kuperberg 06), but nothing much else is known...

- The problem put in terms of Hamiltonian complexity:

Do ground states of 1D local Hamiltonians require in the worst case exponential sized quantum circuits to be created?

UQMA versus QCMA

- We have shown QCMA is contained in UQMA. Could they be the same?

UQMA versus QCMA

- We have shown QCMA is contained in UQMA. Could they be the same?

- Using the contruction of (Aaronson and Kuperberg 06) we can find an quantum oracle for which they are not....

UQMA versus QCMA

- We have shown QCMA is contained in UQMA. Could they be the same?

- Using the contruction of (Aaronson and Kuperberg 06) we can find an quantum oracle for which they are not....

- In Hamiltonian complexity terms:

- Can we find for every poly-gapped local Hamiltonian *H* another local Hamiltonian *H'* whose ground state is *simple* and such that for every 0 < s < 1

$$\Delta(sH'+(1-s)H) = \Omega(1/poly(n)) \qquad ??$$

Open problems

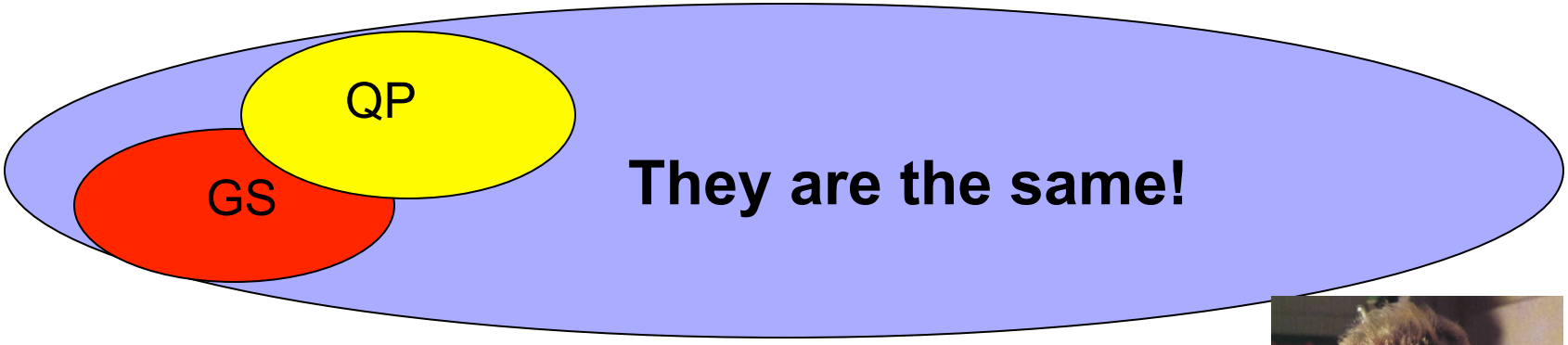
- Can we find a quantum oracle separation for UQMA and QMA? We have a guess from (Aaronson, Kuperberg 06)
- Are there any other quantum tricks that might help?
- Can we find similar results for *gapped* models in higher dimensions?
- Can we go beyond Feynman/Kitaev construction?
- Can we find more evidence in favor/against QMA versus QCMA and UQMA versus QCMA?

Thanks!

Quantum proofs versus groundstates

- *Ground states* of local Hamiltonians occupy a tiny fraction of the Hilbert space

- The same is true for *quantum proofs* in QMA



- That's why he should care about quantum proofs: