Quantum Information Theory as a Proof Technique

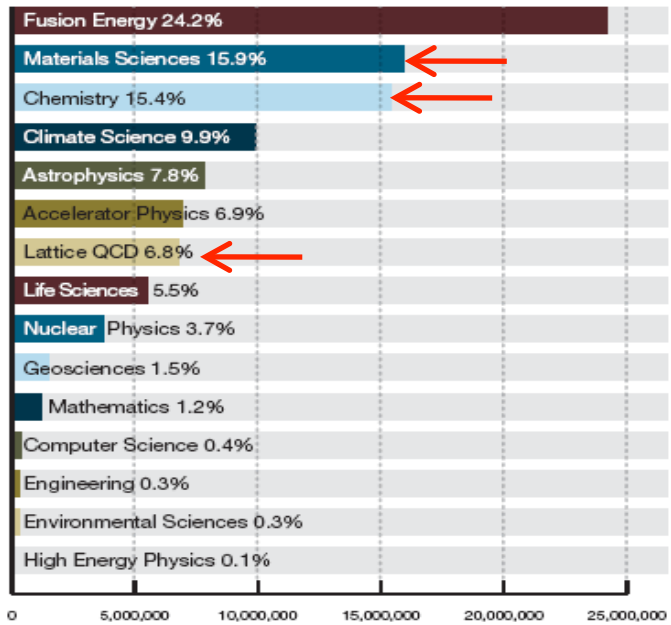
Fernando G.S.L. Brandão

ETH Zürich

With B. Barak (MSR), M. Christandl (ETH), A. Harrow (MIT), J. Kelner (MIT), D. Steurer (Cornell), J. Yard (Station Q), Y. Zhou (CMU)

Caltech, February 2013

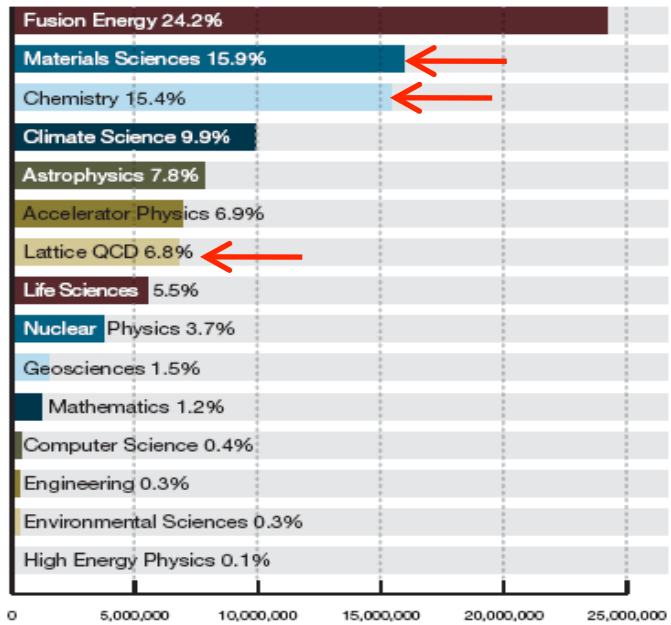
Simulating quantum is hard



More than **25%** of **DoE supercomputer power** is devoted to simulating quantum physics

Can we get a better handle on this ***simulation*** problem?

Simulating quantum is hard, secrets are hard to conceal



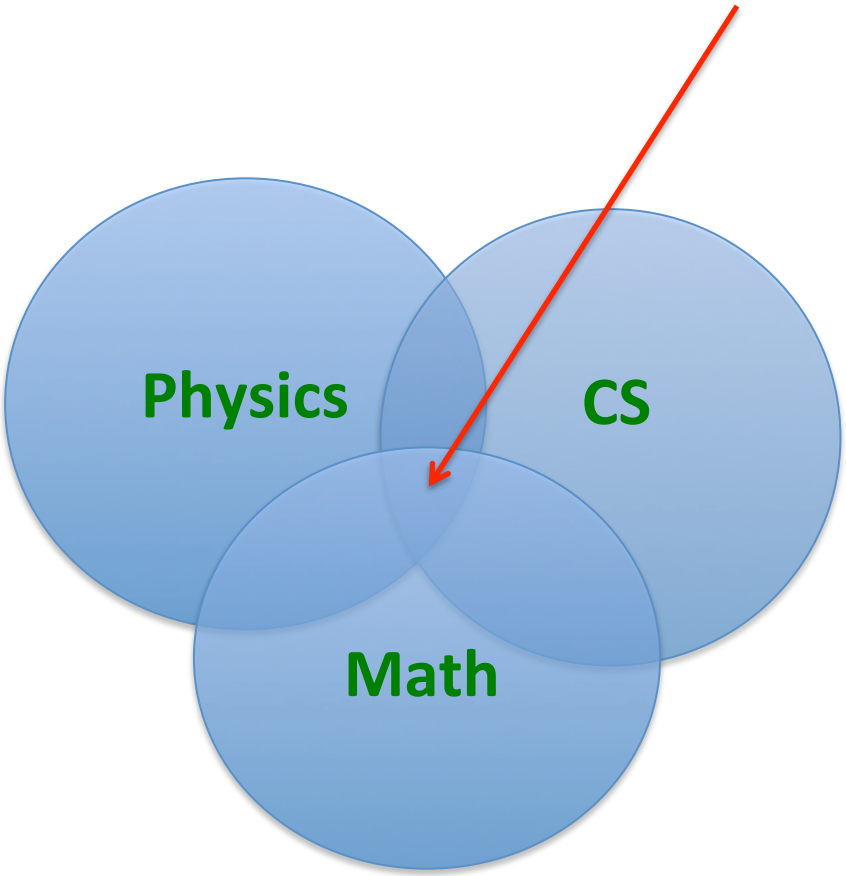
More than **25%** of **DoE supercomputer power** is devoted to simulating quantum physics

Can we get a better handle on this ***simulation*** problem?

All current **cryptography** is based on **unproven hardness assumptions**

Can we have ***better security guarantees*** for our secrets?

Quantum Information Science…



… gives a path for solving both problems. But it's a long journey

QIS is at the **crossover** of **computer science, mathematics** and **physics**

The Two Holy Grails of QIS

Quantum Computation:

Use of well-controlled **quantum systems for** performing **computation**

Exponential speed-ups over classical computing

E.g. Factoring (RSA)
Simulating quantum systems

Quantum Cryptography:

Use of well-controlled **quantum systems for secret key distribution**

Unconditional security based solely on the correctness of quantum mechanics

The Two Holy Grails of QIS

Quantum Computation:

Use of well-controlled quantum systems for performing computations.

State-of-the-art:
5 qubits computer

Can prove with *high probability* that **15 = 3 x 5**

Exponential speed-ups over classical computing

Quantum Cryptography:

Use of well-controlled **quantum systems for secret key distribution**

Unconditional security based solely on the correctness of quantum mechanics

The Two Holy Grails of QIS

Quantum Computation:

State-of-the-art:
5 qubits computer

Can prove with *high probability* that **15 = 3 x 5**

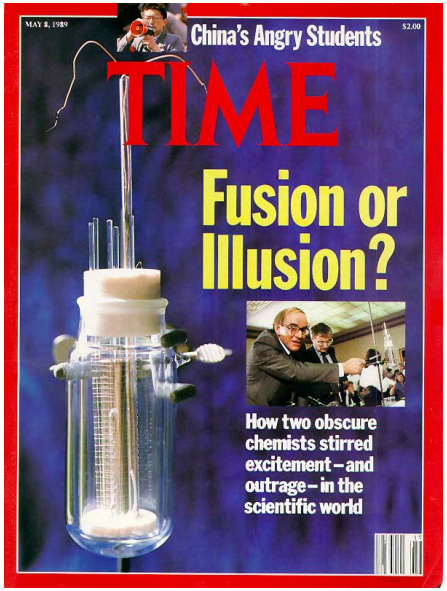
Quantum Cryptography:

State-of-the-art:
100 km

Still many technological challenges

What If…

…one can never build a quantum computer?

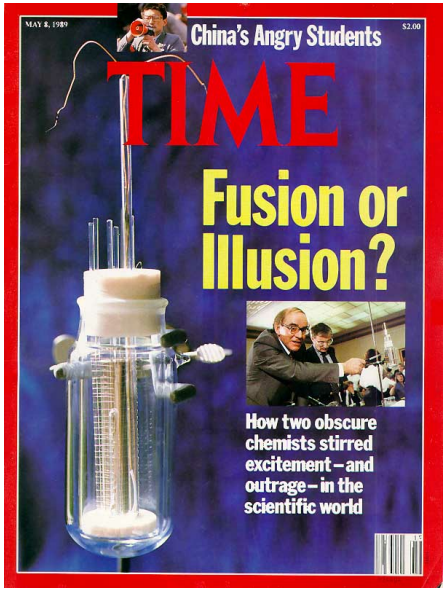


Answer 1: Then we **ought to know** why: **new physical principle** that makes **quantum computers impossible?**

Answer 2: QIS is interesting and **useful independent** of building a **quantum computer**

What If…

…one can never build a quantum computer?



Answer 1: Then we **ought to know** why: **new physical principle** that makes **quantum computers impossible?**

Answer 2: QIS is interesting and **useful independent** of building a **quantum computer**

This talk

Outline

- **Sum-Of-Squares Hierarchy and Entanglement**
- **Mean-Field and the Quantum PCP Conjecture**
- **Conclusions**

Outline

- **Sum-Of-Squares Hierarchy and Entanglement**
- **Mean-Field and the Quantum PCP Conjecture**
- **Conclusions**

Quadratic vs Biquadratic Optimization

Problem 1: For M in $H(C^d)$ (d x d matrix) compute

$$\max_{\|x\|=1} x^T M x = \max_{\|x\|=1} \sum_{i,j} M_{ij} x_i x_j^*$$

Very Easy!

Quadratic vs Biquadratic Optimization

Problem 1: For M in $H(C^d)$ (d x d matrix) compute

$$\max_{\|x\|=1} x^T M x = \max_{\|x\|=1} \sum_{i,j} M_{ij} x_i x_j^*$$

Very Easy!

Problem 2: For M in $H(C^d \otimes C^l)$, compute

$$\max_{\|x\|=\|y\|=1} (x \otimes y)^T M (x \otimes y) = \max_{\|x\|=\|y\|=1} \sum_{ijkl} M_{ij;kl} x_i x_j^* y_k y_l^*$$

Next:

Best known algorithm (and best hardness result) using ideas from Quantum Information Theory

Quantum Mechanics

Pure State: norm-one vector in C^d: $|\psi\rangle := (\psi_1, \ldots, \psi_d)^T$

Mixed State: positive semidefinite matrix of unit trace:

$$\rho \geq 0, tr(\rho) = 1 \qquad \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Dirac notation reminder: $\langle\psi| := (\psi_1^*, \ldots, \psi_d^*)$

Quantum Measurement: To any experiment with **d** outcomes we associate **d** PSD matrices $\{M_k\}$ such that $\Sigma_k M_k = I$

Born's rule: $\Pr(k) = tr(M_k \rho)$

Quantum Entanglement

Pure States: $|\psi\rangle_{AB} \in C^d \otimes C^l$

If $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B$, it's separable

otherwise, it's *entangled*.

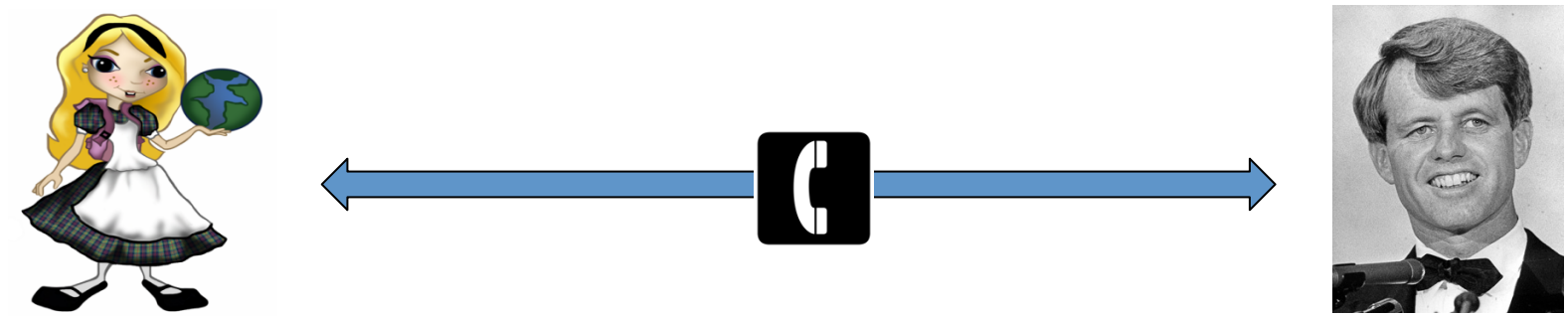
Mixed States: $\rho_{AB} \in D(C^d \otimes C^l)$

If $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$, it's separable

otherwise, it's *entangled*.

A Physical Definition of Entanglement

LOCC: Local quantum Operations and Classical Communication



Separable states can be created by LOCC:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$$

Entangled states cannot be created by LOCC:

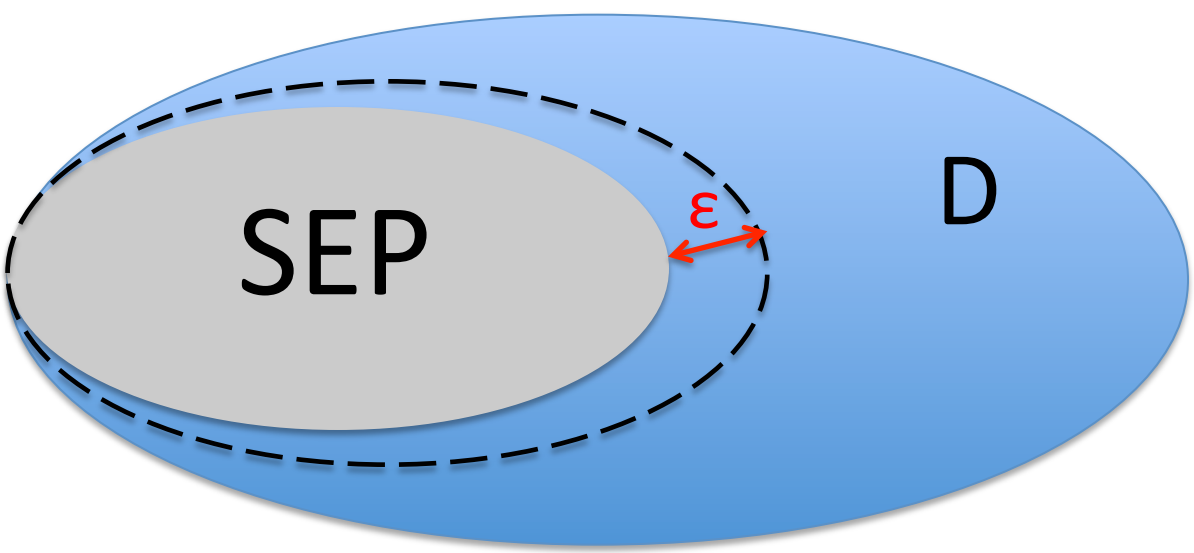
non-classical correlations

The Separability Problem

- Given $\rho_{AB} \in D(C^d \otimes C^l)$

  is it entangled?

- (Weak Membership: $W_{SEP}(\varepsilon, ||*||)$) Given ρ_{AB} determine if it is separable, or ε-away from SEP



The Separability Problem

- Given $\rho_{AB} \in D(C^d \otimes C^l)$

  is it entangled?

- (Weak Membership: $W_{SEP}(\varepsilon, ||*||)$) Given ρ_{AB} determine if it is separable, or ε-away from SEP

- Dual Problem: Optimization over separable states

$$h_{SEP}(M) := \max_{\sigma \in SEP} tr(M\sigma) = \max_{\|x\|=\|y\|=1} (x \otimes y)^T M (x \otimes y)$$

The Separability Problem

- Given $\rho_{AB} \in D(C^d \otimes C^l)$

  is it entangled?

- (Weak Membership: $W_{SEP}(\varepsilon, ||*||)$) Given ρ_{AB} determine if it is separable, or ε-away from SEP

- Dual Problem: Optimization over separable states

$$h_{SEP}(M) := \max_{\sigma \in SEP} tr(M\sigma) = \max_{\|x\|=\|y\|=1} (x \otimes y)^T M (x \otimes y)$$

- Relevance: Entanglement is a resource in quantum cryptography, quantum communication, etc…

Norms on Quantum States EDIT

How to quantify the distance in Weak-Membership?

1. Euclidean Norm (Hilbert-Schmidt): $||X||_2 = tr(X^T X)^{1/2}$

Norms on Quantum States EDIT

How to quantify the distance in Weak-Membership?

1. Euclidean Norm (Hilbert-Schmidt): $||X||_2 = tr(X^T X)^{1/2}$

---

2. Trace Norm: $||X||_1 = tr((X^T X)^{1/2})$

$$||\rho - \sigma||_1 = 2 \max_{0<M<I} tr(M(\rho - \sigma))$$

Norms on Quantum States EDIT

How to quantify the distance in Weak-Membership?

1. Euclidean Norm (Hilbert-Schmidt): $||X||_2 = tr(X^T X)^{1/2}$

2. Trace Norm: $||X||_1 = tr((X^T X)^{1/2})$

$$||\rho - \sigma||_1 = 2 \max_{0<M<I} tr(M(\rho - \sigma))$$

3. 1-LOCC Norm:

$$||\rho_{AB} - \sigma_{AB}||_{1\text{-LOCC}} = 2 \max_{0<M<I} tr(M(\rho - \sigma)) : M \text{ in 1-LOCC}$$

M in 1-LOCC $\Leftrightarrow M = \sum_k A_k \otimes B_k,\ \sum_k A_k \leq I,\ 0 \leq B_k \leq I$

Previous Work

When is ρ_{AB} entangled?

- Decide if ρ_{AB} is separable or ε-away from separable

Beautiful theory behind it (PPT, entanglement witnesses, etc)

Horribly expensive algorithms

State-of-the-art: $2^{O(|A|\log|B|)}$ time complexity for either $||*||_2$ or $||*||_1$

Same for estimating h_{SEP} (no better than exaustive search!)

Hardness Results

When is ρ_{AB} entangled?

- Decide if ρ_{AB} is separable or ε-away from separable

(Gurvits '02, Gharibian '08)

NP-hard with $\varepsilon=1/\mathrm{poly}(|A||B|)$ for $||*||_1$ or $||*||_2$

(Harrow, Montanaro '10)

No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ time algorithm with $\varepsilon=\Omega(1)$ and any $\nu+\mu>0$ for $||*||_1$, unless ETH fails

ETH (Exponential Time Hypothesis): SAT cannot be solved in $2^{o(n)}$ time

(Impagliazzo&Paruti '99)

Quasipolynomial-time Algorithm

(B., Christandl, Yard '11) There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for $W_{SEP}(||*||, \varepsilon)$ (in $||*||_2$ or $||*||_{1\text{-LOCC}}$)

2 norm natural from geometrical point of view

1-LOCC norm natural from operational point of view (distant lab paradigm)

Quasipolynomial-time Algorithm

(B., Christandl, Yard '11) There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for $W_{SEP}(||*||, \varepsilon)$ (in $||*||_2$ or $||*||_{1\text{-LOCC}}$)

Corollary 1: Solving $W_{SEP}(||*||_2, \varepsilon)$ is not NP-hard for $\varepsilon = 1/\text{polylog}(|A||B|)$, unless ETH fails

Contrast with:

(Gurvits '02, Gharibian '08) Solving $W_{SEP}(||*||_2, \varepsilon)$ NP-hard for $\varepsilon = 1/\text{poly}(|A||B|)$

Quasipolynomial-time Algorithm

(B., Christandl, Yard '11) There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for $W_{SEP}(||*||, \varepsilon)$ (in $||*||_2$ or $||*||_{1\text{-LOCC}}$)

Corollary 2: For M in 1-LOCC, can compute $h_{SEP}(M)$ within additive error ε in time $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$

Contrast with:

(Harrow, Montanaro '10) No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ algorithm for $h_{SEP}(M)$ with $\varepsilon=\Omega(1)$, for *separable* M

$$M = \sum_k A_k \otimes B_k, \;\; A_k, B_k \geq 0, M \leq I$$

Algorithm: SoS Hierarchy

$$h_{SEP}(M) = \max_{\|x\|=\|y\|=1} \sum_{ijkl} M_{ij;kl} x_i x_j^* y_k y_l^*$$

Polynomial optimization over hypersphere

Algorithm: SoS Hierarchy

$$h_{SEP}(M) = \max_{\|x\|=\|y\|=1} \sum_{ijkl} M_{ij;kl} x_i x_j^* y_k y_l^*$$

Polynomial optimization over hypersphere

Sum-Of-Squares (Parrilo/Lasserre) hierarchy:
gives sequence of SDPs that approximate $h_{SEP}(M)$

- Round k SDP has size $\dim(M)^{O(k)}$
- Converge to $h_{SEP}(M)$ when $k \to \infty$

Algorithm: SoS Hierarchy

$$h_{SEP}(M) = \max_{\|x\|=\|y\|=1} \sum_{ijkl} M_{ij;kl} x_i x_j^* y_k y_l^*$$

Polynomial optimization over hypersphere

Sum-Of-Squares (Parrilo/Lasserre) hierarchy:
gives sequence of SDPs that approximate $h_{SEP}(M)$

- Round k SDP has size $\dim(M)^{O(k)}$
- Converge to $h_{SEP}(M)$ when $k \to \infty$

SoS is the strongest SDP hierarchy known for polynomial optimization (connections with SoS proof system, real algebraic geometric, Hilbert's 17th problem, …)

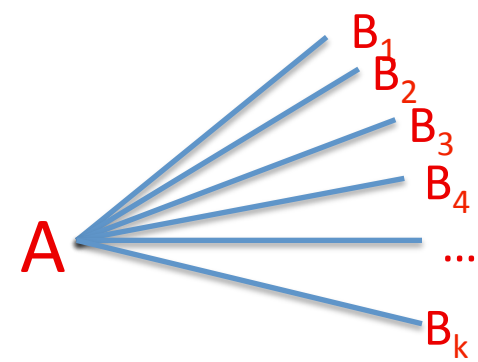
We'll derive SoS hierarchy by a quantum argument

Classical Correlations are Shareable

Given separable state $\sigma_{AB} = \sum_j p_j |\psi_j\rangle\langle\psi_j| \otimes |\varphi_j\rangle\langle\varphi_j|$

Consider the *symmetric extension*

$$\sigma_{AB_1,\ldots,B_k} = \sum_j p_j |\psi_j\rangle\langle\psi_j| \otimes |\varphi_j\rangle\langle\varphi_j|^{\otimes k}$$

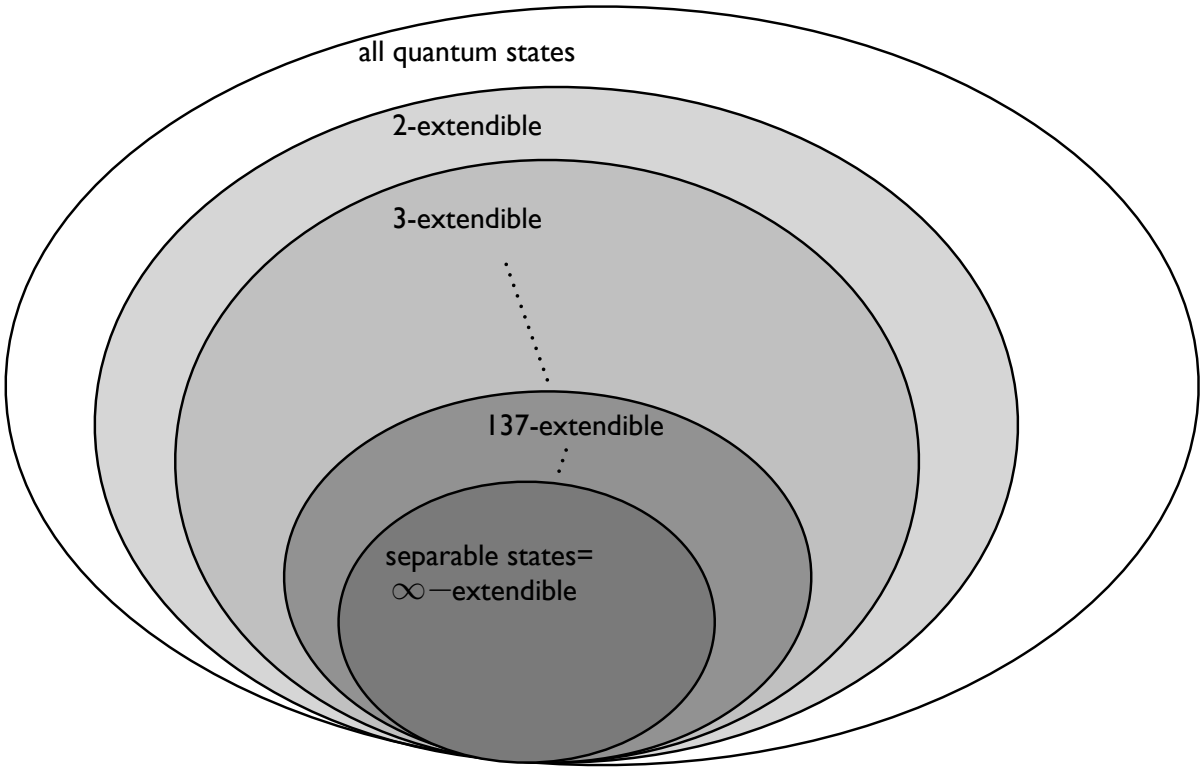


Def. ρ_{AB} is k-extendible if there is $\rho_{AB1\ldots Bk}$ s.t for all j in [k], $\mathrm{tr}_{\setminus Bj}(\rho_{AB1\ldots Bk}) = \rho_{AB}$

Entanglement is Monogamous

(Stormer '69, Hudson & Moody '76, Raggio & Werner '89)

ρ_{AB} separable iff ρ_{AB} is k-extendible for all k



$\Longrightarrow$ search for a 2-extension, 3-extension.....

How close to separable is ρ_{AB} if a k-extension is found?

How long does it take to check if a k-extension exists?

SoS as optimization over *k*-extensions

(Doherty, Parrilo, Spedalieri '01) k-level SoS SDP for $h_{SEP}(M)$ is *equivalent* to optimization over k-extendible states (plus PPT (positive partial transpose) test):

$$\max tr(M\pi): \ \exists\, \sigma_{AB_1\ldots B_k} \geq 0,\ tr(\sigma)=1,\ \sigma_{AB_j}=\pi\ \forall j$$

SoS as optimization over *k*-extensions

(Doherty, Parrilo, Spedalieri '01) k-level SoS SDP for $h_{SEP}(M)$ is *equivalent* to optimization over k-extendible states (plus PPT (positive partial transpose) test):

$$\max tr(M\pi): \ \exists\, \sigma_{AB_1\ldots B_k} \geq 0,\ tr(\sigma)=1,\ \sigma_{AB_j}=\pi\ \forall j$$

(Stormer '69, Hudson & Moody '76, Raggio & Werner '89)
give alternative proof that hierarchy converges
(before the hierarchy was even defined :-)

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)
gives a proof of equivalence

How close to separable are *k*-extendible states?

(Christandl, Koenig, Mitschison, Renner '05) De Finetti Bound

If ρ_{AB} is k-extendible $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \leq \Omega\left(\frac{|B|^2}{k}\right)$

But there are *k*-extendible states ρ_{AB} s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$

How close to separable are *k*-extendible states?

(Christandl, Koenig, Mitschison, Renner '05) De Finetti Bound

If ρ_{AB} is k-extendible $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \leq \Omega\left(\frac{|B|^2}{k}\right)$

But there are *k*-extendible states ρ_{AB} s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$

Improved de Finetti Bound (B, Christandl, Yard '11)

If ρ_{AB} is k-extendible:

for 1-LOCC or 2 norm $\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\| \leq \left(\frac{4 \ln 2 \log |A|}{k}\right)^{1/2}$

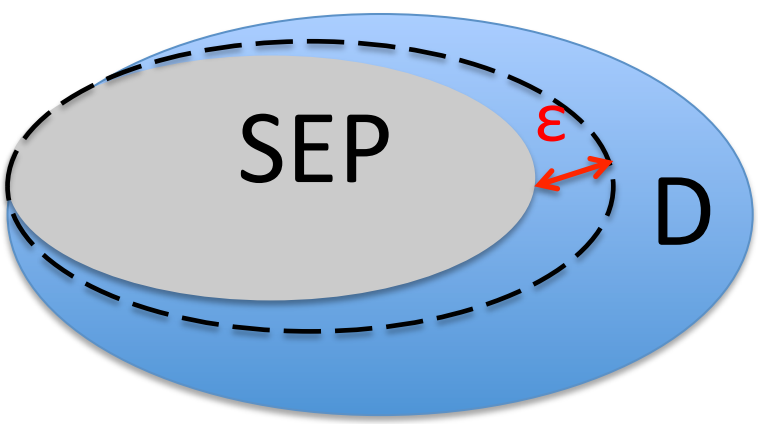
How close to separable are *k*-extendible states?

Improved de Finetti Bound (B, Christandl, Yard '11)

If ρ_{AB} is k-extendible:

for 1-LOCC or 2 norm

$$\min_{\sigma \in SEP} \left\| \rho_{AB} - \sigma_{AB} \right\| \leq \left(\frac{4 \ln 2 \log |A|}{k} \right)^{1/2}$$



$k=2\ln(2)\varepsilon^{-2}\log|A|$ rounds of SoS solves $W_{SEP}(\varepsilon)$ with a SDP of size

$|A||B|^k = \exp(O(\varepsilon^{-2}\log|A| \log|B|))$

Proving…

Improved de Finetti Bound (B, Christandl, Yard '11)

If ρ_{AB} is k-extendible:
for 1-LOCC or 2 norm $\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\| \leq \left(\frac{4 \ln 2 \log |A|}{k} \right)^{1/2}$

Proof is information-theoretic

Mutual Information:

$I(A:B)_\rho := H(A) + H(B) - H(AB)$ $\qquad$ $H(A)_\rho := -\mathrm{tr}(\rho \log(\rho))$

Proving…

Improved de Finetti Bound (B, Christandl, Yard '11)

If ρ_{AB} is k-extendible:
for 1-LOCC or 2 norm $\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\| \leq \left(\frac{4 \ln 2 \log|A|}{k} \right)^{1/2}$

Proof is information-theoretic

Mutual Information:

$I(A:B)_\rho := H(A) + H(B) - H(AB)$ $\qquad$ $H(A)_\rho := -tr(\rho \log(\rho))$

Let $\rho_{AB1\ldots Bk}$ be k-extension of ρ_{AB}

$2\log|A| > I(A:B_1\ldots B_k) = I(A:B_1)+I(A:B_2|B_1)+\ldots+I(A:B_k|B_1\ldots B_{k-1})$

(chain rule)

For some $l<k$: $I(A:B_l|B_1\ldots B_{l-1}) < 2 \log|A|/k$

Proving…

Improved de Finetti Bound (B, Christandl, Yard '11)

If ρ_{AB} is k-extendible:
for 1-LOCC or 2 norm $\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\| \leq \left(\frac{4 \ln 2 \log|A|}{k} \right)^{1/2}$

Proof is information-theoretic

Mutual Information:

$I(A:B)_\rho := H(A) + H(B) - H(AB)$ $\qquad$ $H(A)_\rho := -tr(\rho \log(\rho))$

Let $\rho_{AB1\ldots Bk}$ be k-extension of ρ_{AB}

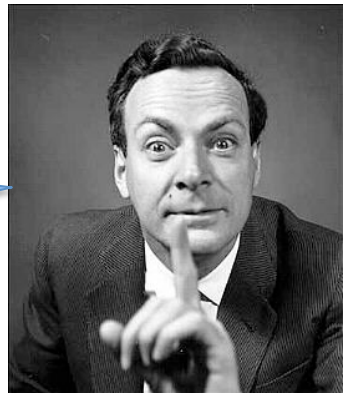
$2\log|A| > I(A:B_1\ldots B_k) = I(A:B_1)+I(A:B_2|B_1)+\ldots+I(A:B_k|B_1\ldots B_{k-1})$

(chain rule)

For some $l<k$: $\boxed{I(A:B_l|B_1\ldots B_{l-1}) < 2 \log|A|/k}$ **What does it imply?**

Quantum Information?

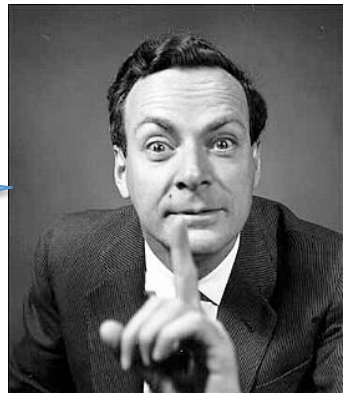
Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.



Quantum Information?

Nature isn't classical, dammit, and if you want to make ~~a simulation~~ of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

information theory



Good news

- $I(A:B|C)$ still defined
- Chain rule, etc. still hold
- $I(A:B|C)_\rho = 0$ implies ρ is separable (Hayden, Jozsa, Petz, Winter'03)

Bad news

- Only definition $I(A:B|C)=H(AC)+H(BC)-H(ABC)-H(C)$
- Can't condition on quantum information.
- $I(A:B|C)_\rho \approx 0$ doesn't imply ρ is approximately separable in 1-norm (Ibinson, Linden, Winter '08)

Proving the Bound

Thm (B, Christandl, Yard '11) For $||*||_{1\text{-LOCC}}$ or $||*||_2$

$$I(A:B|C) \geq \frac{1}{2\ln 2} \min_{\sigma \in SEP} \left\| \rho_{AB} - \sigma_{AB} \right\|^2$$

Chain rule:

$2\log|A| > I(A:B_1 \ldots B_k) = I(A:B_1) + I(A:B_2|B_1) + \ldots + I(A:B_k|B_1 \ldots B_{k-1})$

Then $$2\log|A| \geq \frac{k}{2\ln 2} \min_{\sigma \in SEP} \left\| \rho_{AB} - \sigma_{AB} \right\|^2$$

Conditional Mutual Information Bound

$$I(A:B\,|\,C) \geq \frac{1}{2\ln 2} \min_{\sigma \in SEP} \left\| \rho_{AB} - \sigma_{AB} \right\|^2$$

- Coding Theory
  Strong subadditivity of von Neumann entropy as state redistribution rate (Devetak, Yard '06)

- Large Deviation Theory
  Hypothesis testing for entanglement (B., Plenio '08)

$$\left(I(A:B\,|\,C)_\rho \geq E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \geq D_{1-LOCC}(\rho_{A:B}) \geq \frac{1}{2\ln 2} \min_{\sigma \in SEP} \left\| \rho_{A:B} - \sigma \right\|_{1-LOCC}^2 \right)$$

h_{SEP} equivalent to

1. Injective norm of 3-index tensors
2. Minimum output entropy quantum channel
3. Optimal acceptance probability in QMA(2)
4. 2->4 norm of projectors: $\|P\|_{2\to 4} := \max_{\|x\|_2=1} \|Px\|_4$

$$\|P\|_{2\to 4} = h_{SEP}(M),\ M = \sum_k \left(P|k\rangle\langle k|P\right) \otimes \left(P|k\rangle\langle k|P\right)$$

Unique Games Conjecture

(Unique Games Conjecture, Khot '02) For every $\varepsilon>0$ it's NP-hard to tell for a system of equations $x_i + x_j = c \bmod k$

YES) More than $1-\varepsilon$ fraction constraints satisfiable

NO) Less than ε fraction satisfiable

Unique Games Conjecture

(Unique Games Conjecture, Khot '02) For every $\varepsilon>0$ it's NP-hard to tell for a system of equations $x_i + x_j = c \bmod k$

YES) More than $1-\varepsilon$ fraction constraints satisfiable
NO) Less than ε fraction satisfiable

(Raghavedra '08) UGC implies 2-level SoS gives the best approximation algorithm for *all* Constraints Satisfaction Problems (max-cut, vertex cover, …)

Major barrier in current knowledge of algorithms for combinatorial problems

(Arora, Barak, Steurer '10) $\exp(n^{O(\varepsilon)})$ time algorithm for UG

Small Set Expansion Conjecture

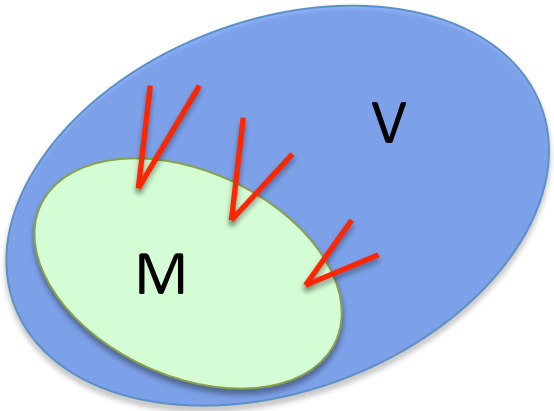
(Small Set Expansion Conjecture, Raghavendra, Steurer '10)

For every $\varepsilon, \delta > 0$ it's NP-hard to tell for a graph $G = (V, E)$ whether

YES) $\Phi(M) < \varepsilon$ for a region M of size $\approx \delta|V|$,

NO) $\Phi(M) > 1-\varepsilon$ for all regions M of size $\approx \delta|V|$,

Expansion: $\Phi(M) = \Pr_{(u,v)\in E}\left(v \notin M \mid u \in M\right)$



Small Set Expansion Conjecture

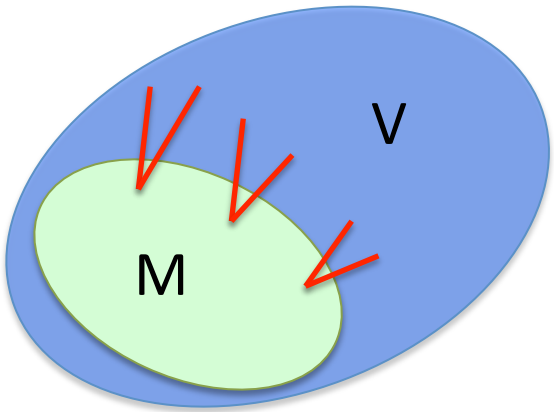
(Small Set Expansion Conjecture, Raghavendra, Steurer '10)

For every $\varepsilon, \delta > 0$ it's NP-hard to tell for a graph $G = (V, E)$ whether

YES) $\Phi(M) < \varepsilon$ for a region M of size $\approx \delta|V|$,

NO) $\Phi(M) > 1-\varepsilon$ for all regions M of size $\approx \delta|V|$,

Expansion: $\Phi(M) = \Pr_{(u,v)\in E}\left(v \notin M \mid u \in M\right)$



(Raghavendra, Steurer '10)

Small Set Expansion ≈ Unique Games

(Barak, B, Harrow, Kelner, Steurer, Zhou '12)

Rough estimate 2->4 norm of projector onto top eigenspace of graphs ≈ Small Set Expansion

Quantum Bound on SoS Implies

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)

1. For n *x* n matrix A can compute with $O(\log(n)\varepsilon^{-3})$ rounds of SoS a number x s.t.

$$\|A\|_{2\to 4}^{4} \le x \le \|A\|_{2\to 4}^{4} + \varepsilon \|A\|_{2\to 2}^{2} \|A\|_{2\to\infty}^{2}$$

Quantum Bound on SoS Implies

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)

1. For n *x* n matrix A can compute with $O(\log(n)\varepsilon^{-3})$ rounds of SoS a number x s.t.

$$\|A\|_{2\to 4}^{4} \le x \le \|A\|_{2\to 4}^{4} + \varepsilon \|A\|_{2\to 2}^{2} \|A\|_{2\to\infty}^{2}$$

2. $n^{O(\varepsilon)}$ -level SoS solves Small Set Expansion

Alternative algorithm to (Arora, Barak, Steurer '10)

Quantum Bound on SoS Implies

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)

1. For n *x* n matrix A can compute with $O(\log(n)\varepsilon^{-3})$ rounds of SoS a number x s.t.

$$\|A\|_{2\to 4}^{4} \le x \le \|A\|_{2\to 4}^{4} + \varepsilon \|A\|_{2\to 2}^{2} \|A\|_{2\to\infty}^{2}$$

2. $n^{O(\varepsilon)}$ -level SoS solves Small Set Expansion
Alternative algorithm to (Arora, Barak, Steurer '10)

3. Improvement in bound (additive -> multiplicative error) would solve SSE in $\exp(O(\log^2(n)))$ time

Quantum Bound on SoS Implies

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)

1. For n *x* n matrix A can compute with $O(\log(n)\varepsilon^{-3})$ rounds of SoS a number x s.t.

$$\|A\|_{2\to 4}^{4} \le x \le \|A\|_{2\to 4}^{4} + \varepsilon \|A\|_{2\to 2}^{2} \|A\|_{2\to\infty}^{2}$$

2. $n^{O(\varepsilon)}$ -level SoS solves Small Set Expansion
Alternative algorithm to (Arora, Barak, Steurer '10)

3. Improvement in bound (additive -> multiplicative error) would solve SSE in $\exp(O(\log^2(n)))$ time

4. Other quantum arguments show one cannot compute rough approximation of $||P||_{2\to 4}$ in less than $\exp(O(\log^2(n)))$ time (under ETH)

Quantum Bound on SoS Implies

(Barak, B., Harrow, Kelner, Steurer, Zhou '12)

1. For n *x* n matrix A can compute with $O(\log(n)\varepsilon^{-3})$ rounds of SoS a number x s.t.

$$\|A\|_{2\to 4}^{4} \le x \le \|A\|_{2\to 4}^{4} + \varepsilon \|A\|_{2\to 2}^{2} \|A\|_{2\to\infty}^{2}$$

2. $n^{O(\varepsilon)}$ -level SoS solves Small Set Expansion
Alternative algorithm to (Arora, Barak, Steurer '10)

3. Improvement in bound (additive -> multiplicative error) would solve SSE in $\exp(O(\log^2(n)))$ time

4. Other quantum arguments show one cannot compute rough approximation of $||P||_{2\to 4}$ in less than $\exp(O(\log^2(n)))$ time (under ETH)

5. Improvement (hardness for P from graphs) would imply $\exp(O(\log^2(n)))$ time lower bound on Unique Games (under ETH)

Quantum Bound on SoS Implies

(Barak, B., H

1. For n *x* n
SoS a numl

2. $n^{O(\varepsilon)}$ -lev
Alternative

Both improvements can be casted as open problems in quantum information theory

Maybe to solve UGC we should learn more about QIT?

3. Improvement in bound (additive -> multiplicative error) would solve SSE in $\exp(O(\log^2(n)))$ time

4. Other quantum arguments show one cannot compute rough approximation of $||P||_{2\to4}$ in less than $\exp(O(\log^2(n)))$ time (under ETH)

5. Improvement (hardness for P from graphs) would imply $\exp(O(\log^2(n)))$ time lower bound on Unique Games (under ETH)

Outline

- **Sum-Of-Squares Hierarchy and Entanglement**
- **<u>Mean-Field and the Quantum PCP Conjecture</u>**
- **Conclusions**

Quantum Mechanics, again

Dynamics in quantum mechanics is given by a

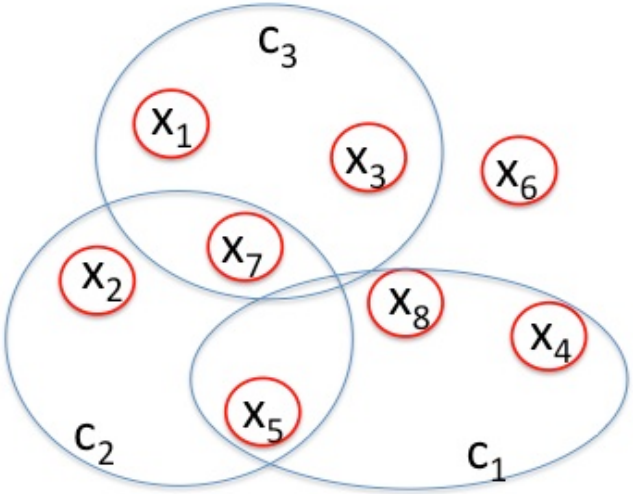
Hamiltonian H: $\left|\psi_t\right\rangle = \exp(itH)\left|\psi_0\right\rangle$

Equilibrium properties are also determined by H

Thermal state: $\propto \exp(-H/T)$

Groundstate: $H\left|\psi_0\right\rangle = E_0\left|\psi_0\right\rangle$

Constraint Satisfaction Problems vs Local Hamiltonians



k-arity CSP:

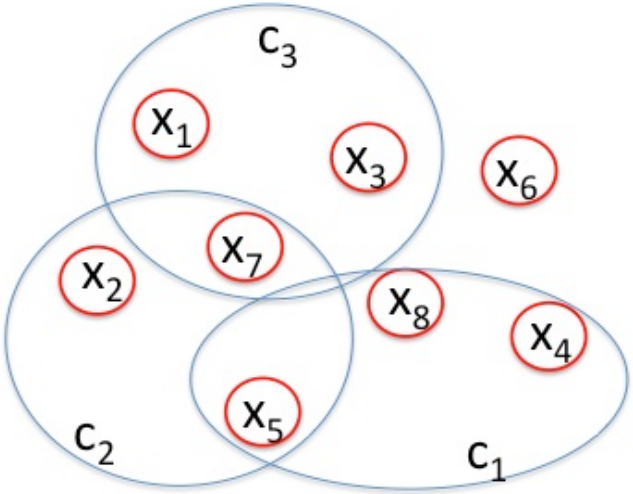
Variables $\{x_1, \ldots, x_n\}$, alphabet Σ

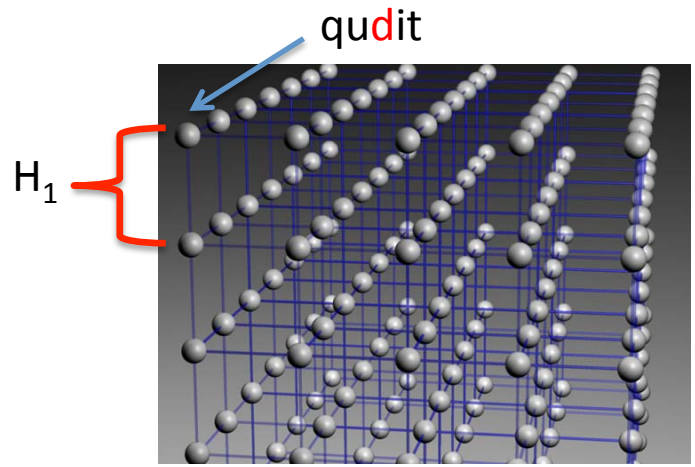
Constraints: $c_j : \Sigma^k \to \{0,1\}$

Assignment: $\sigma : [n] \to \Sigma$

Unsat $:= \min_{\sigma} \sum_j c_j(\sigma(x_{j_1}), \ldots, \sigma(x_{j_k}))$

Constraint Satisfaction Problems vs Local Hamiltonians





k-arity CSP:

Variables $\{x_1, \ldots, x_n\}$, alphabet Σ

Constraints: $c_j : \Sigma^k \to \{0,1\}$

Assignment: $\sigma : [n] \to \Sigma$

Unsat :=$\min_{\sigma} \sum_j c_j(\sigma(x_{j_1}),\ldots,\sigma(x_{j_k}))$

k-local Hamiltonian H:

n qudits in $\left(C^d\right)^{\otimes n}$

Constraints: $H_j \in Her\left(\left(C^d\right)^{\otimes k}\right)$

qUnsat := $E_0\left(\sum_j H_j\right)$

E_0 : min eigenvalue

C. vs Q. Optimal Assignments

Finding optimal assignment of CSPs can be hard

C. vs Q. Optimal Assignments

Finding optimal assignment of CSPs can be hard

Finding optimal assignment of quantum CSPs can be even harder

(BCS Hamiltonian groundstate, Laughlin states for FQHE,…)

Main difference: Optimal Assignment can be a highly entangled state (unit vector in $\left(C^d\right)^{\otimes n}$)

Mean-Field…

…consists in approximating groundstate by a product state $|\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$

$$\max_{\psi_1,\ldots,\psi_n} \langle \psi_1,\ldots,\psi_n | H | \psi_1,\ldots,\psi_n \rangle$$ is a CSP

Successful heuristic in Quantum Chemistry
Condensed matter

Folklore:
Mean-Field good when Many-particle interactions
Low entanglement in state

Mean-Field…

…co

by a

$$\max_{\psi_1,\ldots,\psi_n} \langle$$

Can we make folklore more rigorous?

Can we put limitations on use of mean-field and related schemes?

Successful heur

Quantum Chemistry
Condensed matter

Folklore:
Mean-Field good when

Many-particle interactions
Low entanglement in state

The Local Hamiltonian Problem and Quantum Complexity Theory

Problem

Given a local Hamiltonian H, decide if $E_0(H)=0$ or $E_0(H)>\Delta$

$E_0(H)$: minimum eigenvalue of H

The Local Hamiltonian Problem and Quantum Complexity Theory

Problem

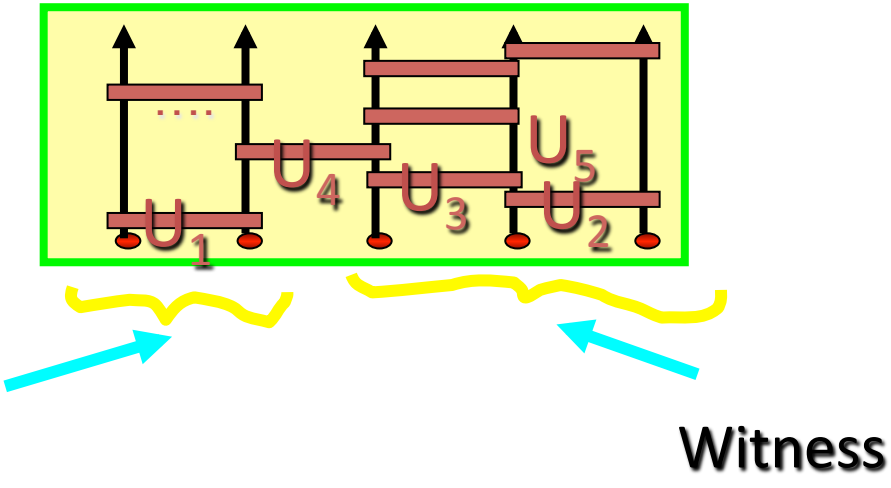
Given a local Hamiltonian H, decide if $E_0(H)=0$ or $E_0(H)>\Delta$

$E_0(H)$: minimum eigenvalue of H

Thm (Kitaev '99) The local Hamiltonian problem is QMA-complete for $\Delta = 1/\mathrm{poly}(n)$

(analogue Cook-Levin thm)

QMA is the quantum analogue of NP, where the proof and the computation are quantum



The meaning of it

It's believed QMA ≠ NP

Thus there is generally no efficient classical description of groundstates of local Hamiltonians

What's the role of the promise gap Δ on the hardness?

.... But first, what happens for CSP?

PCP Theorem

PCP Theorem (Arora et al '98, Dinur '07): There is a $\varepsilon > 0$ s.t. it's NP-complete to determine whether for a CSP with m constraints, Unsat = 0 or Unsat > εm

- NP-hard even for $\Delta = \Omega(m)$

PCP Theorem

PCP Theorem (Arora et al '98, Dinur '07): There is a $\varepsilon > 0$ s.t. it's NP-complete to determine whether for a CSP with m constraints, Unsat = 0 or Unsat > εm

- NP-hard even for $\Delta = \Omega(m)$
- Equivalent to the existence of **P**robabilistically **C**heckable **P**roofs for NP.

PCP Theorem

PCP Theorem (Arora et al '98, Dinur '07): There is a $\varepsilon > 0$ s.t. it's NP-complete to determine whether for a CSP with m constraints, Unsat = 0 or Unsat > εm

- NP-hard even for $\Delta=\Omega(m)$

- Equivalent to the existence of **P**robabilistically **C**heckable **P**roofs for NP.

- Central tool in the theory of hardness of approximation
  (optimal threshold for 3-SAT (7/8-factor), max-clique ($n^{1-\varepsilon}$-factor))
  (obs: Unique Game Conjecture is about the existence of strong form of PCP)

Quantum PCP?

The qPCP conjecture: There is $\varepsilon > 0$ s.t. the following problem is QMA-complete: Given 2-local Hamiltonian H with m local terms determine whether

(i) $E_0(H)=0$ or (ii) $E_0(H) > \varepsilon m$.

- (Bravyi, DiVincenzo, Loss, Terhal '08) Equivalent to conjecture for $O(1)$-local Hamiltonians over qdits.

Quantum PCP?

The qPCP conjecture: There is $\varepsilon > 0$ s.t. the following problem is QMA-complete: Given 2-local Hamiltonian H with m local terms determine whether

(i) $E_0(H)=0$ or (ii) $E_0(H) > \varepsilon m$.

- (Bravyi, DiVincenzo, Loss, Terhal '08) Equivalent to conjecture for $O(1)$-local Hamiltonians over qdits.
- Equivalent to estimating mean groundenergy to constant accuracy ($e_o(H) := E_0(H)/m$)

Quantum PCP?

The qPCP conjecture: There is $\varepsilon > 0$ s.t. the following problem is QMA-complete: Given 2-local Hamiltonian H with m local terms determine whether

(i) $E_0(H)=0$ or (ii) $E_0(H) > \varepsilon m$.

- (Bravyi, DiVincenzo, Loss, Terhal '08) Equivalent to conjecture for $O(1)$-local Hamiltonians over qdits.
- Equivalent to estimating mean groundenergy to constant accuracy ($e_o(H) := E_0(H)/m$)
- And to estimate the energy at constant temperature

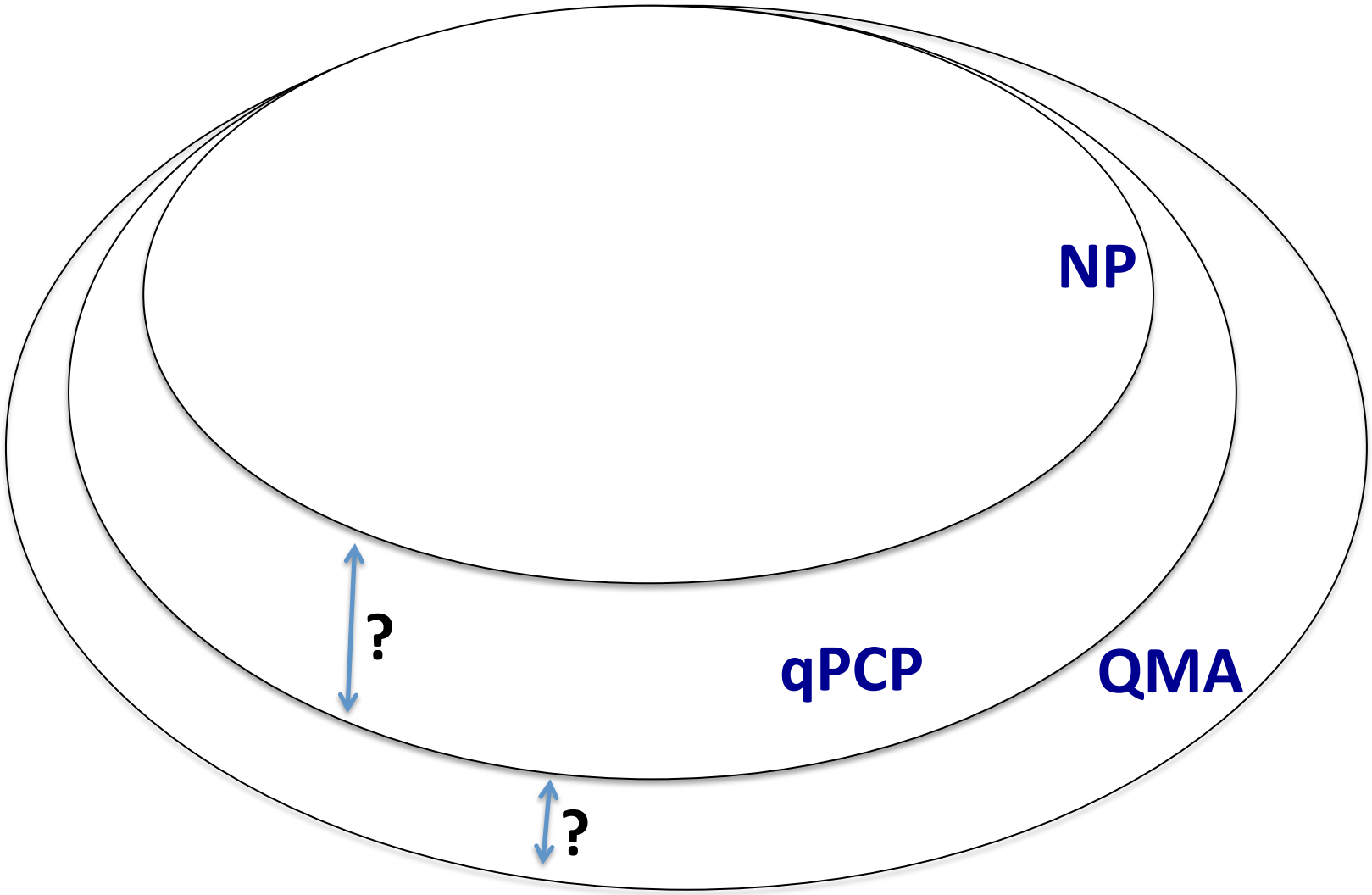
Quantum PCP?

The qPCP conjecture: There is $\varepsilon > 0$ s.t. the following problem is QMA-complete: Given 2-local Hamiltonian H with m local terms determine whether

(i) $E_0(H)=0$ or (ii) $E_0(H) > \varepsilon m$.

- (Bravyi, DiVincenzo, Loss, Terhal '08) Equivalent to conjecture for $O(1)$-local Hamiltonians over qdits.
- Equivalent to estimating mean groundenergy to constant accuracy ($e_o(H) := E_0(H)/m$)
- And to estimate the energy at constant temperature
- At least NP-hard (by PCP Thm) and in QMA

Quantum PCP?



Previous Work and Obstructions

(Aharonov, Arad, Landau, Vazirani '08)
Quantum version of 1 of 3 parts of Dinur's proof of the PCP thm (gap amplification)

But: The other two parts (alphabet and degree reductions) involve massive copying of information; not clear how to do it with a highly entangled assignment

Previous Work and Obstructions

(Aharonov, Arad, Landau, Vazirani '08)
Quantum version of 1 of 3 parts of Dinur's proof of the PCP thm (gap amplification)

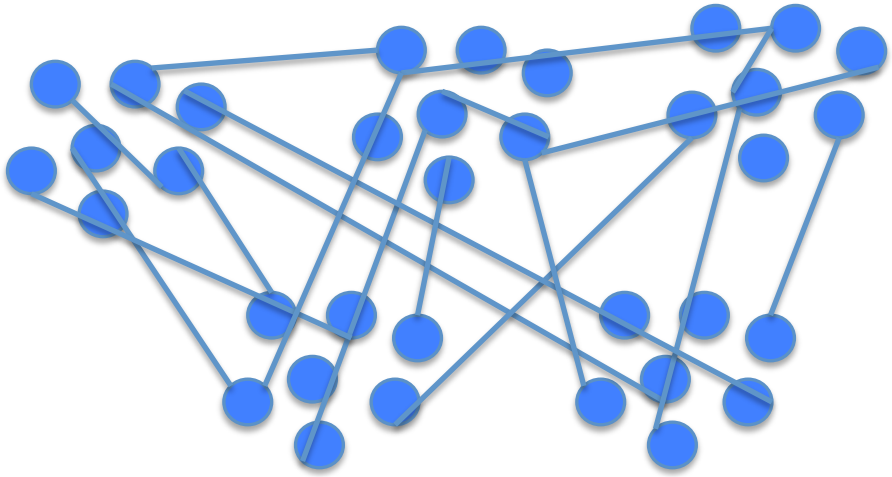
But: The other two parts (alphabet and degree reductions) involve massive copying of information; not clear how to do it with a highly entangled assignment

(Bravyi, Vyalyi '03; Arad '10; Hastings '12; Freedman, Hastings '13; Aharonov, Eldar '13, …)
No-go for large class of *commuting* Hamiltonians and almost commuting Hamiltonians

But: Commuting case might always be in NP

Approximation in NP

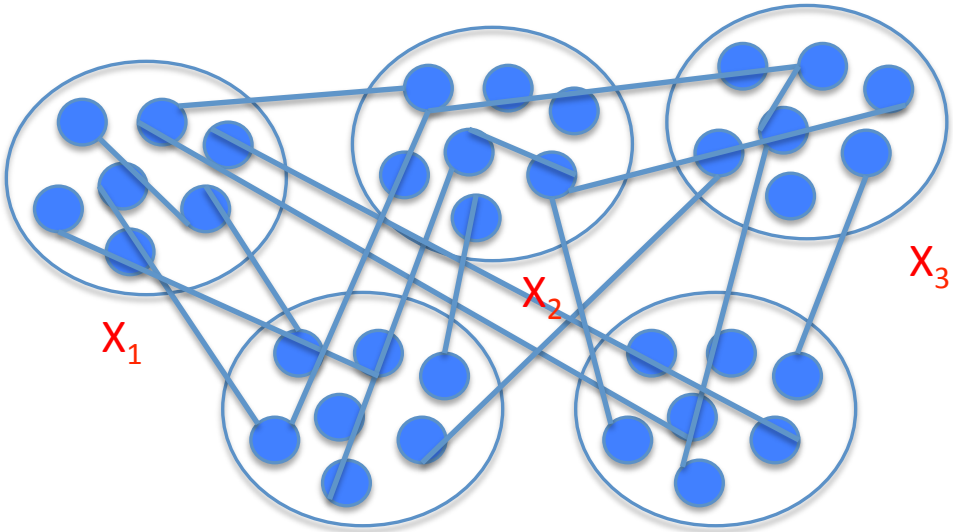
(B., Harrow '12) Let H be a 2-local Hamiltonian on qudits with interaction graph G(V, E) and |E| local terms.



Approximation in NP

(B., Harrow '12) Let H be a 2-local Hamiltonian on qudits with interaction graph $G(V, E)$ and $|E|$ local terms.

Let $\{X_i\}$ be a partition of the sites with each X_i having m sites.



$m < O(\log(n))$

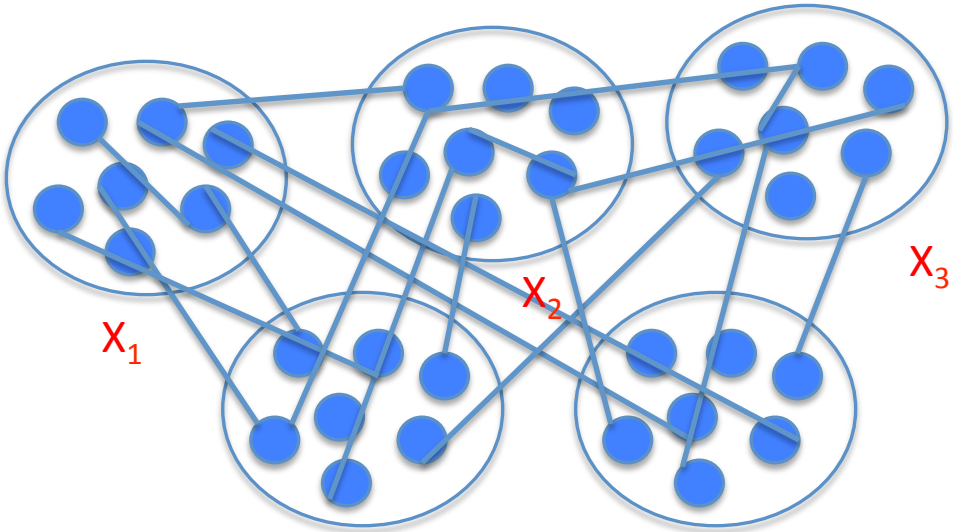
Approximation in NP

(B., Harrow '12) Let H be a 2-local Hamiltonian on qudits with interaction graph G(V, E) and |E| local terms.

Let $\{X_i\}$ be a partition of the sites with each X_i having m sites.
Then there are products states ψ_i in X_i s.t.

$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H)+\Omega\left(d^6 E_i \Phi(X_i)\frac{1}{\deg(G)}E_i\frac{S(X_i)}{m}\right)^{1/8}$$

E_i : expectation over X_i
deg(G) : degree of G
$\Phi(X_i)$: expansion of X_i
$S(X_i)$: entropy of groundstate in X_i



m < O(log(n))

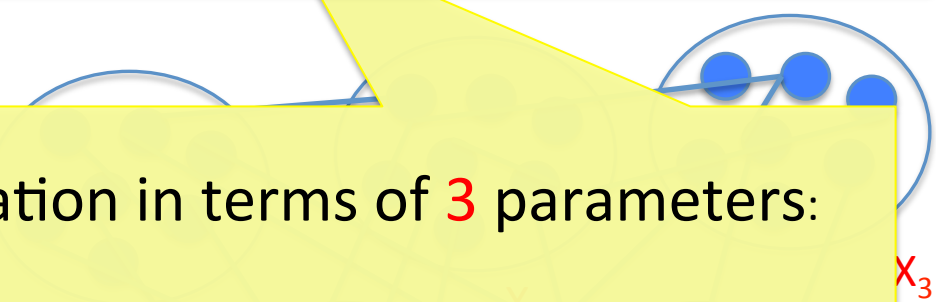
Approximation in NP

(B., Harrow '12) Let H be a 2-local Hamiltonian on qudits with interaction graph G(V, E) and |E| local terms.

Let $\{X_i\}$ be a partition of the sites with each X_i having m sites.
Then there are products states ψ_i in X_i s.t.

$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H)+\Omega\left(d^6 E_i \Phi(X_i)\frac{1}{\deg(G)}E_i\frac{S(X_i)}{m}\right)^{1/8}$$

E_i : expectation over X_i
deg(G) : degree of G
$\Phi(X_i)$: expansion of X_i
$S(X_i)$: entropy of groundstate in X_i



Approximation in terms of 3 parameters:

1. Average expansion
2. Degree interaction graph
3. Average entanglement groundstate

Approximation in terms of degree

$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H)+\Omega\left(d^6 E_i \Phi(X_i)\boxed{\frac{1}{\deg(G)}}E_i\frac{S(X_i)}{m}\right)^{1/8}$$

No classical analogue:

(PCP + parallel repetition) For all $\alpha, \beta, \gamma > 0$ it's NP-complete to determine whether a CSP *C* is s.t.

Unsat = 0 or Unsat > $\alpha\, \Sigma^{\beta}/\deg(G)^{\gamma}$

Parallel repetition: *C* -> *C'*

i. $\deg(G') = \deg(G)^k$
ii. $\Sigma' = \Sigma^k$
ii. Unsat(G') > Unsat(G)

(Raz '00) even showed Unsat(G') approaches 1 exponentially fast

Approximation in terms of degree

$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H) + \Omega\left(d^6 E_i \Phi(X_i) \boxed{\frac{1}{\deg(G)}} E_i \frac{S(X_i)}{m}\right)^{1/8}$$

No classical analogue:

(PCP + parallel repetition) For all $\alpha, \beta, \gamma > 0$ it's NP-complete to determine whether a CSP *C* is s.t.

Unsat = 0 or Unsat > $\alpha\, \Sigma^{\beta}/\deg(G)^{\gamma}$

Contrast: It's in NP determine whether a Hamiltonian H is s.t

$E_0(H)=0$ or $E_0(H) > \alpha d^{3/4}/\deg(G)^{1/8}$

Quantum generalizations of PCP *and* parallel repetition *cannot* both be true (assuming QMA not in NP)

Approximation in terms of degree

$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H)+\Omega\left(d^6 E_i \Phi(X_i)\boxed{\frac{1}{\deg(G)}}E_i\frac{S(X_i)}{m}\right)^{1/8}$$

No classical analogue:

(PCP + parallel repetition) For all $\alpha, \beta, \gamma > 0$ it's NP-complete to determine whether a CSP *C* is s.t.

Unsat = 0 or Unsat > $\alpha\ \Sigma^{\beta}/\deg(G)^{\gamma}$

Bound: $\Phi_G < ½ - \Omega(1/\deg)$ implies

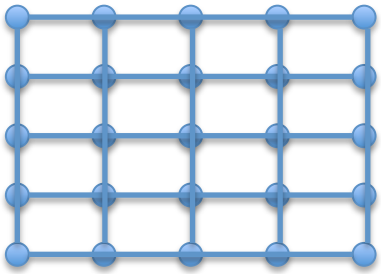
Highly expanding graphs (Φ_G -> 1/2) are not hard instances

Approximation in terms of degree

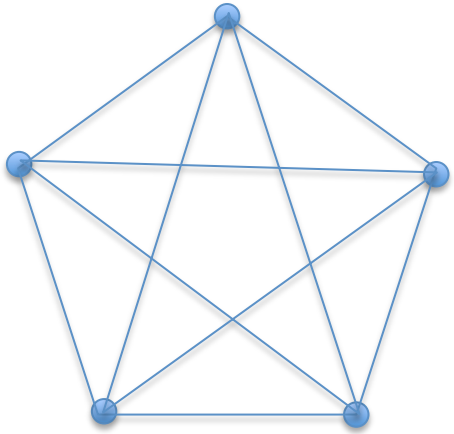
...shows mean field becomes exact in high dim

1-D

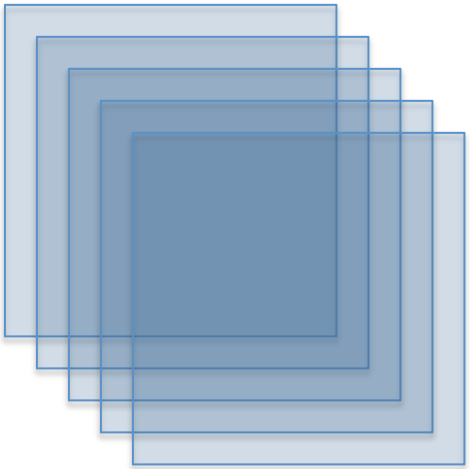
2-D



∞-D



3-D



Rigorous justification to folklore in condensed matter physics

Approximation in terms of average entanglement

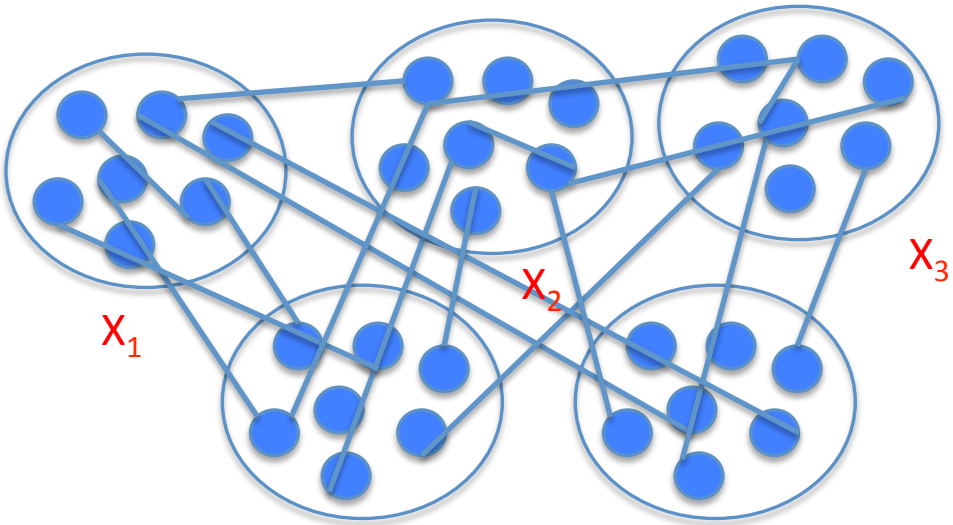
$$\frac{1}{|E|}\langle\psi_1,\ldots,\psi_m|H|\psi_1,\ldots,\psi_m\rangle \le e_0(H)+\Omega\left(d^6 E_i \Phi(X_i)\frac{1}{\deg(G)}\boxed{E_i\frac{S(X_i)}{m}}\right)^{1/8}$$

The problem is in NP if entanglement of groundstate satisfies a subvolume law:

$$E_i\frac{S(X_i)}{m}=o(1)$$

Connection of amount of entanglement in groundstate and computational complexity of the model

m < O(log(n))



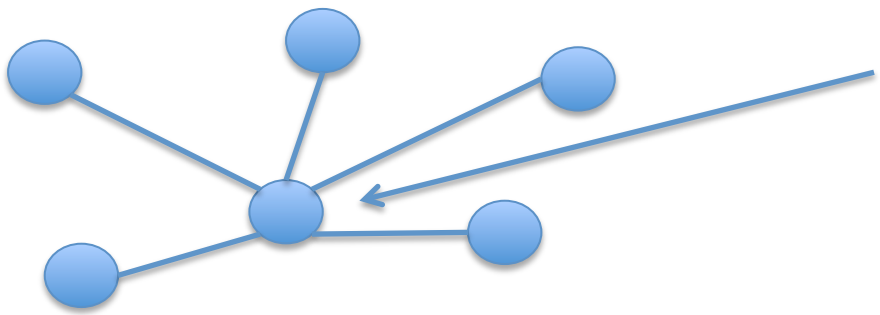
New Classical Algorithms for Quantum Hamiltonians

Following same approach we also obtain polynomial time algorithms for approximating the groundstate energy of

1. Planar Hamiltonians, improving on (Bansal, Bravyi, Terhal '07)
2. Dense Hamiltonians, improving on (Gharibian, Kempe '10)
3. Hamiltonians on graphs with low threshold rank, building on (Barak, Raghavendra, Steurer '10)

In all cases we prove that a product state does a good job and use efficient algorithms for CSPs.

Proof Idea: Monogamy of Entanglement



Cannot be highly entangled with too many neighbors

Entropy quantifies how entangled can be

Proof uses information-theoretic techniques (chain rule of conditional mutual information, informationally complete POVMs, etc) to make this intuition precise

Inspired by classical information-theoretic ideas for bounding convergence of SoS hierarchy for CSPs
(Tan, Raghavendra '10, Barak, Raghavendra, Steurer '10)

Quantum Information Method

- Condensed Matter Physics: Tensor Network States (Cirac, Hastings, Verstraete, Vidal, …)
- Mathematical Physics: Area Law from Exponential Decay of Correlations (B., Horodecki '12)
- Computational Complexity: Lower bounds on LP extensions for Travel Salesman Problem (Fiorini et al '11)
- Compressed Sensing: Better low rank matrix recovery methods (Gross et al '10)
- Etc, see (Drucker, de Wolf '09) for more

Conclusions

QIT useful to bound SoS hierarchy

- Quasi-polynomial algorithm for deciding entanglement
- Connections 2->4 norm, Small Set Expansion
- New approach to resolve UGC
  (improve quantum SoS bound and/or quantum hardness)

QIT useful to bound efficiency of mean-field theory

- Cornering quantum PCP
- Poly-time algorithms for planar and dense Hamiltonians

Thank you!