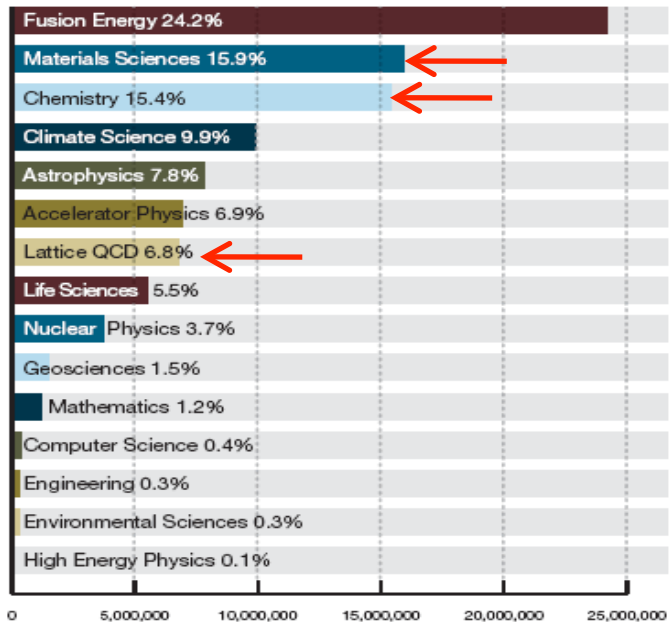
Monogamy of Quantum Entanglement

Fernando G.S.L. Brandão
ETH Zürich

Princeton EE Department, March 2013

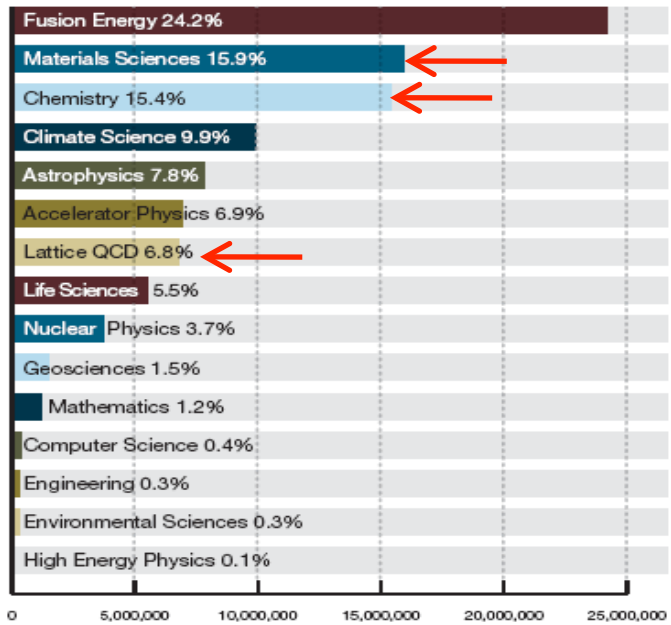
Simulating quantum is hard



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



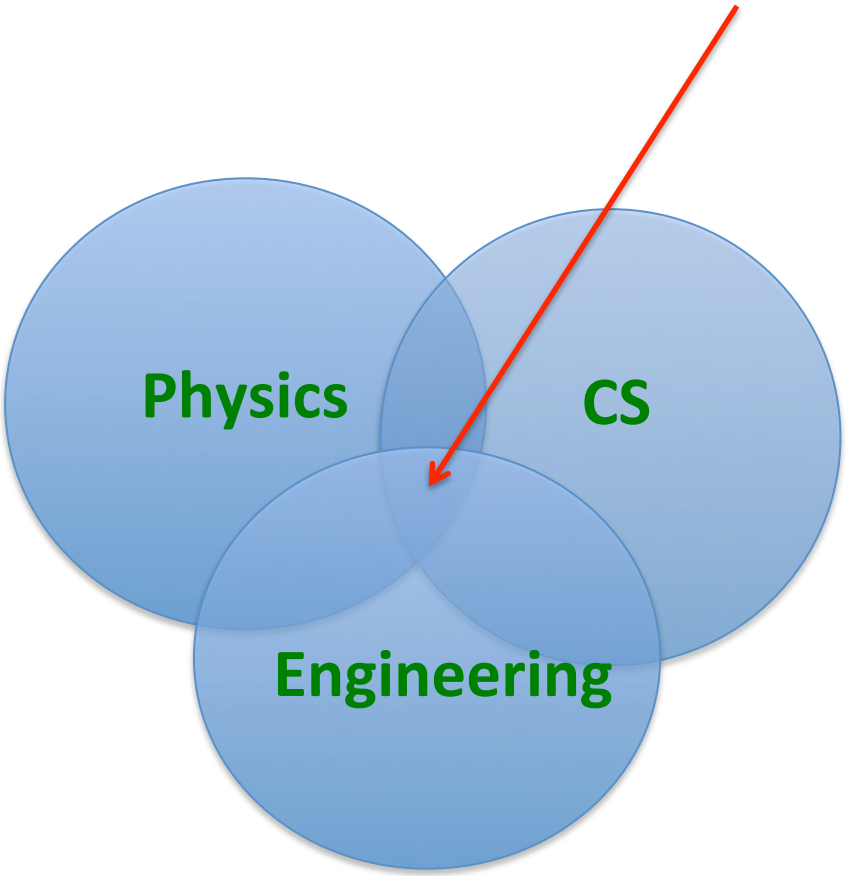
More than **25%** of **DoE supercomputer power** is devoted to simulating quantum physics

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, engineering** and **physics**

The Two Holy Grails of QIS

Quantum Computation:

Use of engineered **quantum systems for** performing **computation**

Exponential speed-ups over classical computing

E.g. Factoring (RSA)
Simulating quantum systems

Quantum Cryptography:

Use of engineered **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:

Use of engineered **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

While waiting for a quantum computer

…how can a *theorist* help?

Answer 1: figuring out **what to do with a quantum computer** and the **fastest way of building one**

(quantum communication, quantum algorithms, quantum fault tolerance, quantum simulators, …)

While waiting for a quantum computer

…how can a *theorist* help?

Answer 1: figuring out **what to do with a quantum computer** and the **fastest way of building one**

(quantum communication, quantum algorithms, quantum fault tolerance, quantum simulators, …)

Answer 2: finding applications of **QIS independent** of building a **quantum computer**

While waiting for a quantum computer

…how can a *theorist* help?

Answer 1: figuring out **what to do with a quantum computer** and the **fastest way of building one**

(quantum communication, quantum algorithms, quantum fault tolerance, quantum simulators, …)

Answer 2: finding applications of **QIS independent** of building a **quantum computer**

This talk

Quantum Mechanics I

probability theory based on L_2 norm instead of L_1

States: norm-one vector in C^d:

$$|\psi\rangle := (\psi_1, \ldots, \psi_d)^T$$

$$\|\psi\|_2 = \sqrt{\langle\psi|\psi\rangle} = 1$$

Dynamics: L_2 norm preserving linear maps,
unitary matrices: $\mathbf{UU^T = I}$

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

Born's rule: $\Pr(k) = \langle\psi|M_k|\psi\rangle$

Quantum Mechanics II

probability theory based on PSD matrices

Mixed States: PSD 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: $\langle\psi| := (\psi_1^*, \ldots, \psi_d^*)$

Dynamics: linear operations mapping density matrices to density matrices (unitaries + adding ancilla + ignoring subsystems)

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

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*.

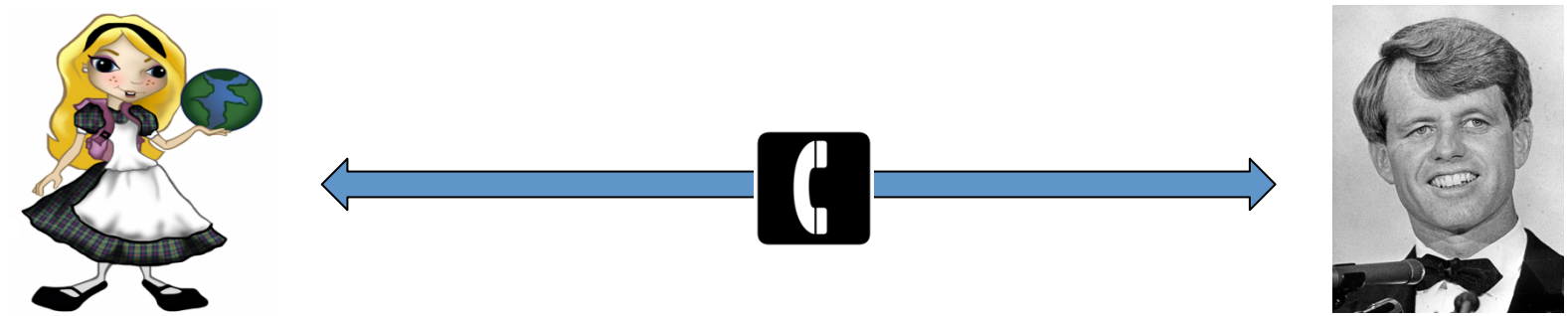
Mixed States: $\rho_{AB} \in D(C^d \otimes C^l)$

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:

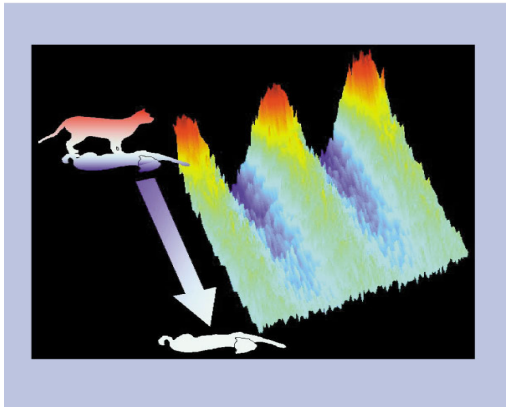
$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$$

Entangled states cannot be created by LOCC:

non-classical correlations

Quantum Features

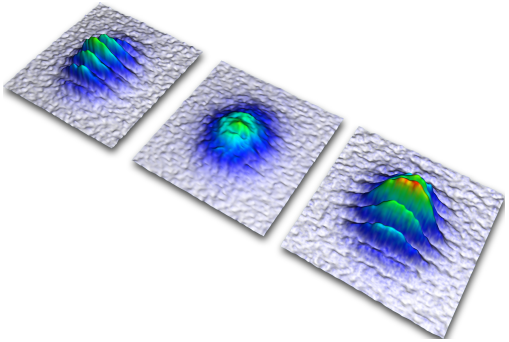
Superposition principle



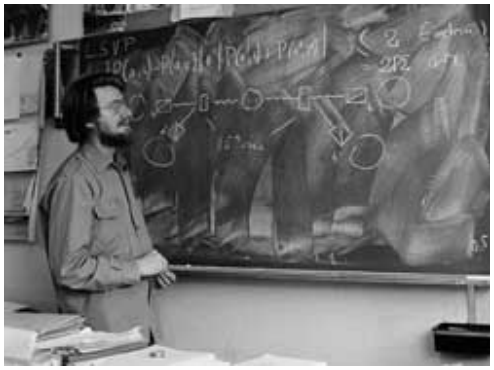
uncertainty principle

$$\Delta x \Delta P \geqslant \hbar/2$$

interference



non-locality



Monogamy of Entanglement

Monogamy of Entanglement

Maximally Entangled State: $|\phi\rangle_{AB} = \left(|00\rangle + |11\rangle\right)/\sqrt{2}$

Correlations of A and B in $|\phi\rangle\langle\phi|_{AB}$ *cannot* be shared:

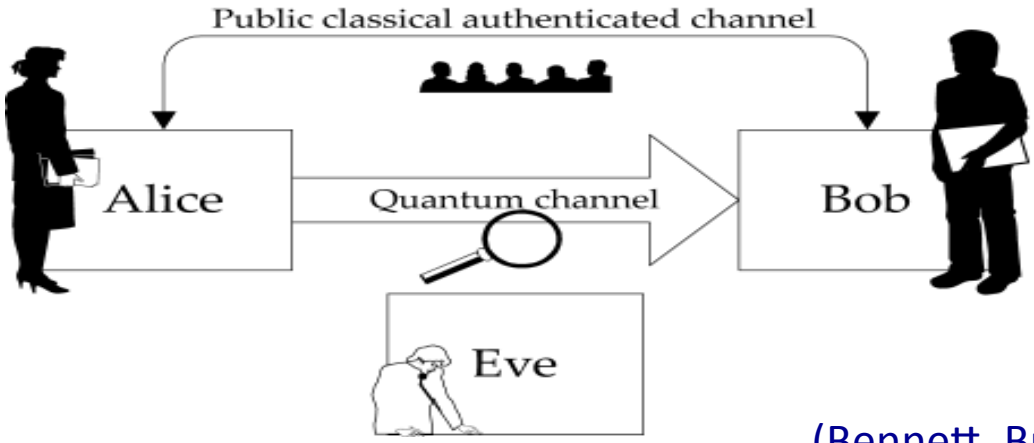
If ρ_{ABE} is s.t. $\rho_{AB} = |\phi\rangle\langle\phi|_{AB}$, then $\rho_{ABE} = |\phi\rangle\langle\phi|_{AB} \otimes \rho_E$

Only knowing that the quantum correlations of A and B are very strong one can infer A and B are *not* correlated with anything else.

Purely quantum mechanical phenomenon!

Quantum Key Distribution…

… as an application of entanglement monogamy

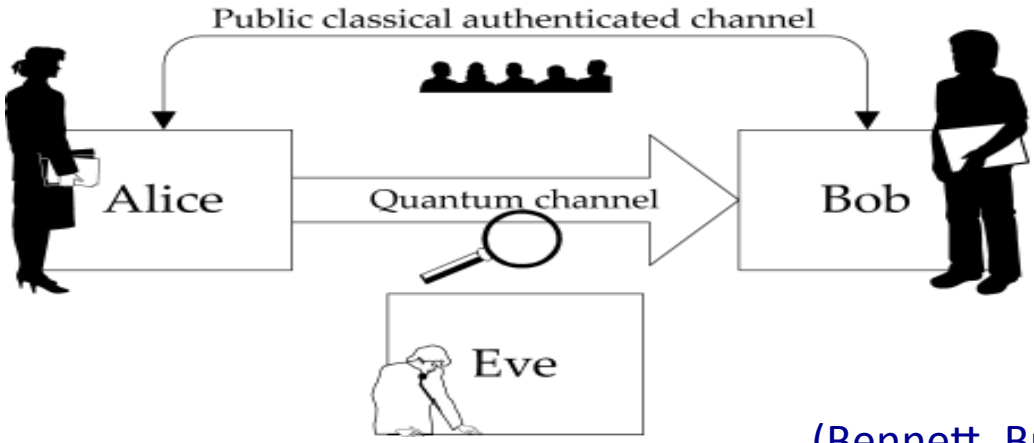


(Bennett, Brassard 84, Ekert 91)

- Using insecure channel Alice and Bob share entangled state ρ_{AB}
- Applying LOCC they distill $|\phi\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$

Quantum Key Distribution…

… as an application of entanglement monogamy



(Bennett, Brassard 84, Ekert 91)

- Using insecure channel Alice and Bob share entangled state ρ_{AB}
- Applying LOCC they distill $|\phi\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$

Let π_{ABE} be the state of Alice, Bob and the Eavesdropper. Since $\pi_{AB} = |\phi\rangle\langle\phi|_{AB}$, $\pi_{AB} = |\phi\rangle\langle\phi|_{AB} \otimes \pi_E$. Measuring A and B in the computational basis give 1 bit of secret key.

Outline

Entanglement Monogamy

How general is the concept?
Can we make it quantitative?
Are there other applications/implications?

1. Detecting Entanglement and Sum-Of-Squares Hierarchy

2. Accuracy of Mean-Field Approximation

3. Other Applications

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:

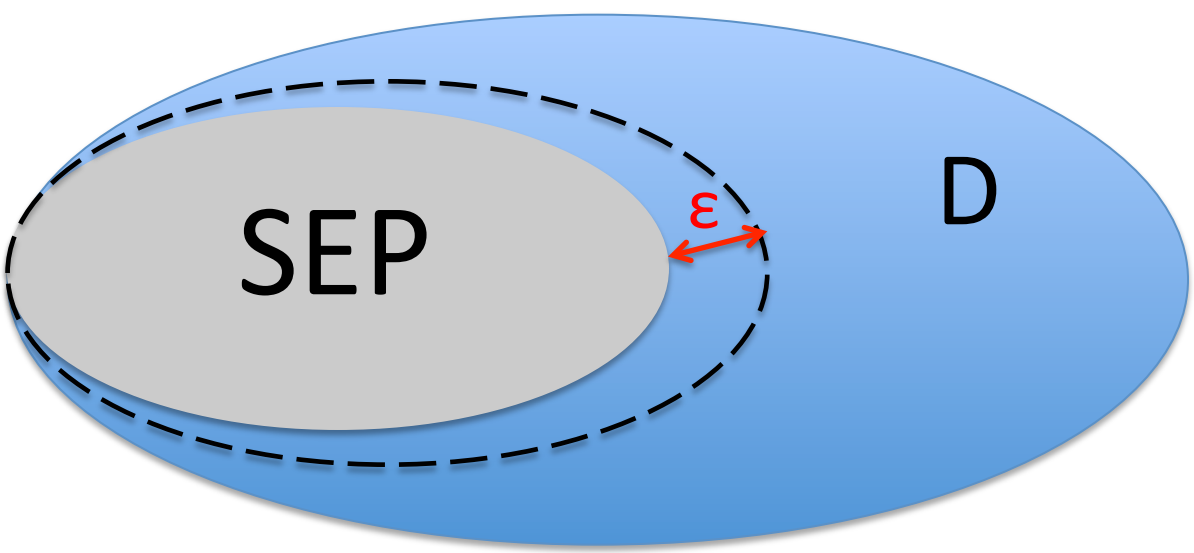
Best known algorithm using monogamy of entanglement

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

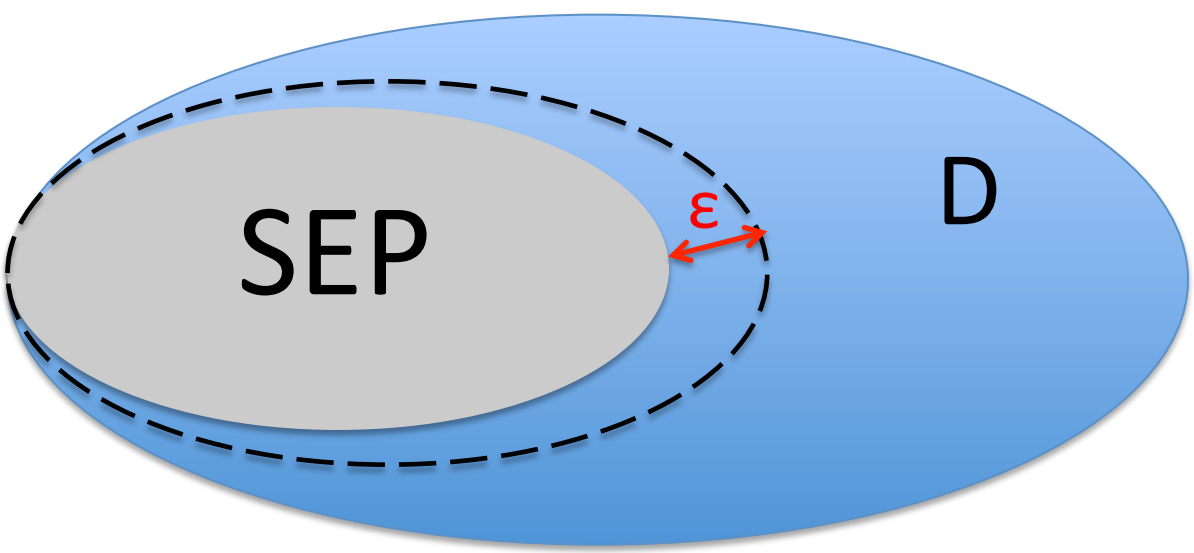


The Separability Problem

- 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



Frobenius norm

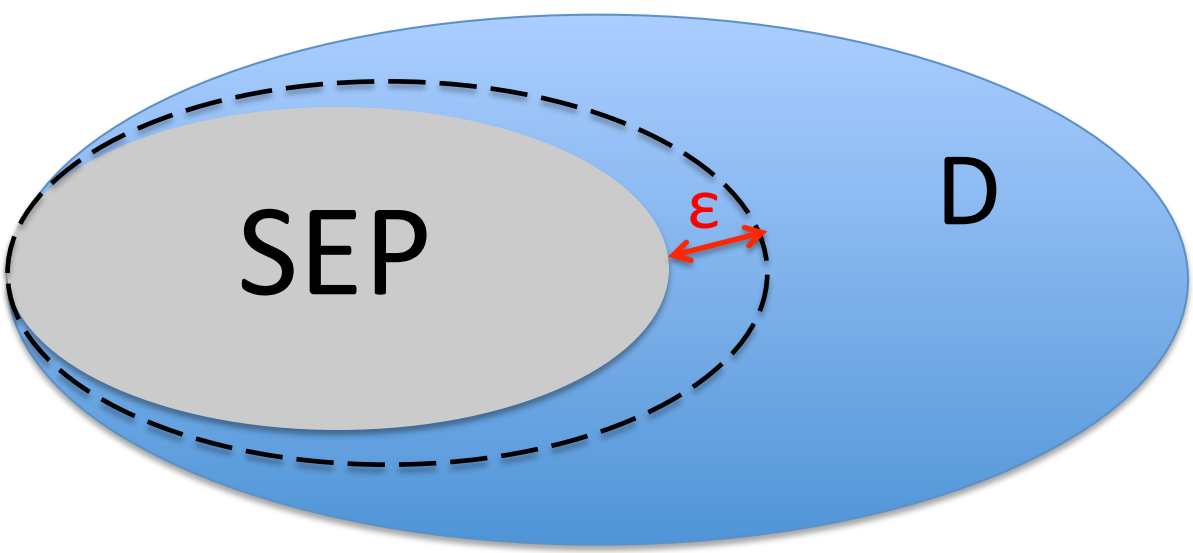
$$\|X\|_2 = tr\left(X^T X\right)^{1/2}$$

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



Frobenius norm

$$\|X\|_2 = tr\left(X^T X\right)^{1/2}$$

LOCC norm

$$\|\rho - \sigma\|_{LOCC} = \max_{M \in LOCC} tr(M(\rho - \sigma))$$

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…

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

dim of A

State-of-the-art: $2^{O(|A|\log|B|)}$ time complexity

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 $\varepsilon=1/\mathrm{poly}(|A||B|)$

(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 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 an algorithm with run time $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ for $W_{SEP}(||*||, \varepsilon)$

Quasipolynomial-time Algorithm

(B., Christandl, Yard '11) There is an algorithm with run time $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ for $W_{SEP}(||*||, \varepsilon)$

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

Contrast with:

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

Quasipolynomial-time Algorithm

(B., Christandl, Yard '11) For M in 1-LOCC, can compute $h_{SEP}(M)$ within additive error ε in time $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$

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

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 in SEP: $$M = \sum_k A_k \otimes B_k, \quad A_k, B_k \geq 0, M \leq I$$

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, …)

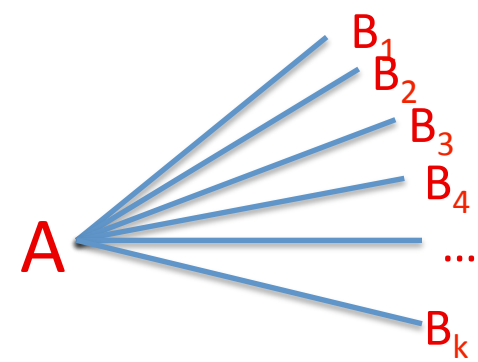
We'll derive SoS hierarchy exploring ent. monogamy

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*

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

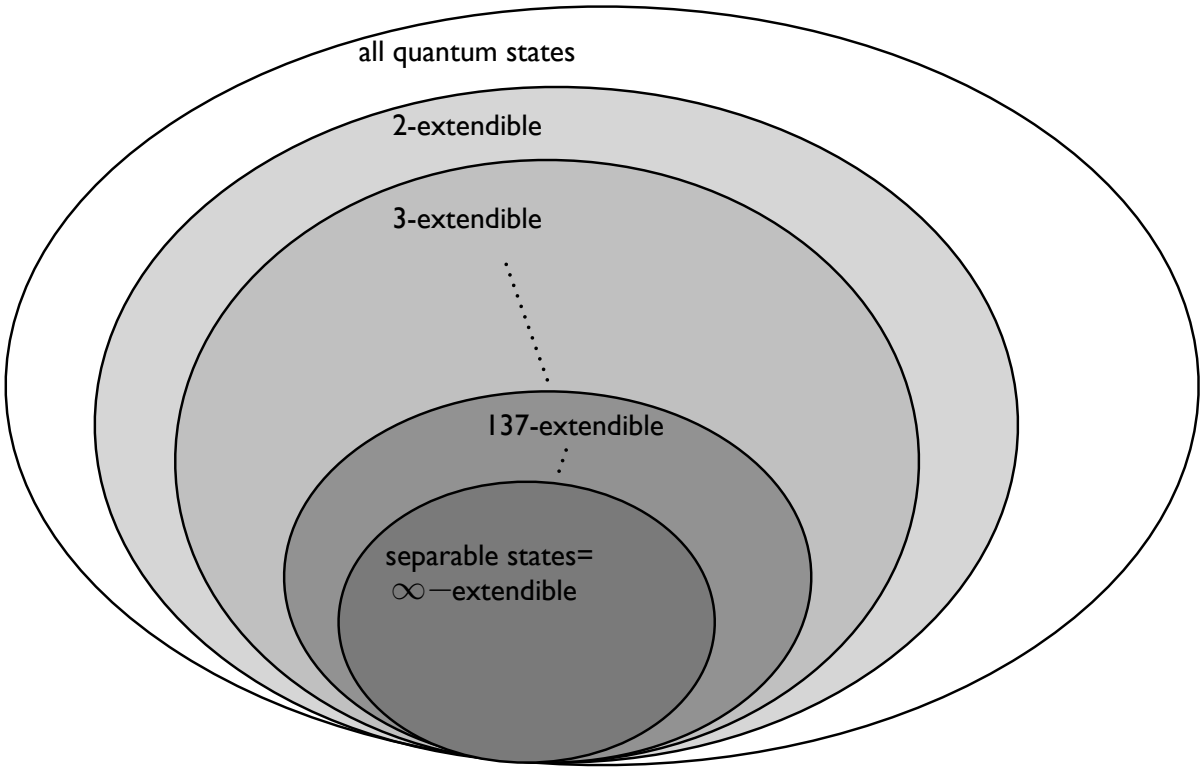


Def. ρ_{AB} is k-extendible if there is $\rho_{AB1\ldots Bk}$ s.t for all j in [k], $\mathrm{tr}_{\setminus Bj}(\rho_{AB1\ldots Bk}) = \rho_{AB}$

Monogamy Defines Entanglement

(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):

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

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

(Koenig, Renner '04) De Finetti Bound

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

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

(Koenig, Renner '04) De Finetti Bound

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

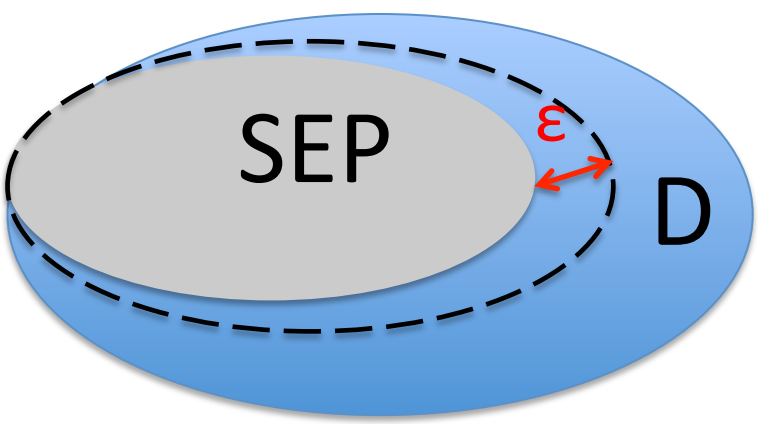
<u>Improved de Finetti Bound</u> (B., Christandl, Yard '11)

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

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

<u>Improved de Finetti Bound</u>

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



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

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

Proving…

<u>Improved de Finetti Bound</u>

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

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…

<u>Improved de Finetti Bound</u>

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

Proof is information-theoretic

Mutual Information:

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

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

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

(chain rule)

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

Proving…

<u>Improved de Finetti Bound</u>

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

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}

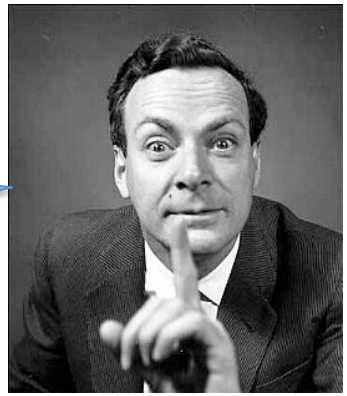
$\log|A| > I(A:B_1\ldots B_k) = I(A:B_1)+I(A:B_2|B_1)+\ldots+I(A:B_k|B_1\ldots B_{k-1})$

(chain rule)

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

Quantum Information?

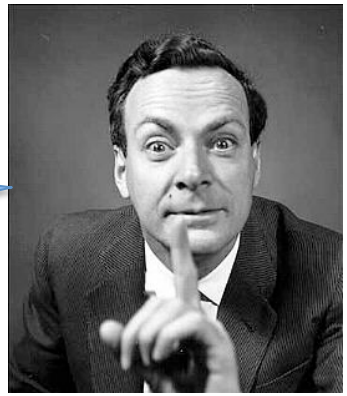
Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.



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)

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

Obs: I(A:B|E)≥0 is strong subadditivity inequality (Lieb, Ruskai '73)

Chain rule:

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

For ρ_{AB} *k*-extendible: $$2\log|A| \geq \frac{k}{2\ln 2} \min_{\sigma \in SEP} \left\| \rho_{AB} - \sigma_{AB} \right\|^2$$

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, Optimal acceptance probability in QMA(2), ….

4. 2->q norms of projectors: $\|P\|_{2\to q} := \max_{\|x\|_2=1} \|Px\|_q$

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

($||*||_{2\text{->}q}$ for q > 2 are hypercontractive norms: useful in Markov Chain Monte Carlo (rapidly mixing condition), etc)

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 ε-Small Set Expansion Problem (closely related to unique games).
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 ε-Small Set Expansion Problem (closely related to unique games).
Alternative algorithm to (Arora, Barak, Steurer '10)

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

Can formulate it as a quantum information-theoretic problem

Outline

Entanglement Monogamy

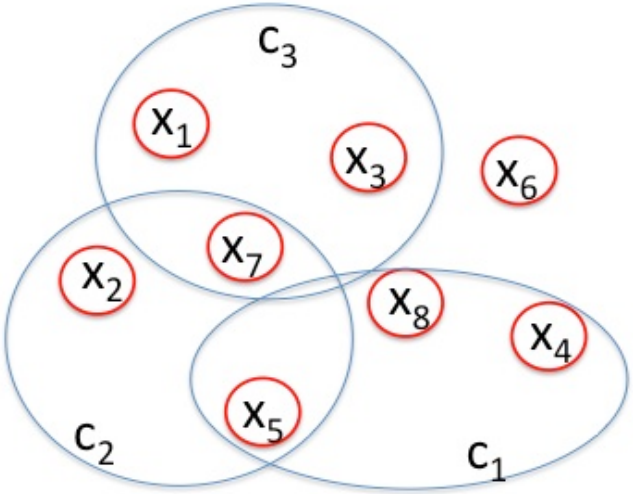
How general is the concept?
Can we make it quantitative?
Are there other applications/implications?

1. Detecting Entanglement and Sum-Of-Squares Hierarchy

2. Accuracy of Mean Field Approximation

3. Other applications

Constraint Satisfaction Problems vs Local Hamiltonians



k-arity CSP:

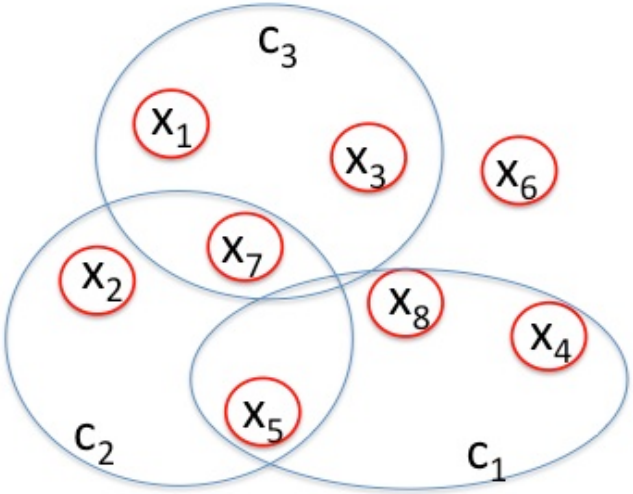
Variables $\{x_1, \ldots, x_n\}$, alphabet Σ

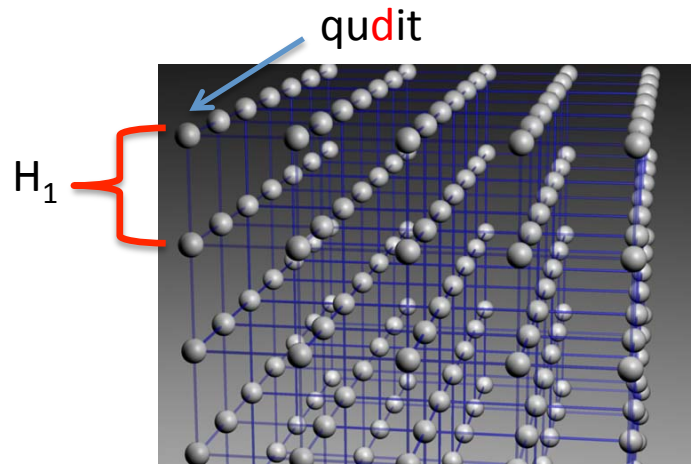
Constraints: $c_j : \Sigma^k \to \{0,1\}$

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, Laughlin states for FQHE,…)

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

Optimal Assignments: Entangled States

Non-entangled state: $\left(a_1|0\rangle + b_1|1\rangle\right) \otimes \ldots \otimes \left(a_n|0\rangle + b_n|1\rangle\right)$

e.g. $|\uparrow\rangle \otimes \ldots \otimes |\uparrow\rangle$

Entangled states: $\sum_{i_1,\ldots,i_n} c_{i_1,\ldots,i_n} |i_1,\ldots,i_n\rangle$

e.g. $\left(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right) / \sqrt{2}$

To describe a general entangled state of n spins requires exp(O(n)) bits

How Entangled?

Given bipartite entangled state $\left|\psi\right\rangle_{AB} \in C^n \otimes C^m$

the reduced state on A is mixed: $\rho_A \geq 0,\ tr(\rho_A) = 1$

The more mixed ρ_A, the more entangled ψ_{AB}:

Quantitatively: $E(\psi_{AB}) := S(\rho_A) = -tr(\rho_A \log \rho_A)$

Is there a relation between the amount of entanglement in the ground-state and the computational complexity of the model?

Mean-Field…

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

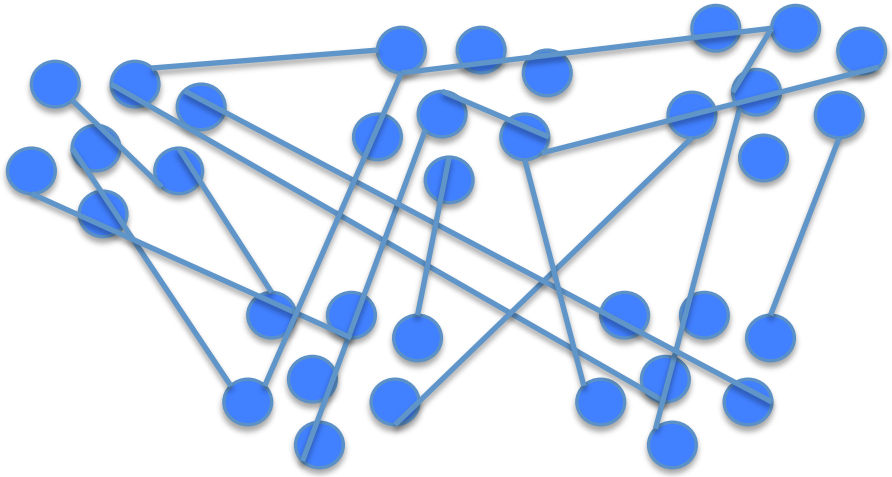
$$\max_{\psi_1,\ldots,\psi_n} \langle \psi_1,\ldots,\psi_n | H | \psi_1,\ldots,\psi_n \rangle$$ is a CSP

Successful heuristic in Quantum Chemistry (e.g. Hartree-Fock)
Condensed matter (e.g. BCS theory)

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

Mean-Field Good When

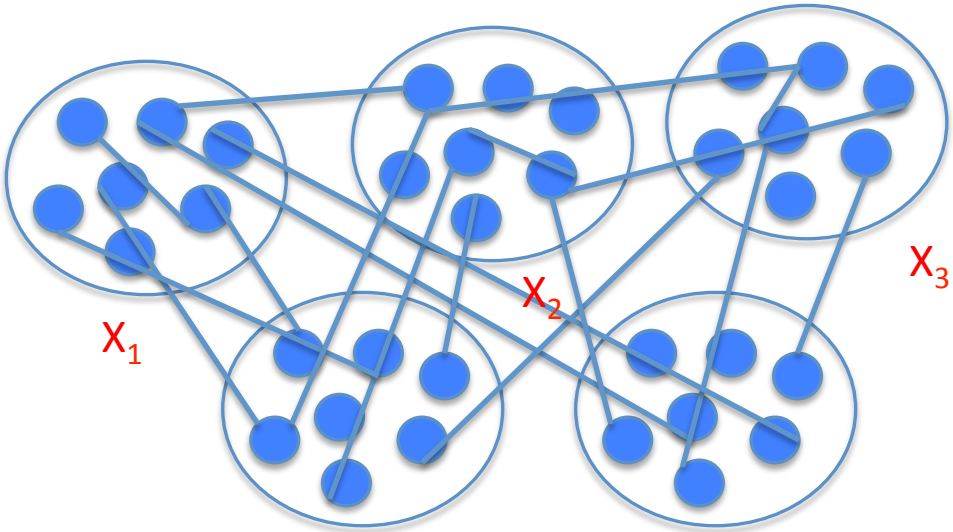
(B., Harrow '12) Let H be a 2-local Hamiltonian on qudits with interaction graph G(V, E) and |E| local terms.



Mean-Field Good When

(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.



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

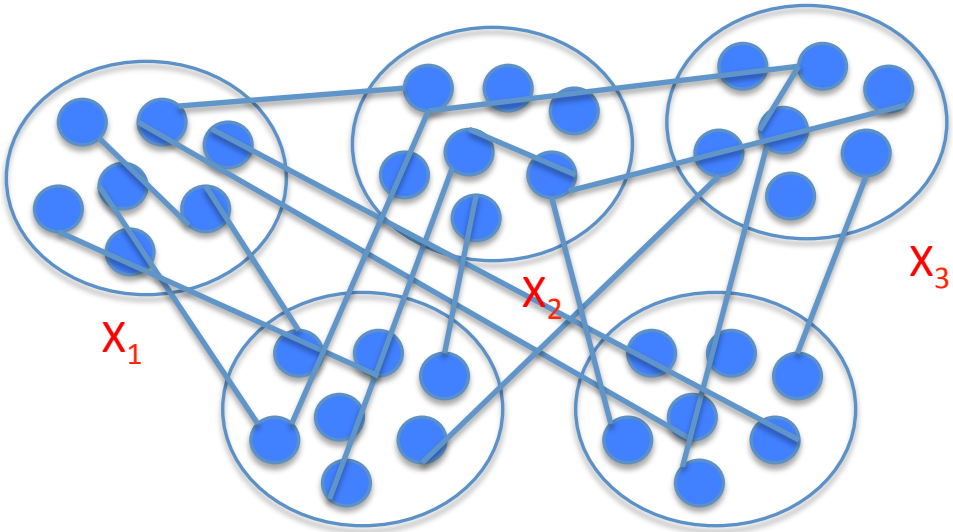
Mean-Field Good When

(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.

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

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



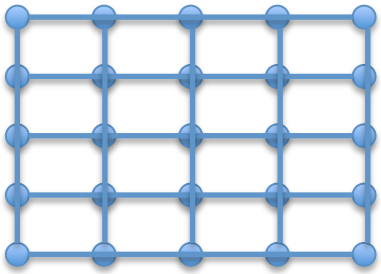
$m < O(\log(n))$

Approximation in terms of degree

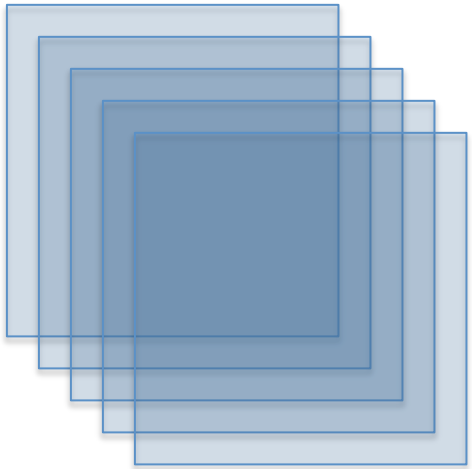
...shows mean field becomes exact in high dim

1-D

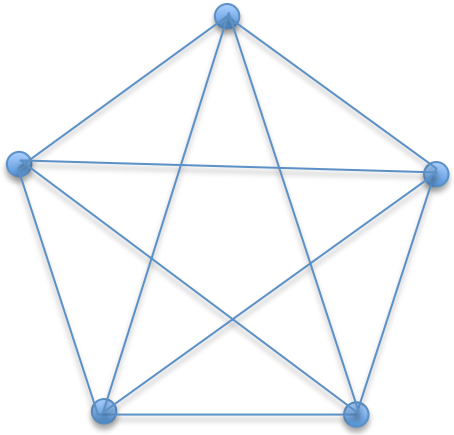
2-D



3-D



∞-D



Approximation in terms of degree

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

Relevant to the quantum PCP problem:

(Aharonov, Arad, Landau, Vazirani '08; Freedman, Hastings '12; Bravyi, DiVincenzo, Loss, Terhal '08, Aaronson '08)

Is approximating $e_0(H)$ to constant accuracy *quantum NP-hard*?

It shows that quantum generalizations of PCP theorem and parallel repetition *cannot* both be true (assuming "quantum NP"= QMA ≠ NP)

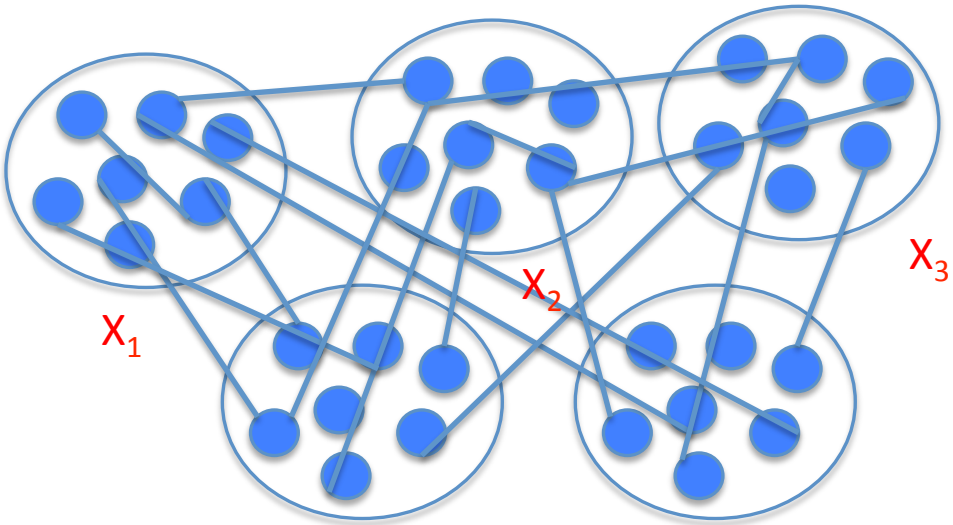
Approximation in terms of average entanglement

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

Mean-field works well if entanglement of groundstate satisfies a subvolume law:

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

m < O(log(n))



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

Approximation in terms of average entanglement

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

Systems with low entanglement are expected to be simpler

So far only precise in 1D:

Area law for entanglement -> Succinct classical description (MPS)

Here:

Good: arbitrary lattice, only subvolume law

Bad: Only mean energy approximated well

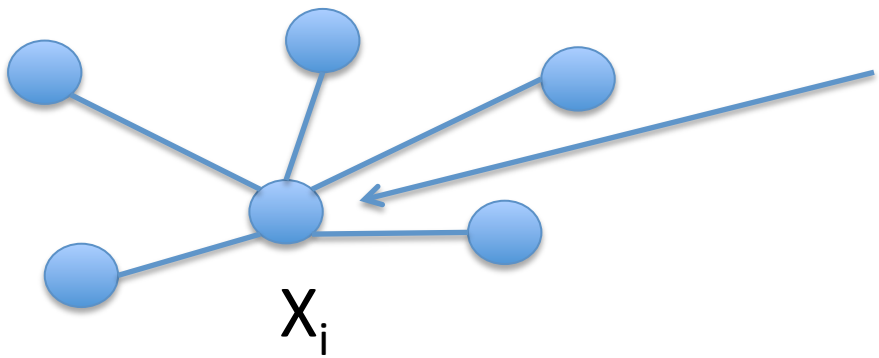
New Algorithms for Quantum Hamiltonians

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 $S(X_i)$ quantifies how entangled it can be

Proof uses information-theoretic techniques (chain rule of conditional mutual information, informationally complete measurements, 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)

Outline

Entanglement Monogamy

How general is the concept?
Can we make it quantitative?
Are there other applications/implications?

1. Detecting Entanglement and Sum-Of-Squares Hierarchy

2. Accuracy of Mean Field Approximation

3. Other applications

Other Applications

(B., Horodecki '12)

Proving entanglement area law from exponential decay of correlations for 1D states

(Almheiri, Marolf, Polchinski, Sully '12)

Black hole firewall controversy

(Vidick, Vazirani '12; Bartett, Colbeck, Kent '12; …)

Device independent key distribution

(Vidick and Ito '12)

Entangled multiple proof systems: NEXP in MIP*

Conclusions

Entanglement Monogamy is a distinguishing feature of quantum correlations

(quantum engineering)
It's at the heart of quantum cryptography

(convex optimization)
Can be used to detect entanglement efficiently and understand Sum-Of-Squares hierarchy better

(computational physics)
Can be used to bound efficiency of mean-field approximation

(quantum many-body physics)
Can be used to prove area law from exponential decay of correlations

Thank you!