

The Complexity of Quantum Entanglement

Fernando G.S.L. Brandão

ETH Zürich

Based on joint work with M. Christandl and J. Yard

Journées Déformation de Recherche en Mathématiques de Paris
Centre/GT Informatique Quantique

Paris, 09/05/2012

Quadratic vs Biquadratic Optimization

Problem 1: For M in $H(\mathbb{C}^d)$ ($d \times d$ 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 $H(\mathbb{C}^d)$ ($d \times d$ 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 $H(\mathbb{C}^d \otimes \mathbb{C}^l)$, compute

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

Quadratic vs Biquadratic Optimization

Problem 1: For M in $H(\mathbb{C}^d)$ ($d \times d$ 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 $H(\mathbb{C}^d \otimes \mathbb{C}^l)$, compute

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

This talk:

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

Outline

- **The Problem**
Quantum States
Quantum Entanglement
- **The Algorithm**
Parrilo-Lasserre Relaxation
Monogamy of Entanglement
Quantum de Finetti Theorem
- **Applications**
A new characterization of Quantum NP
Small Set Expansion
- **Proof Ideas**

Quantum States

- **Pure States:** norm-one vector in \mathbb{C}^d :

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

- **Mixed States:** positive semidefinite matrix of unit trace:

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

Dirac notation reminder: $\langle\psi| := (\psi_1, \dots, \psi_d)$

Quantum Measurements

- To any experiment with d outcomes we associate d

positive matrices $\{M_k\}$ such that
$$\sum_k M_k = I$$

and calculate probabilities as
$$\Pr(k) = \text{tr}(M_k \rho)$$

E.g. For pure states,
$$\Pr(k) = \langle \psi | M_k | \psi \rangle$$

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*.

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:

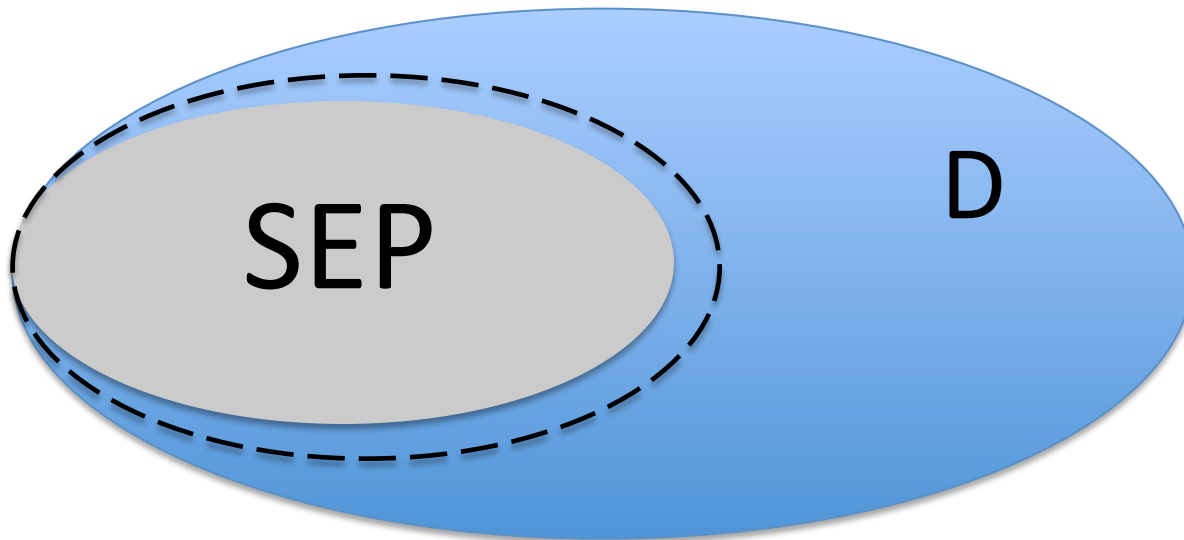
$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$$

Entangled states cannot be created by LOCC:

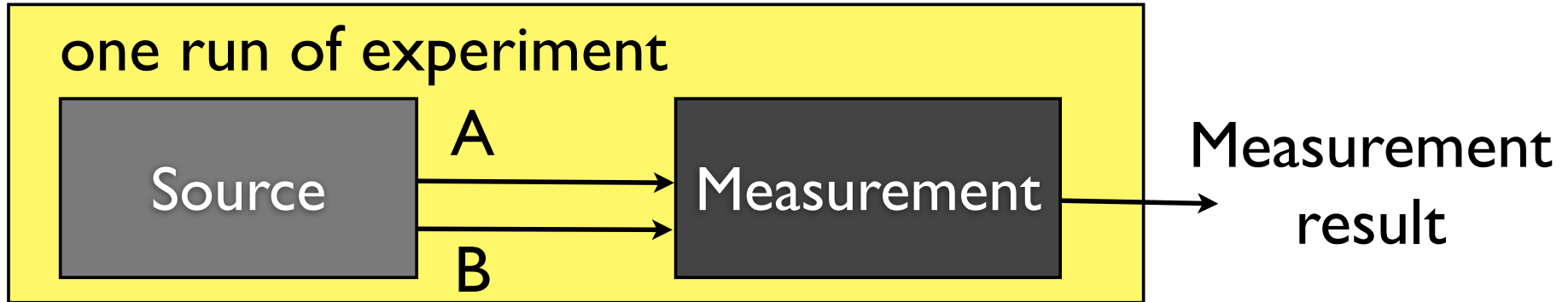
non-classical correlations

The Separability Problem

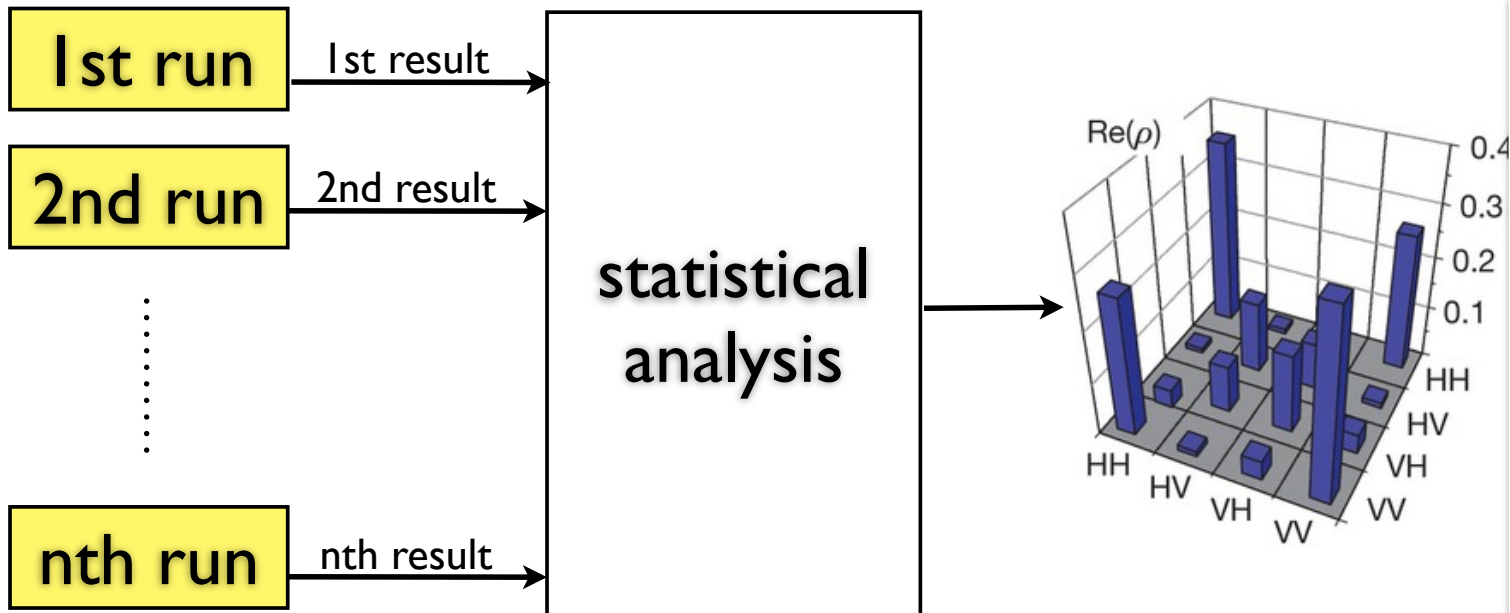
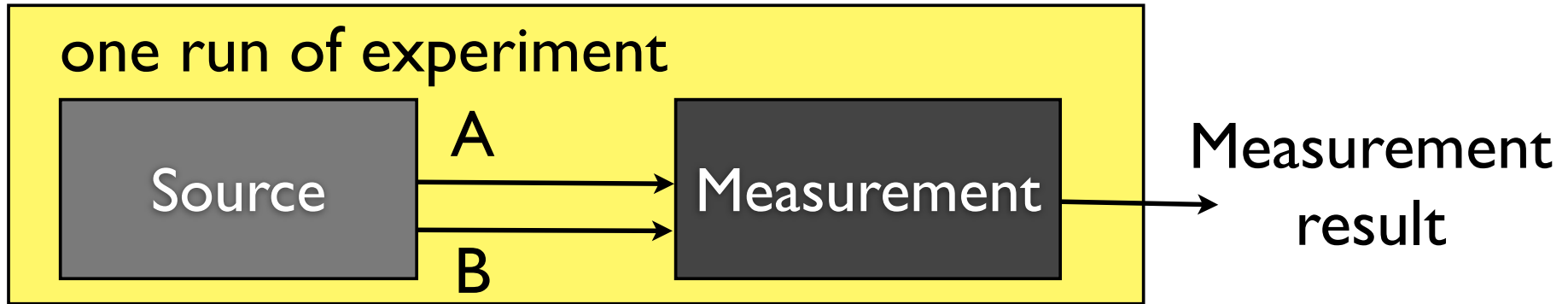
- Given $\rho_{AB} \in D(C^d \otimes C^l)$
is it separable or entangled?
- **(Weak Membership: $W_{\text{SEP}}(\epsilon, ||*||)$)** Given ρ_{AB}
determine if it is separable, or ϵ -way from SEP



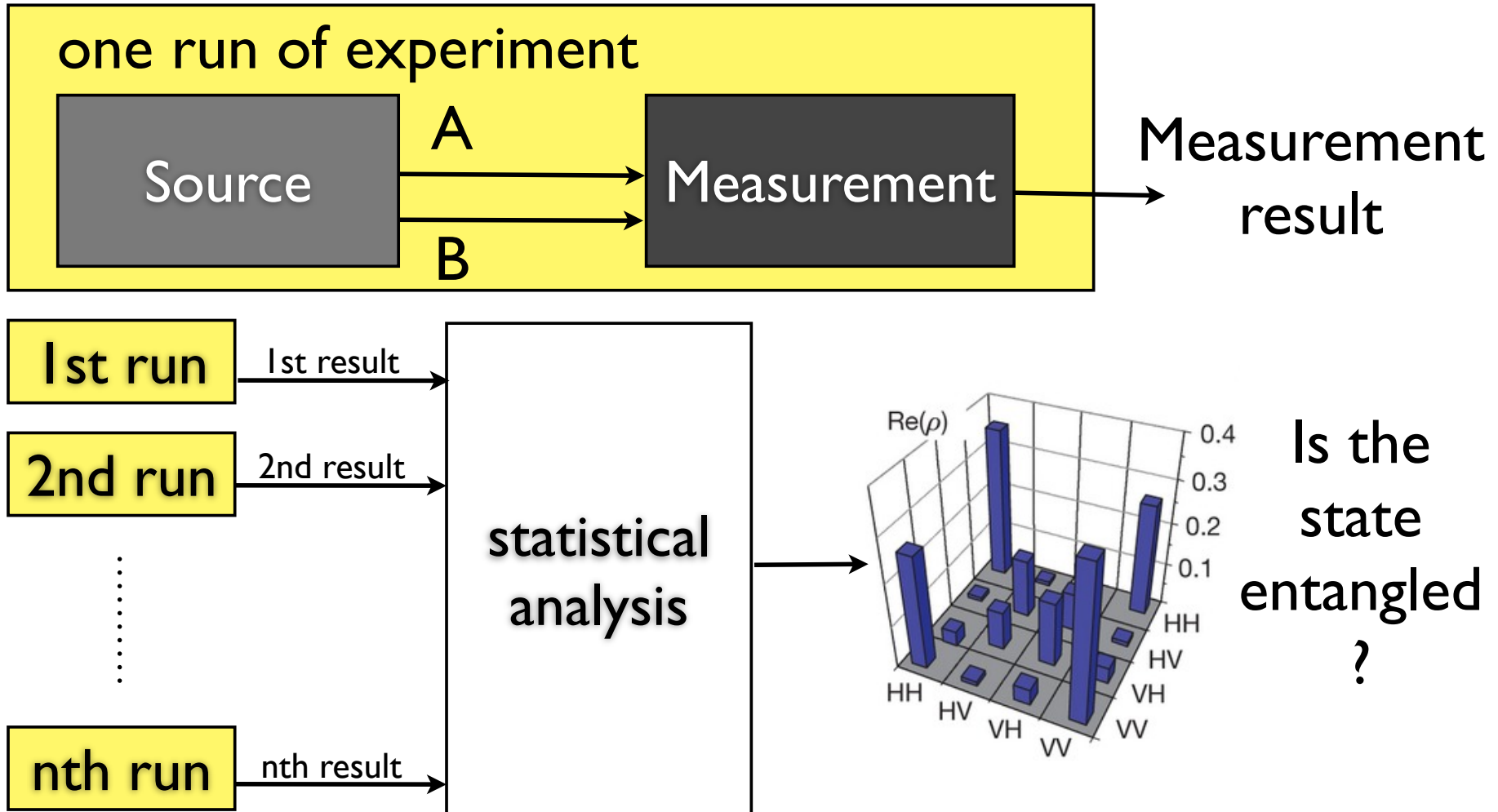
The Problem (for experimentalists)



The Problem (for experimentalists)



The Problem (for experimentalists)



Relevance

- **Quantum Cryptography**
Security only if state is entangled
- **Quantum Communication**
Advantage over classical (e.g. teleportation, dense coding) only if state is entangled
- **Computational Physics**
Entanglement responsible for difficulty of simulation of quantum systems

Deciding Entanglement

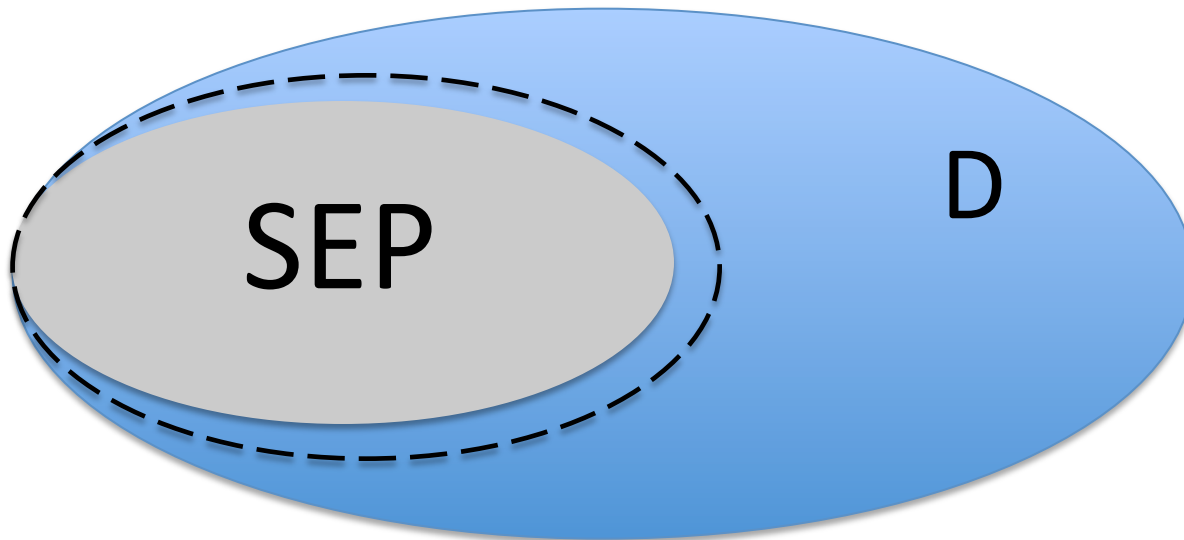
The problem of deciding whether a state is entangled

- has been considered since the early days of the field of quantum information theory
- is regarded as a computationally difficult problem

In this talk I'll discuss the fastest known algorithm for this problem

The Separability Problem (again)

- Given $\rho_{AB} \in D(C^d \otimes C^l)$
is it separable or entangled?
- **(Weak Membership: $W_{\text{SEP}}(\epsilon, ||*||)$)** Given ρ_{AB}
determine if it is separable, or ϵ -way from SEP

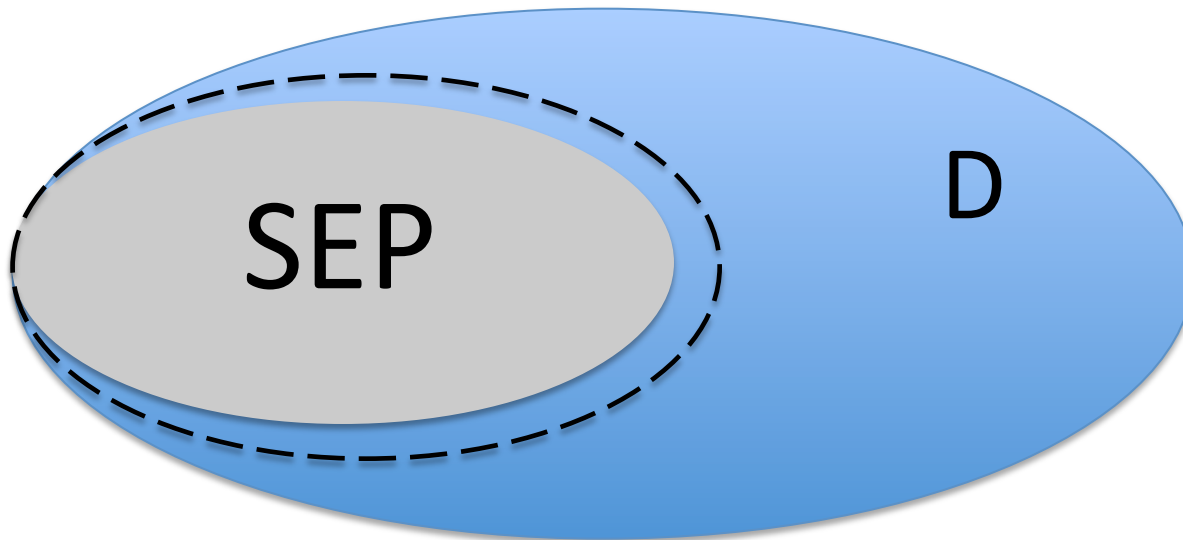


The Separability Problem (again)

- Given $\rho_{AB} \in \mathcal{D}$
is it separable or

Which norm should we use?

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



Norms on Quantum States

How to quantify the distance in Weak-Membership?

- Euclidean Norm (Hilber-Schmidt):

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

- Trace Norm

$$||X||_1 = \text{tr}((X^T X)^{1/2})$$

Obs: $||X||_1 \geq ||X||_2 \geq d^{-1/2} ||X||_1$

The LOCC Norm

- Operational interpretation trace norm:

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

optimal bias of distinguishing the two states by quantum measurements

The LOCC Norm

- Operational interpretation trace norm:

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

optimal bias of distinguishing the two states by quantum measurements

- For ρ_{AB}, σ_{AB} define the LOCC norm

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

Optimal bias of distinguishing two states by LOCC measurements

E.g. (one-way LOCC)
$$M = \sum_k A_k \otimes B_k, \quad \sum_k A_k \leq I, \quad 0 \leq B_k \leq I$$

Optimization Over Separable States

(Best Separable State BSS(ϵ)) Given $M \in H(C^d \otimes C^l)$

estimate

$$\begin{aligned} \max_{\sigma \in SEP} \text{tr}(M\sigma) &= \max_{|\psi\rangle, |\phi\rangle} \langle \psi, \varphi | M | \psi, \varphi \rangle \\ &= \max_{x^T x = y^T y = 1} (x \otimes y)^T M (x \otimes y) \end{aligned}$$

to additive error ϵ

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: $2^{O(|A| \log |B| \log (1/\varepsilon))}$ time complexity

for either $\|\cdot\|_2$ or $\|\cdot\|_1$ norms

(Doherty, Parrilo, Spedalieri '04)

Hardness Results

When is ρ_{AB} entangled?

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

(Gurvits '02) NP-hard with $\varepsilon=1/\exp(|A||B|)$

Hardness Results

When is ρ_{AB} entangled?

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

(Gurvits '02) NP-hard with $\varepsilon=1/\exp(|A||B|)$

(Gharibian '08, Beigi '08) NP-hard with $\varepsilon=1/\text{poly}(|A||B|)$

Hardness Results

When is ρ_{AB} entangled?

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

(Gurvits '02) NP-hard with $\varepsilon=1/\exp(|A||B|)$

(Gharibian '08, Beigi '08) NP-hard with $\varepsilon=1/\text{poly}(|A||B|)$

(Beigi, Shor '08) Favorite separability tests fail

Hardness Results

When is ρ_{AB} entangled?

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

(Gurvits '02) NP-hard with $\varepsilon=1/\exp(|A||B|)$

(Gharibian '08, Beigi '08) NP-hard with $\varepsilon=1/\text{poly}(|A||B|)$

(Beigi, Shor '08) Favorite separability tests fail

(Harrow, Montanaro '10) No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ time algorithm for membership in any convex set within $\varepsilon=\Omega(1)$ trace distance to SEP, and any $\nu+\mu>0$, unless ETH fails

ETH (Exponential Time Hypothesis): SAT cannot be solved in $2^{o(n)}$ time
(Impagliazzo&Paruti '99)

Algorithms for BSS

Estimate $\max_{\sigma \in SEP} tr(M\sigma)$ with additive error ε

State-of-the-art: $2^{O((|A|+|B|)\log(1/\varepsilon))}$ time complexity

Exhaustive search over ε -nets on A and B!

Hardness Results for BSS

Estimate $\max_{\sigma \in SEP} tr(M\sigma)$ with additive error ε

(Gurvits '02, Gharibian '08, Beigi '08) NP-hard with $\varepsilon=1/\text{poly}(|A| |B|)$

(Harrow, Montanaro '10, built on Aaronson *et al* '08) No $\exp(O(\log^{1-\nu} |A| \log^{1-\mu} |B| |M| |\infty)))$ time algorithm for any $\nu+\mu>0$ and constant ε , unless ETH fails

Main Result 1: Weak Membership

(B., Christandl, Yard '10) There is a $\exp(O(\varepsilon^{-2} \log |A| \log |B|))$ time algorithm for $W_{\text{SEP}}(\|\cdot\|, \varepsilon)$ (in $\|\cdot\|_2$ or $\|\cdot\|_{\text{LOCC}}$)

Main Result 1: Weak Membership

(B., Christandl, Yard '10) There is a $\exp(O(\varepsilon^{-2} \log |A| \log |B|))$ time algorithm for $W_{\text{SEP}}(\|\cdot\|, \varepsilon)$ (in $\|\cdot\|_2$ or $\|\cdot\|_{\text{LOCC}}$)

Remind: NP-hard for $\varepsilon = 1/\text{poly}(|A| |B|)$ in $\|\cdot\|_2$
(Gurvits '02, Gharibian '08, Beigi '08)

Corollary: the problem in $\|\cdot\|_2$ is not NP-hard
for $\varepsilon = 1/\text{polylog}(|A| |B|)$, unless ETH fails

Main Result 2: Best Separable State

(BCY '10)

1. There is a $\exp(O(\epsilon^{-2} \log |A| \log |B| (\|M\|_2)^2))$ time algorithm for BSS(ϵ)
2. For M in LOCC, there is a $\exp(O(\epsilon^{-2} \log |A| \log |B|))$ time algorithm for BSS(ϵ)

Main Result 2: Best Separable State

(BCY '10)

1. There is a $\exp(O(\varepsilon^{-2} \log |A| \log |B| (||M||_2)^2))$ time algorithm for BSS(ε)
2. For M in LOCC, there is a $\exp(O(\varepsilon^{-2} \log |A| \log |B|))$ time algorithm for BSS(ε)

Contrast with:

(Harrow, Montanaro '10) No $\exp(O(\log^{1-\nu} |A| \log^{1-\mu} |B| ||M||_\infty))$ time algorithm for any $\nu + \mu > 0$ and constant ε , unless ETH fails, even for

separable M: $M = \sum_k A_k \otimes B_k$, $0 \leq M \leq I$.

Remember: Part 2 works for $M = \sum_k A_k \otimes B_k$, $\sum_k A_k \leq I$, $0 \leq B_k \leq I$

Main Result 2: Best Separable State

(E) **Quantum Info Remark:**

- 1 The difficulty to show optimality of the algorithm is the existence of separable measurements that are *not* LOCC,
- 2 a well studied phenomena in quantum information (e.g. [Bennett et al '98](#)). Here we have a new computational-complexity motivation for further studying the problem!

Contrast with:

(Harrow, Montanaro '10) **No $\exp(O(\log^{1-\nu} |A| |M|))$ time algorithm for any $\nu + \mu > 0$ and constant ϵ , unless P vs BPP fails, even for**

separable M : $M = \sum_k A_k \otimes B_k, 0 \leq M \leq I.$

Remember: Part 2 works for $M = \sum_k A_k \otimes B_k, \sum_k A_k \leq I, 0 \leq B_k \leq I$

The Algorithm

- We consider the a Parrilo-Lasserre hierarchy of SDP relaxations to the problem introduced in (Doherty, Parrilo and Spedalieri '01)
- We prove it converges to a good approximate solution in a $O(\log |B|)$ number of rounds. Previously convergence only in $\Omega(|B|)$ rounds was known.

Optimization Over Separable States (again)

(Best Separable State BSS(ϵ)) Given $M \in H(C^d \otimes C^l)$
estimate

$$\begin{aligned} \max_{\sigma \in SEP} \text{tr}(M\sigma) &= \max_{|\psi\rangle, |\phi\rangle} \langle \psi, \varphi | M | \psi, \varphi \rangle \\ &= \max_{x^T x = y^T y = 1} (x \otimes y)^T M (x \otimes y) \end{aligned}$$

to additive error ϵ

This is a polynomial optimization problem. One can calculate a sequence of SDP approximations to it following the approach of (Parrilo '00, Lasserre '01)

We'll derive the SDP hierarchy by a *quantum* argument

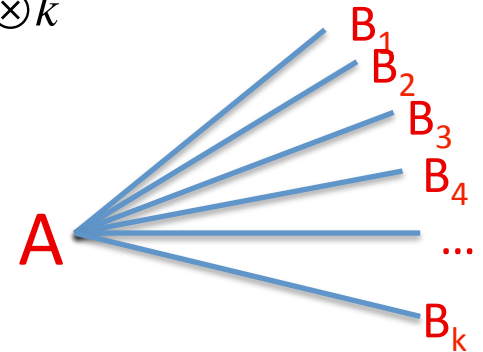
Entanglement Monogamy

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*

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



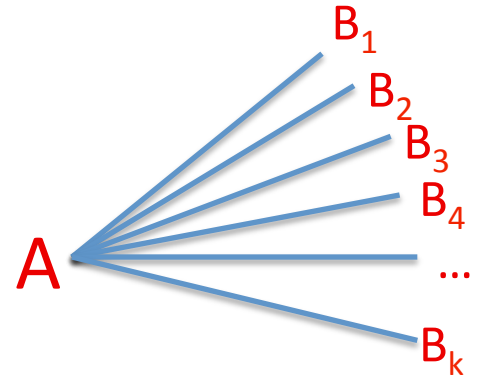
Def. ρ_{AB} is *k*-extendible if there is $\rho_{AB_1 \dots B_k}$
s.t for all j in $[k]$, $\text{tr}_{\setminus B_j}(\rho_{AB_1 \dots B_k}) = \rho_{AB}$

Entanglement Monogamy

Classical correlations are shareable:

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

Def. ρ_{AB} is *k*-extendible if there is $\rho_{AB_1 \dots B_k}$
s.t for all j in $[k]$, $\text{tr}_{\setminus B_j}(\rho_{AB_1 \dots B_k}) = \rho_{AB}$



Separable states are k-extendible for every k

Entanglement Monogamy

Quantum correlations are non-shareable:

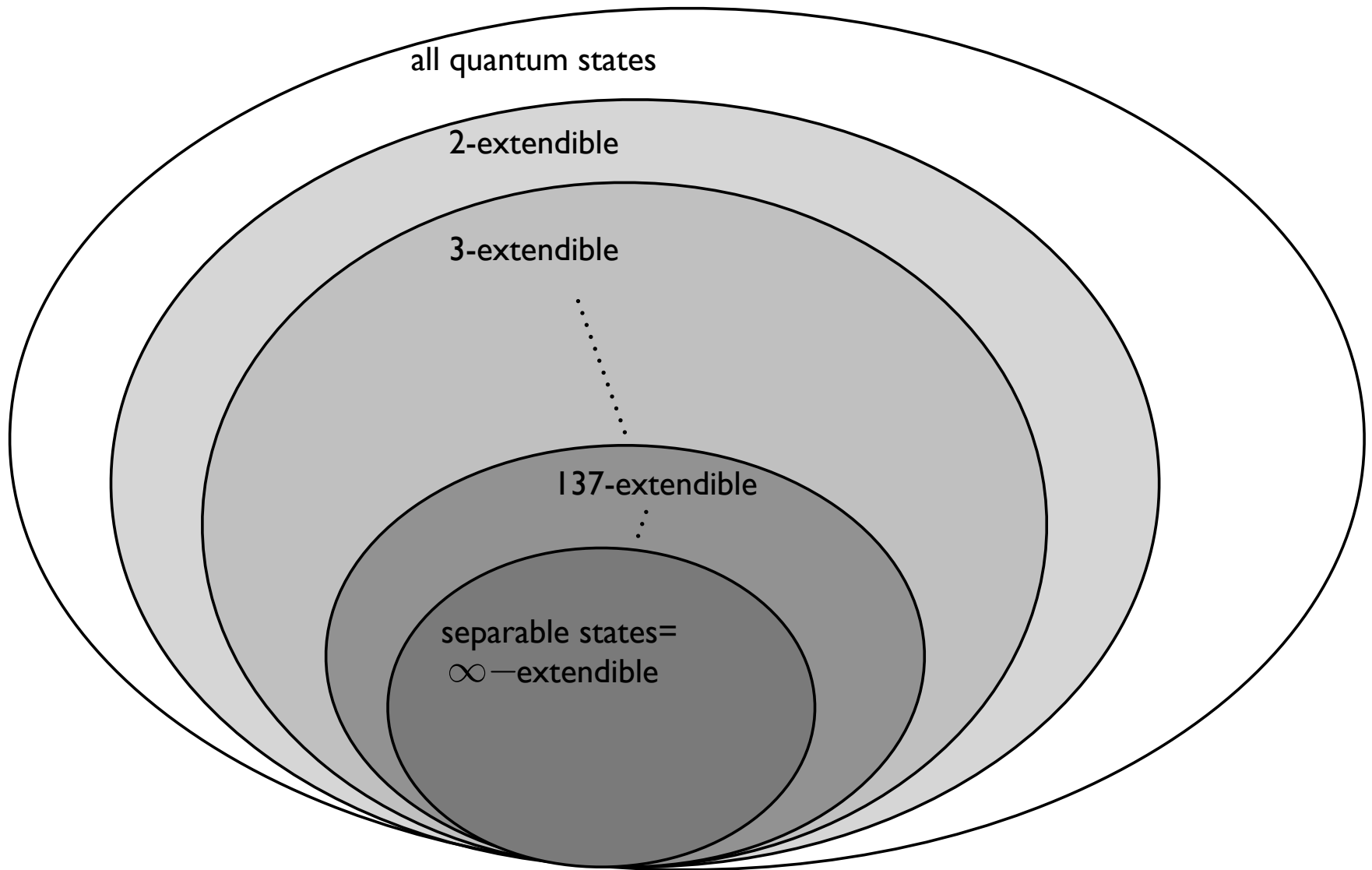
ρ_{AB} separable **iff** ρ_{AB} k -extendible for all k

Follows from: Quantum de Finetti Theorem

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

Monogamy of entanglement:

Very useful concept in general, application e.g. in quantum key distribution



⇒ 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?

Entanglement Monogamy

Quantitative version: For any k -extendible ρ_{AB} ,

$$\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \leq O\left(\frac{|B|^2}{k}\right)$$

- Follows from: **Finite quantum de Finetti Theorem**
(Christandl, König, Mitchson, Renner '05)

Entanglement Monogamy

Quantitative version: For any k -extendible ρ_{AB} ,

$$\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \leq O\left(\frac{|B|^2}{k}\right)$$

- Follows from: **Finite quantum de Finetti Theorem**
(Christandl, König, Mitchson, Renner '05)

Close to optimal:

there is a k -ext state ρ_{AB} s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$

For **other norms** ($\|\cdot\|_2, \|\cdot\|_{LOCC}, \dots$) no better bound known.

Exponentially Improved de Finetti type bound

(B., Christandl, Yard '10) For any k -extendible ρ_{AB} , with $\|\cdot\|^*$ equals $\|\cdot\|_2$ or $\|\cdot\|_{\text{LOCC}}$

$$\min_{\sigma \in \text{SEP}} \|\rho - \sigma\| \leq O\left(\frac{\log |A|}{k}\right)^{\frac{1}{2}}$$

Bound proportional to the (square root) of the **number of qubits**: exponential improvement over previous bound

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

- Search for a symmetric extension is a semidefinite program (Doherty, Parrilo, Spedalieri '04)

$$\exists \pi_{AB_1, \dots, B_k} \geq 0 : \pi_{AB_j} = \rho_{AB} \quad \forall j \in [k]$$

- Can be solved in $\text{poly}(n)$ time in the number of variables n
- $n = |A|^2 |B|^{2k}$
- Our bound implies $k = O(\epsilon^{-2} \log |A|)$
- Time Complexity:
 $\text{poly}(|A| |B|^{2k}) = \exp(O(\epsilon^{-2} \log |A| \log |B|))$

Does it work for 1-norm?

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

Does it work for 1-norm?

- There are k -extendible states s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$
- For such states the SDP hierarchy only gives good solutions for $k = O(|B|)$, which requires exponential time

Does it work for 1-norm?

- There are k -extendible states s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$
- For such states the SDP hierarchy only gives good solutions for $k = O(|B|)$, which requires exponential time
- But we know also: $\min_{\sigma \in SEP} \|\rho - \sigma\|_{LOCC} \leq O\left(\frac{\log|A|}{k}\right)^{\frac{1}{2}}$

Does it work for 1-norm?

- There are **k-extendible** states s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$
- For such states **the SDP hierarchy** only gives good solutions for $k = O(|B|)$, which requires **exponential time**
- **But we know** also: $\min_{\sigma \in SEP} \|\rho - \sigma\|_{LOCC} \leq O\left(\frac{\log|A|}{k}\right)^{\frac{1}{2}}$
- So, **hard instances** are always “**data hiding**” states, i.e.

$$\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \gg \min_{\sigma \in SEP} \|\rho - \sigma\|_{LOCC}$$

Algorithm for Best Separable State

The idea Optimize over $k=O(\log |A| \epsilon^{-2} (\|X\|_2)^2)$ extension of ρ_{AB} by SDP

$$\max_{\pi} \text{tr}(\pi_{AB_1} X) : \pi_{AB_1, \dots, B_k} \geq 0, \quad \pi_{AB_j} = \pi_{AB_1} \quad \forall j \in [k]$$

This is precisely the Parrilo-Lasserre hierarchy for the problem!
(written in a somewhat different form)

By Cauchy Schwartz: $|\text{tr}(X(\rho - \sigma))| \leq \|\rho - \sigma\|_2 \|X\|_2$

By de Finetti Bound:

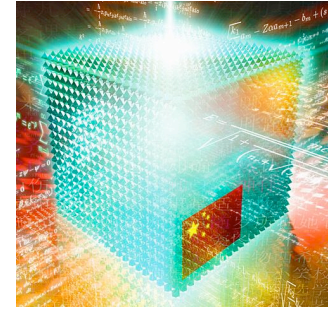
$$\max_{\pi \in k\text{-Ext}} \text{tr}(\pi X) \geq \max_{\sigma \in \text{SEP}} \text{tr}(\sigma X) \geq \max_{\pi \in k\text{-Ext}} \text{tr}(\pi X) - \|X\|_2 \sqrt{O(k^{-1} \log |A|)}$$

Application 1: Quantum NP

QMA



$|\Psi\rangle$



**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 $> 1/3$

QMA

- Quantum analogue of NP (or MA)
- Local Hamiltonian Problem, N-representability, ...

Is QMA a robust complexity class?

(Aharonov, Regev '03) superverifiers don't help

(Marriott, Watrous '05) Exponential amplification with fixed proof size

(Beigi, Shor, Watrous '09) logarithmic size interaction doesn't help

New Characterization QMA

Corollary QMA doesn't change allowing $k = O(1)$ different proofs if the verifier can only apply LOCC measurements in the k proofs

New Characterization QMA

Corollary QMA doesn't change allowing $k = O(1)$ different proofs if the verifier can only apply LOCC measurements in the k proofs

Def $\text{QMA}_m(k)$: analogue of QMA with k proofs and proof size m

New Characterization QMA

Corollary QMA doesn't change allowing $k = O(1)$ different proofs if the verifier can only apply **LOCC measurements** in the k proofs

Def $\text{QMA}_m(k)$: analogue of QMA with k proofs and proof size m

Def $\text{LOCCQMA}_m(k)$: analogue of QMA with k proofs, proof size m and **LOCC verification** procedure along the k proofs.

QMA(k)

Def $\text{QMA}_m(k)$: A language L is in $\text{QMA}_m(k)$ if there is a quantum poly-time circuit that for every instance x implements the measurement $\{A_x, I - A_x\}$ such that

- **Completeness:** If x in L , there exists k proofs, each of m qubits, s.t.

$$\text{tr}(A_x (|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes \dots \otimes |\psi_k\rangle\langle\psi_k|)) \geq 2/3$$

- **Soundness:** If x not in L , for any k states,

$$\text{tr}(A_x (|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes \dots \otimes |\psi_k\rangle\langle\psi_k|)) \leq 1/3$$

Def 2 $\text{LOCCQMA}_m(k)$: Likewise, but $\{A_x, I - A_x\}$ must be **LOCC**

New Characterization QMA

Corollary $\text{QMA} = \text{LOCCQMA}(k), k = O(1)$

$\text{LOCCQMA}_m(2)$ contained in $\text{QMA}_{O(m^2)}$

New Characterization QMA

Corollary $\text{QMA} = \text{LOCCQMA}(k), k = O(1)$

$\text{LOCCQMA}_m(2)$ contained in $\text{QMA}_{O(m^2)}$

Contrast: $\text{QMA}_m(2)$ not in $\text{QMA}_{O(m^{2-\delta})}$

for any $\delta > 0$ unless Quantum ETH* fails

Follows from $\text{QMA}_{n^{1/2}}(2)$ protocol for SAT with n clauses

(Harrow and Montanaro '10 – built on Aaronson et al '08)

And: SAT has a $\text{LOCCQMA}_{O(\log(n))}(n^{1/2})$ protocol

(Chen and Drucker '10)

* Quantum ETH: SAT cannot be solved in $2^{o(n)}$ quantum time

New Characterization QMA

Corollary $\text{QMA} = \text{LOCCQMA}(k), k = O(1)$

$\text{LOCCQMA}_m(2)$ contained in $\text{QMA}_{O(m^2)}$

Idea to simulate $\text{LOCCQMA}_m(2)$ in QMA:

- Arthur asks for proof ρ on $AB_1B_2\dots B_k$ with $k = m\varepsilon^{-2}$
- He **symmetrizes** the B systems and applies the original verification procedure to AB_1

Correctness

de Finetti bound implies: $\min_{\sigma \in \text{SEP}} \left\| \rho_{AB_1} - \sigma \right\|_{\text{LOCC}} \leq \sqrt{\frac{m}{k}} = \varepsilon$

Application 2: Small Set Expansion

Small Set Expansion Problem: Given a graph determine whether all sets of sublinear size expand almost perfectly.

Introduced in (Raghavendra, Steurer '09), where it was conjectured to be a hard problem. It's closely related to Khot's Unique Games Conjecture

Application 2: Small Set Expansion

Small Set Expansion Problem: Given a graph determine whether all sets of sublinear size expand almost perfectly.

Introduced in (Raghavendra, Steurer '09), where it was conjectured to be a hard problem. It's closely related to Khot's Unique Games Conjecture

- (Barak, B., Harrow, Kelner, Steurer, and Zhou '12) connection of the Small Set Expansion Problem to the Best-Separable-State Problem for a LOCC operator (via the 2- \rightarrow 4 norm of a projector)
- Can show that the SDP hierarchy gives a subexponential-time algorithm for the small set expansion problem, matching the performance of the algorithm of (Arora, Barak and Steurer '10)

Proof Techniques

k-extendible

$$\min_{\sigma_{AB} \text{ separable}} \|\rho_{AB} - \sigma_{AB}\| \leq \text{const.} \sqrt{\frac{\log |A|}{k}}$$

- Coding Theory

Strong subadditivity of von Neumann entropy as state redistribution rate

(Devetak, Yard '06)

- Large Deviation Theory

Hypothesis testing of separable states

(B., Plenio '08)

- Entanglement Measure Theory

Squashed Entanglement

(Christandl, Winter '04)

$I(A:B | E)$

Conditional Mutual Information: Measures the correlations of **A** and **B** relative to **E** in ρ_{ABE}

$$I(A:B | E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$$

Always positive: $I(A:B | E)_\rho \geq 0$ (strong-subadditivity of entropy)

(Lieb, Ruskai '73)

When does it vanish?

$I(A:B | E)_\rho = 0$ **iff** ρ_{ABE} is a “**Quantum Markov Chain State**”

(Hayden, Jozsa, Petz, Winter '04)

E.g.
$$\rho_{ABE} = \sum_k p_k \rho_k^A \otimes \sigma_k^B \otimes |k\rangle^E \langle k|$$

Approximate version??? ...

New Inequality for $I(A:B|E)$

Thm: (B., Christandl, Yard '10)

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

- Either LOCC or 2-norm
- Obs: The statement fails badly for 1-norm!
- The monogamy bound follows from this inequality and the chain rule (via an entanglement measure called squashed entanglement)

Summary

- Testing **separability** is rather **easy**
- Family of Parrilo-Lasserre SDP relaxations converge in $\log(n)$ rounds; proof by a *quantum* argument – new approach to proving fast convergence of SDP hierarchies.
- New Pinsker type **lower bound** for $I(A:B|E)$
- **QMA** is **robust**

Open Problems

- Is there a **polynomial** algorithm in **2-norm**?
- Can we **close** the **LOCC norm vs. trace norm gap** in the results?
(hardness vs. algorithm, LOCCQMA(k) vs QMA(k))
- Are there **more applications** of the bound on the convergence of the **SDP relaxation**? Can we prove a quasipolynomial time algorithm for Small set Expansion? And for unique games or other UG-hard problems?
- Can we put new problems in QMA using $QMA = LOCCQMA(k)$?
- Are there **more application** of the inequality for $I(A:B | E)$?

Thank you!

Proof Outline

Relative Entropy of Entanglement

The proof is largely based on the properties of the following *entanglement measure*:

Def Relative Entropy of Entanglement (Vedral, Plenio '99)

$$E_R^\infty(\rho_{AB}) := \lim_{n \rightarrow \infty} \frac{E_R(\rho_{AB}^{\otimes n})}{n} \quad E_R(\rho_{AB}) := \min_{\sigma \in SEP} S(\rho \parallel \sigma)$$

$$S(\rho \parallel \sigma) := \text{tr}(\rho(\log \rho - \log \sigma))$$

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB} , what's the optimal probability of distinguishing it from a separable state?

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB} , what's the optimal probability of distinguishing it from a separable state?

Def Rate Function: $D(\rho_{AB})$ is maximum number r s.t. there exists $\{M_n, I-M_n\}$, $0 < M_n < I$,

$$\min_{\sigma \in SEP} \text{tr}(M_n \sigma) \leq 2^{-nr}, \quad \text{tr}(M \rho_{AB}^{\otimes n}) \geq \Omega(1)$$

$D_{LOCC}(\rho_{AB})$: defined analogously, but now $\{M, I-M\}$ must be LOCC

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB} , what's the optimal probability of distinguishing it from a separable state?

Def Rate Function: $D(\rho_{AB})$ is maximum number r s.t there exists $\{M_n, I-M_n\}$, $0 < M_n < I$,

$$\min_{\sigma \in SEP} tr(M_n \sigma) \leq 2^{-nr}, \quad tr(M \rho_{AB}^{\otimes n}) \geq \Omega(1)$$

$D_{LOCC}(\rho_{AB})$: defined analogously, but now $\{M, I-M\}$ must be LOCC

(B., Plenio '08) $D(\rho_{AB}) = E_R^\infty(\rho_{AB})$

Obs: Equivalent to reversibility of entanglement under non-entangling operations (B., Plenio '08)

Proof in 1 Line

$$I(A : B | E)_{\rho_{ABE}} \stackrel{(i)}{\geq} E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \stackrel{(ii)}{\geq} D_{LOCC}(\rho_{A:B}) \stackrel{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \|\rho_{A:B} - \sigma\|_{LOCC}^2\right)$$

Proof in 1 Line

$$I(A : B | E)_{\rho_{ABE}} \stackrel{(i)}{\geq} E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \stackrel{(ii)}{\geq} D_{LOCC}(\rho_{A:B}) \stackrel{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \|\rho_{A:B} - \sigma\|_{LOCC}^2\right)$$

Relative entropy of Entanglement plays a triple role:

- (i) **Quantum Shannon Theory:** State redistribution Protocol
(Devetak and Yard '07)
- (ii) **Large Deviation Theory:** Entanglement Hypothesis Testing
(B. and Plenio '08)
- (iii) **Entanglement Theory:** Faithfulness bounds

First Inequality

$$I(A : B | E)_{\rho_{ABE}} \stackrel{(i)}{\geq} E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E})$$

Non-lockability: $E_R(\rho_{A:BE}) \leq E_R(\rho_{A:E}) + 2 \log |B|$
(Horodecki³ and Oppenheim '04)

State Redistribution: How much does it cost to redistribute a quantum system? $\frac{1}{2} I(A:B | E)$

$$\text{A} \mid \text{BE} \mid \text{F} \longrightarrow \text{A} \mid \text{E} \mid \text{BF} \quad \left| \psi \right\rangle_{\text{A:BE:F}}^{\otimes n} \longrightarrow \left| \psi \right\rangle_{\text{A:E:BF}}^{\otimes n}$$

Proof (i):

Apply **non-lockability** to $\rho_{A:BE}^{\otimes n}$ and use **state redistribution** to trace out B at a rate of $\frac{1}{2} I(A:B | E)$ qubits per copy

Second Inequality

$$E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \stackrel{(ii)}{\geq} D_{LOCC}(\rho_{A:B})$$

Equivalent to: $D(\rho_{A:BE}) \geq D(\rho_{A:E}) + D_{LOCC}(\rho_{A:B})$

Monogamy relation for entanglement hypothesis testing

Proof (ii)

Use **optimal measurements** for ρ_{AE} and ρ_{AB} achieving $D(\rho_{AE})$ and $D_{LOCC}(\rho_{AB})$, resp., to **construct a measurement** for $\rho_{A:BE}$ achieving $D(\rho_{A:BE})$

Third Inequality

$$D_{LOCC}(\rho_{A:B}) \stackrel{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \|\rho_{A:B} - \sigma\|_{LOCC}^2\right)$$

Pinsker type inequality for entanglement hypothesis testing

Proof (iii)

minimax theorem + **martingale like property** of the set of separable states

Thank you!