Title: Quantum Data Hiding: Challenges and Opportunities

Date: Nov 02, 2011 11:00 AM

URL: http://pirsa.org/11110109

Abstract: Correlations in quantum states are sometimes inaccessible if only restricted types of quantum measurements can be performed, an effect known as quantum data hiding. For example highly entangled states shared by two parties might appear uncorrelated if the parties can only measure locally their shares of the state and communicate classically with each other.

In this talk I will first discuss how a better understanding of the peculiar type of correlations found in quantum data hiding states is useful in addressing two challenges of quantum information theory: the design of efficient algorithms for determining if a quantum state is entangled, and the establishment of area laws in gapped local Hamiltonians.

Second, I will present new efficient ways of generating data hiding, e.g. employing random local quantum circuits, and will briefly discuss the relevance of this approach to the problem of proving quick equilibration of quantum systems unitarily interacting with a large environment.

Quantum Data Hiding

Challenges and Opportunities

Fernando G.S.L. Brandão

Universidade Federal de Minas Gerais, Brazil

Based on joint work with

M. Christandl, A. Harrow, M. Horodecki, J. Yard

PI, 02/11/2011

Outline

- **Data Hiding**
  From LOCC
  Other Examples
- **Determining Entanglement**
  Data Hiding States are the Hardest Instances
- **Computational Data Hiding**
  Random Quantum Circuits are Unitary Poly-Designs
- **Area Law in Gapped Models**
  The Guessing Probability Decay of Correlations

Data Hiding

P_{sym}, P_{asym}: projectors onto symmetric and antisymmetric subspaces of $C^d \otimes C^d$.

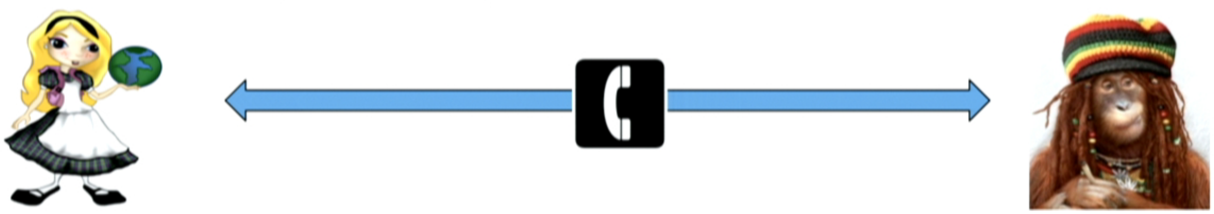
Define $w_- := P_{sym}/\dim(P_{sym})$, $w_+ := P_{asym}/\dim(P_{asym})$.
States are orthogonal, hence perfectly distinguishable.

How about under LOCC measurements?
They cannot be distinguished with probability > ½+1/d

(Eggeling, Werner '02)

They are data hiding against LOCC.

LOCC: Local quantum Operations and Classical Communication



The LOCC Norm

Trace norm:

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

optimal bias of distinguishing two states by a quantum measurement

LOCC norm

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

We have $\frac{1}{2} ||w_+ - w_-||_1 = 1,$

$\frac{1}{2} ||w_+ - w_-||_{LOCC} < 1/d$

Data Hiding

(Shor '95, Steane '96, …) Error Correcting Codes

(Wen et al '89, …) Topological Order

(Cleve et al '99) Quantum secret sharing schemes

(Leung et al '01) Hiding bits in quantum states

(Hayden et al '04) Generic states are data hiding

(Horodecki, Oppenheim '04) Big gap of key versus distillable entanglement

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

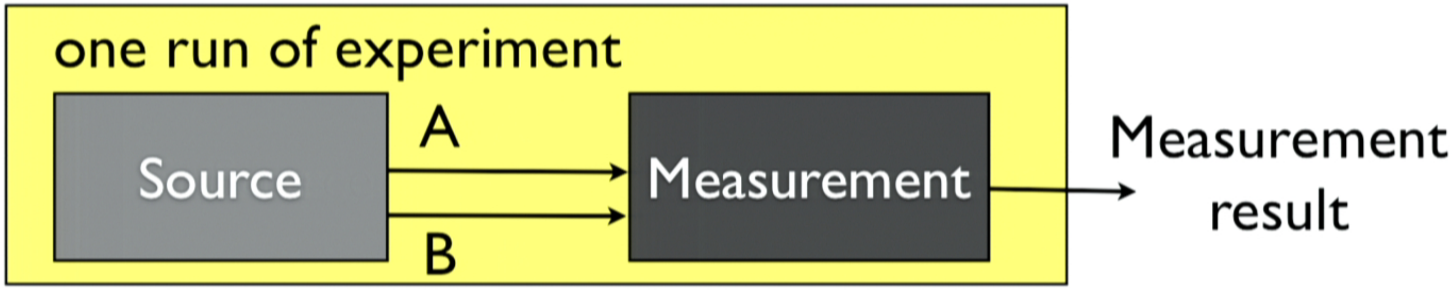
otherwise, it's entangled.

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

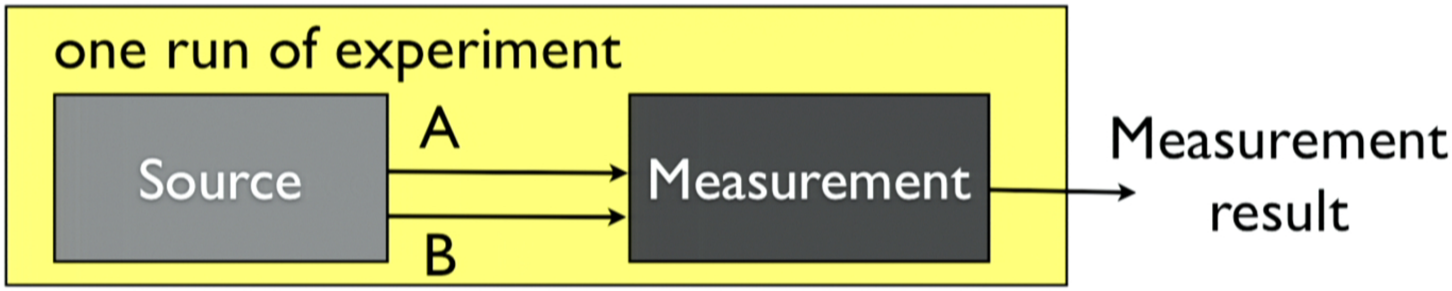
If $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$, it's separable

otherwise, it's entangled.

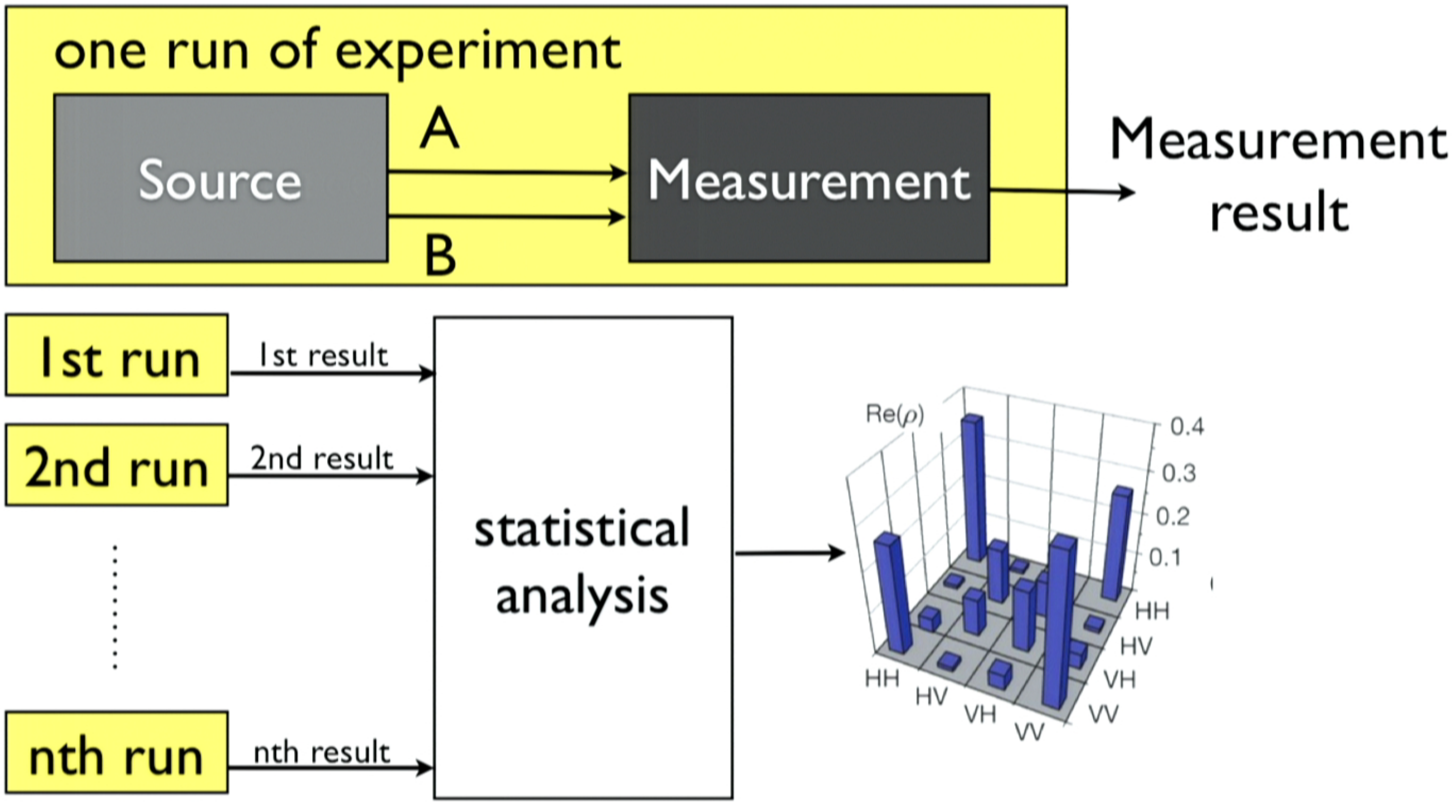
The problem


one run of experiment
Source
A
B
Measurement
Measurement
result

The problem


one run of experiment
Source
A
B
Measurement
Measurement result

The problem

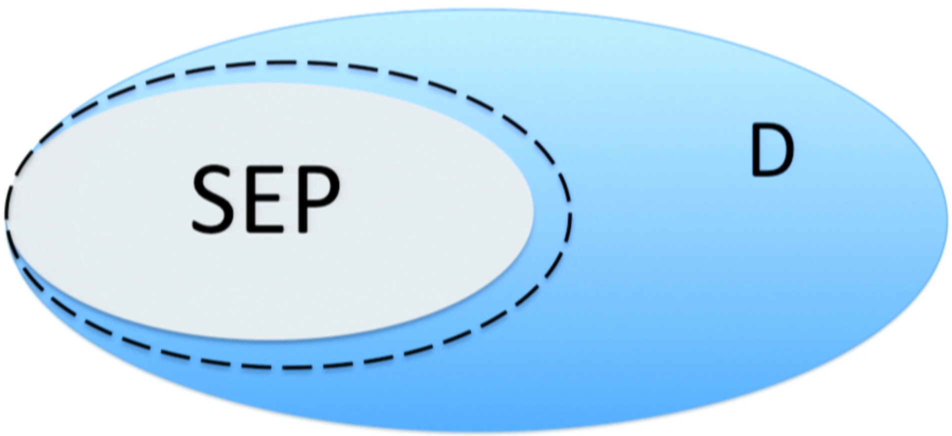


one run of experiment
Source
A
B
Measurement
Measurement
result
1st run
1st result
2nd run
2nd result
nth run
nth result
statistical
analysis
Re(ρ)
0.4
0.3
0.2
0.1
HH
HV
VH
VV
HH
HV
VH
VV

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-way from SEP



Relevance

- Quantum Cryptography
  Security only if state is entangled

- Quantum Communication
  Advantage over classical (e.g. teleportation, dense coding) only if state is entangled

- Quantum Many-body Theory
  Best Separable State problem: compute ground state energy of mean-field Hamiltonians

The separability problem

When is ρ_{AB} entangled?

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

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

Horribly expensive algorithms

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

(Doherty, Parrilo, Spedalieri ‘04)

The separability problem

When is ρ_{AB} entangled?

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

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

Horribly expensive algorithms

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

(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 $\varepsilon=1/\exp(|A||B|)$

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

(Harrow, Montanaro '10) No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ time algorithm for $||*||_1$, with $\nu + \mu > 0$
(unless there is a subexponential algorithm for SAT)

A Faster Algorithm

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

Compare (Harrow, Montanaro '10)
No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ algorithm for $W_{SEP}(||*||_1, \varepsilon)$,
with $\nu + \mu > 0$ and constant ε.

I.e. a similar algorithm in trace norm would be optimal

A Faster Algorithm

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

Compare (Harrow, Montanaro '10)
No $\exp(O(\log^{1-\nu}|A|\log^{1-\mu}|B|))$ algorithm for $W_{SEP}(||*||_1, \varepsilon)$, with $\nu + \mu > 0$ and constant ε.

I.e. a similar algorithm in trace norm would be optimal

Entanglement Monogamy

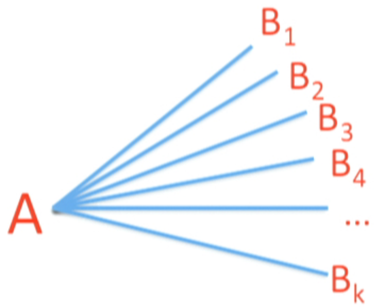
Classical correlations are shareable:

$$\sigma_{AB_1,\ldots,B_k} = \sum_j p_j \sigma_{A,j} \otimes \sigma_{B,j}$$

Entanglement Monogamy

Classical correlations are shareable:

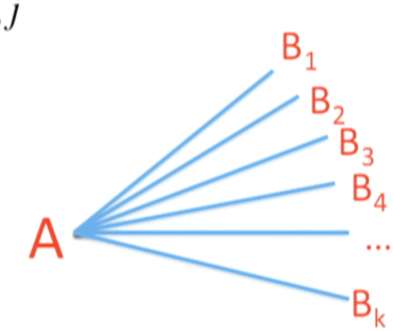
$$\sigma_{AB_1,\ldots,B_k} = \sum_j p_j \sigma_{A,j} \otimes \sigma_{B,j}^{\otimes k}$$



Entanglement Monogamy

Classical correlations are shareable:

$$\sigma_{AB_1,\dots,B_k} = \sum_j p_j \sigma_{A,j} \otimes \sigma_{B,j}^{\otimes k}$$



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

- Separable states are k-extendible for every k

Entanglement Monogamy

Quantum correlations are non-shareable:

ρ_{AB} entangled iff ρ_{AB} not k-extendible for *some* k

Follows from:

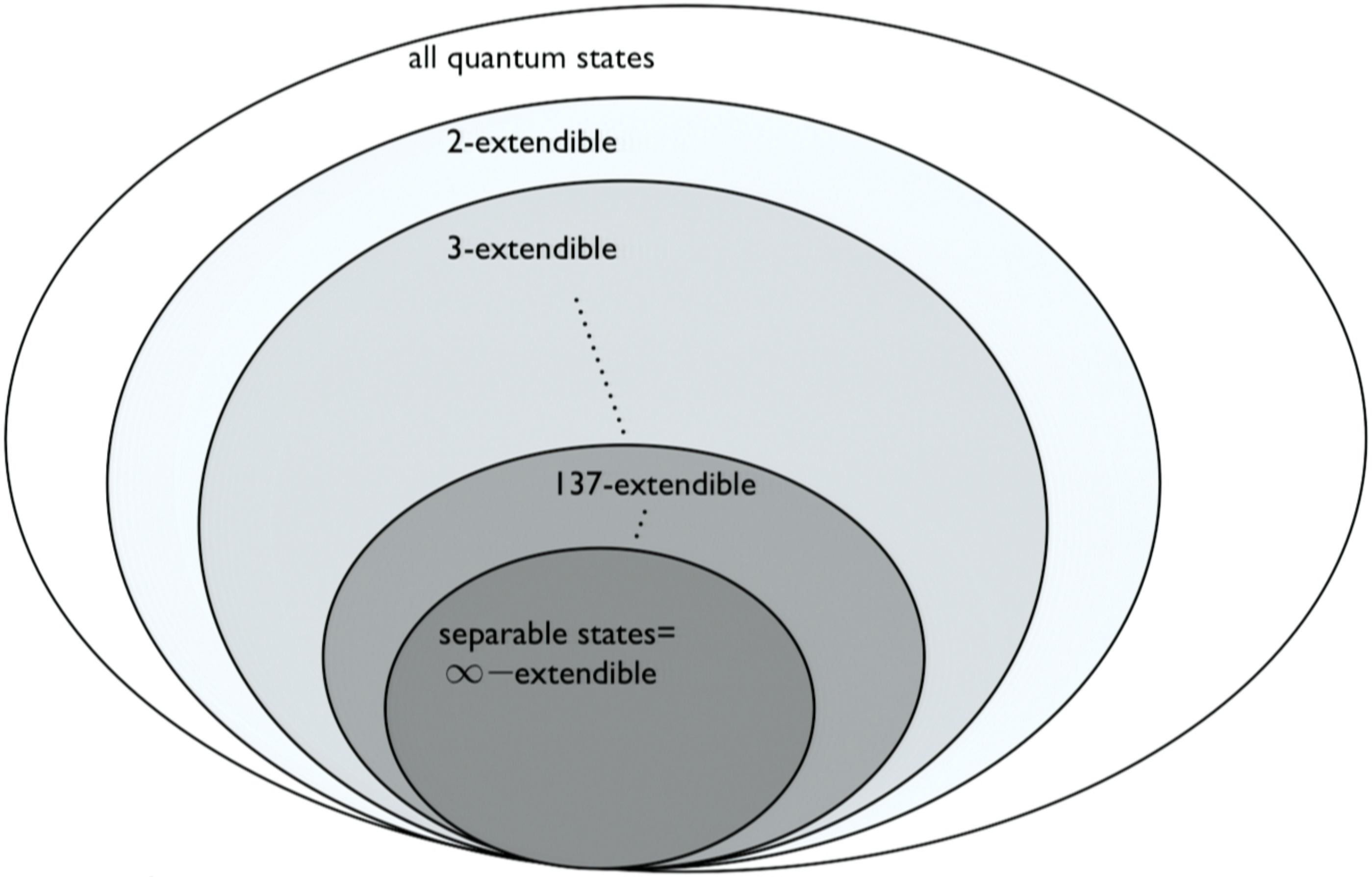
Quantum de Finetti Theorem

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

E.g. Any pure entangled state is not 2-extendible

The *d x d* antisymmetric state is not *d*-extendible

(but is (d-1)-extendible…)



$\Rightarrow$ 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 $\rho_{AB,}$

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

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

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

Guess what? ☺

Entanglement Monogamy

Quantitative version: For any *k*-extendible $\rho_{AB,}$

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

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

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

Guess what? ☺

Exponentially Improved Monogamy

(B. Christandl, Yard '11) For any *k*-extendible ρ_{AB},

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

Bound proportional to the (square root) of # qubits

Highly extendible entangled states *must* be data hiding

Algorithm follows by searching for a $(O(\log|A|/\varepsilon^2))$-symmetric extension by Semidefinite Programming

(SDP with $|A||B|^{O(\log|A|/\varepsilon 2)}$ variables - the dimension of the k-extension)

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 entangled states (B., Plenio '08)

- Entanglement Measure Theory
  Squashed Entanglement (Christandl, Winter '04)

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 entangled states (B., Plenio '08)
- Entanglement Measure Theory
  Squashed Entanglement (Christandl, Winter '04)

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 entangled states (B., Plenio '08)

- Entanglement Measure Theory
  Squashed Entanglement (Christandl, Winter '04)

Computational Data Hiding

"Most quantum states look maximally mixed for all polynomial sized circuits"

Most with respect to the Haar measure: We choose the state as $U|0^n\rangle$, for a random Haar distributed unitary U in $U(2^n)$

I.e. For every integrable function in **U**(d) and every V in **U**(d)

$$E_{U \sim \text{Haar}} f(U) = E_{U \sim \text{Haar}} f(VU)$$

Computational Data Hiding

"Most quantum states look maximally mixed for all polynomial sized circuits"

e.g. most quantum states are useless for measurement based quantum computation (Gross et al '08, Bremner et al '08)

Let QC(k) be the set of 2-outcome POVM {A, I-A} that can be implemented by a circuit with *k* gates

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

Proof by Levy's Lemma + eps-net on the set of poly(n) POVMS

The Price You Have to Pay…

To sample from the Haar measure with error ε you need $\exp(4^n \log(1/\varepsilon))$ different unitaries

Exponential amount of random bits and quantum gates…

E.g. most quantum require $\exp(cn)$ two qubit gates to be approximately created…

Question Can data hiding states against computational bounded measurements be prepared efficiently?

Quantum Pseudo-Randomness

Sometimes, can replace a Haar random unitary by *pseudo-random* unitaries:

Quantum Unitary t-designs

Def. An ensemble of unitaries $\{\mu(dU), U\}$ in $\mathbf{U}(d)$ is an ε-approximate unitary t-design if for every monomial $M = U_{p1, q1\ldots} U_{pt, qt} U^*_{r1, s1\ldots} U^*_{rt, st,}$

$$|E_\mu(M(U)) - E_{Haar}(M(U))| \leq d^{-2t}\varepsilon$$

Quantum Unitary Designs

Conjecture 1. There are efficient ε-approximate unitary t-designs $\{\mu(dU), U\}$ in $\mathbf{U}(2^n)$

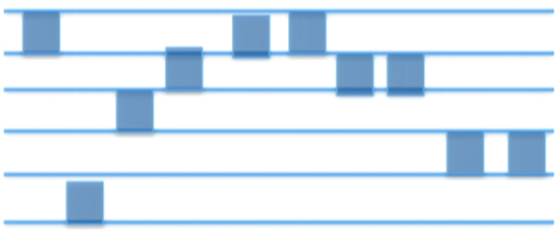
Efficient means:

- unitaries created by poly(n, t, log(1/ε)) two-qubit gates
- $\mu(dU)$ can be sampled in poly(n, t, log(1/ε)) time.

(Harrow and Low '08)
Efficient construction of approximate unitary (n/log(n))-design

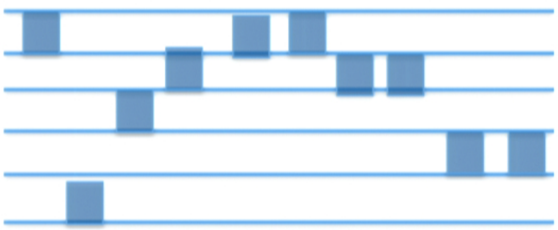
Random Quantum Circuits

Local Random Circuit: in each step an index *i* in {1, … ,n} is chosen uniformly at random and a two-qubits Haar unitary is applied to qubits i e i+1



Random Quantum Circuits

Local Random Circuit: in each step an index *i* in {1, … ,n} is chosen uniformly at random and a two-qubits Haar unitary is applied to qubits i e i+1



Random Walk in $\mathbf{U}(2^n)$
(Another example: Kac's random walk – toy model Boltzmann gas)

Introduced in (Hayden and Preskill '07) as a toy model for the dynamics of a black hole

Random Quantum Circuits as t-designs?

Conjecture 2. Random Circuits of size poly(n, log(1/ε)) are an ε-approximate unitary poly(n)-design

Computational Data Hiding

Most quantum states created by $O(n^k)$ circuits look maximally mixed for every circuit of size $O(n^{(k+4)/6})$

Most is defined in terms of the measure on quantum circuits given by the local random circuit model

Computational Data Hiding

Most quantum states created by $O(n^k)$ circuits look maximally mixed for every circuit of size $O(n^{(k+4)/6})$

Most is defined in terms of the measure on quantum circuits given by the local random circuit model

Computational Data Hiding

Most quantum states created by $O(n^k)$ circuits look maximally mixed for every circuit of size $O(n^{(k+4)/6})$

Same idea (small probability + eps-net), but replace Levy's lemma by a *t*-design bound from (Low '08):

$$\Pr_{U \sim \nu_{s,n}}\left(\left|\langle 0|UAU|0\rangle - 2^{-n} tr(A)\right| \geq \delta\right) \leq \exp\left(O(t \log(1/\delta) - nt)\right)$$

with $t = s^{1/6} n^{-1/3}$ and $\nu_{s,n}$ the measure on $U(2^n)$ induced by s steps of the local random circuit model

Proof Techniques

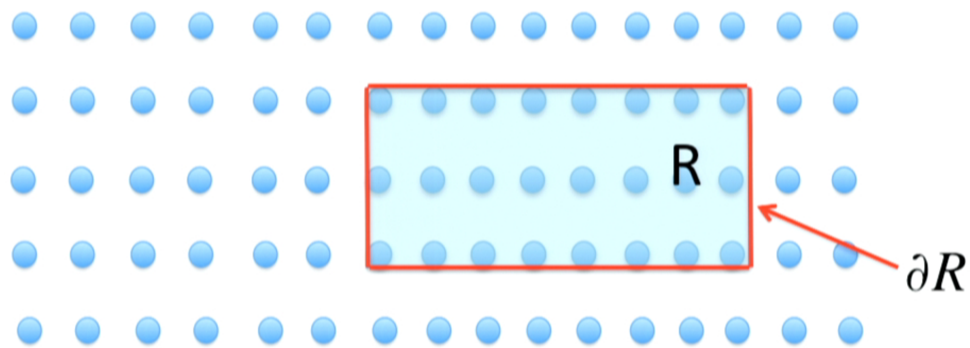
- Quantum Many-body Theory
  Technique for lower bounding spectral gap of frustration-free local Hamiltonians (Nachtergaele '96)

- Representation Theory
  Permutation matrices are approximately orthogonal (Harrow '11)

- Markov Chains
  Path coupling to the unitary group (Oliveira '08)

Area Laws

Let H be a local Hamiltonian on a lattice and $|\psi_0\rangle$ its groundstate



How complex is $|\psi_0\rangle$?

Conjecture: For gapped H,

$$S(\rho_R) \leq O(\partial R), \qquad \rho_R = tr_{\setminus R}\left(|\psi_0\rangle\langle\psi_0|\right)$$

Previous Work

(Vidal et al '02, Plenio et al '05, Etc) Area law for particular models (XY, quasi-free bosonic models, etc)

(Hastings '04) Exponential decay of correlations in gapped models

(Aharonov et al '07, Gottesman, Hastings '09) Groundstates of 1D systems with volume law

(Hastings '07) are law for every gapped 1D Hamiltonian!

(Arad et al '11) improved area law for 1D frustration free models

Previous Work

(Vidal et al ‘02, Plenio et al ’05, Etc) Area law for particular models (XY, quasi-free bosonic models, etc)

(Hastings ‘04) Exponential decay of correlations in gapped models

(Aharonov et al ‘07, Gottesman, Hastings ’09) Groundstates of 1D systems with volume law

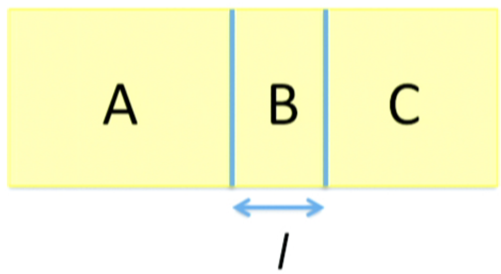
(Hastings ’07) are law for every gapped 1D Hamiltonian!

(Arad et al ’11) improved area law for 1D frustration free models

Area Law vs Decay of Correlations

Decay of Correlations: $\left|tr(\rho_{AC} X \otimes Y) - tr(\rho_A X) tr\left(\rho_C Y\right)\right| \leq e^{-cl}$

Does it imply $\rho_{AC} \approx \rho_A \otimes \rho_C$?



Would lead to area law

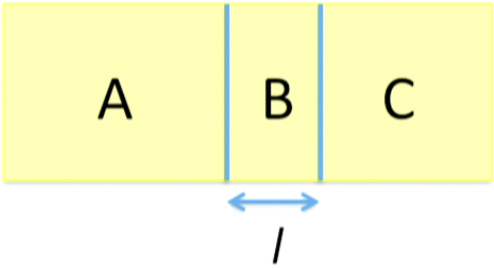
Unfortunately,
No, because of Data Hiding states (Hastings '07)

Does it work for stronger forms of decay of correlations?

Area Law vs Decay of Correlations

Decay of Correlations: $\left|tr(\rho_{AC} X \otimes Y) - tr(\rho_A X) tr\left(\rho_C Y\right)\right| \le e^{-cl}$

Does it imply $\rho_{AC} \approx \rho_A \otimes \rho_C$?



Would lead to area law

Unfortunately,
No, because of Data Hiding states (Hastings '07)

Does it work for stronger forms of decay of correlations?

Stronger Decay of Correlations

One-way LOCC:

$$\max_{X_k, Y_k}\left(\sum_k \left| tr(\rho_{AC} X_k \otimes Y_k) - tr(\rho_A X_k) tr\left(\rho_C Y_k\right)\right| : \sum_k X_k \leq I, 0 \leq Y_k \leq I\right) \leq e^{-cl}$$

Implies area law. But is it satisfied by gapped systems?

Guessing Probability:

$$\max_{X_k, Y_k}\left(\sum_k \left| tr(\rho_{AC} X_k \otimes Y_k) - tr(\rho_A X_k) tr\left(\rho_C Y_k\right)\right| : \sum_k X_k \leq I, \sum_k Y_k \leq I\right) \leq e^{-cl}$$

Is satisfied by gapped systems. But does it imply area law?

Stronger Decay of Correlations

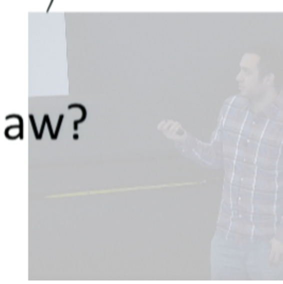
One-way LOCC:

$$\max_{X_k, Y_k}\left(\sum_k \left| tr(\rho_{AC} X_k \otimes Y_k) - tr(\rho_A X_k) tr\left(\rho_C Y_k\right)\right| : \sum_k X_k \leq I, 0 \leq Y_k \leq I\right) \leq e^{-cl}$$

Implies area law. But is it satisfied by gapped systems?

Guessing Probability:

$$\max_{X_k, Y_k}\left(\sum_k \left| tr(\rho_{AC} X_k \otimes Y_k) - tr(\rho_A X_k) tr\left(\rho_C Y_k\right)\right| : \sum_k X_k \leq I, \sum_k Y_k \leq I\right) \leq e^{-cl}$$



Is satisfied by gapped systems. But does it imply area law?

Summary

- Quantum correlations can be hidden in interesting ways
- LOCC data hiding entangled states are the hardest to characterize – correlations more shareable
- One can hide data against efficient measurements efficiently
- $\tilde{O}(n^2 t^5 \log(1/\varepsilon))$ local random circuits are ε-approximate unitary t-designs
- Data Hiding is obstruction to area law. Can we overcome it? Guessing probability decay of correlations useful?