Limitations for Quantum PCPs

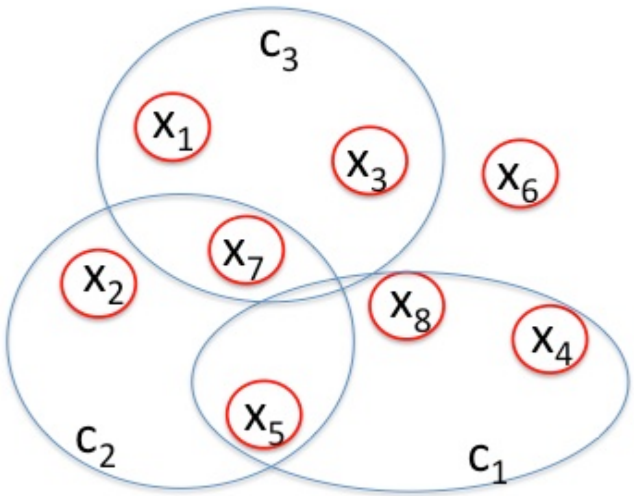
Fernando G.S.L. Brandão
University College London

Based on joint work arXiv:1310.0017 with

Aram Harrow
MIT

Simons Institute, Berkeley, February 2014

Constraint Satisfaction Problems



(k, Σ, n, m)-CSP :

k: arity

Σ: alphabet

n: number of variables

m: number of constraints

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

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

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Quantum Constraint Satisfaction Problems

(k, d, n, m)-*q*CSP *H*

k: arity
d: local dimension
n: number of qudits
m: number of constraints

Constraints: P_j *k*-local projection
Assignment: $|\psi>$ quantum state

(k, Σ, n, m)-CSP : *C*

k: arity
Σ: alphabet
n: number of variables
m: number of constraints

Constraints: $C_j : \Sigma^k \to \{0, 1\}$
Assignment: $\sigma : [n] \to \Sigma$

$$\mathrm{unsat}(H) := \min_{|\psi\rangle} \frac{1}{m} \sum_{j=1}^{m} \langle\psi|P_j|\psi\rangle$$

Quantum Constraint Satisfaction Problems

(k, d, n, m)-*q*CSP *H*

k: arity
d: local dimension
n: number of qudits
m: number of constraints

Constraints: P_j *k*-local projection
Assignment: |ψ> quantum state

(k, Σ, n, m)-CSP : *C*

k: arity
Σ: alphabet
n: number of variables
m: number of constraints

Constraints: $C_j : \Sigma^k \to \{0, 1\}$
Assignment: $\sigma : [n] \to \Sigma$

$$\mathrm{unsat}(H) := \min_{|\psi\rangle} \frac{1}{m} \sum_{j=1}^{m} \langle\psi|P_j|\psi\rangle = \frac{1}{m} \lambda_{\min}\left(\sum_j P_j\right)$$

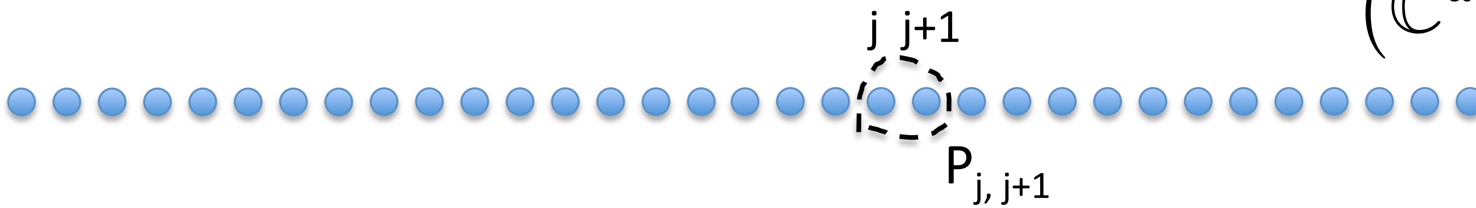
min eigenvalue

Hamiltonian

Quantum Constraint Satisfaction Problems

Ex 1: (2, 2, n, n-1)-qCSP on a line

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

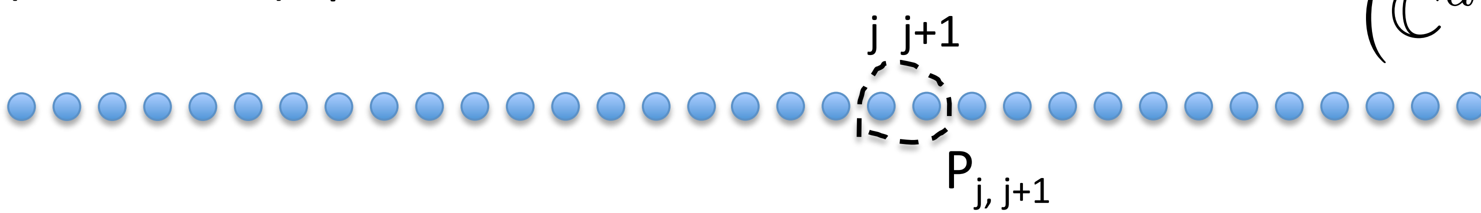


$$H = \sum_j P_j = \sum_j \mathrm{id}_{1,\ldots,j-1} \otimes P_{j,j+1} \otimes \mathrm{id}_{j+2,\ldots,n}$$

Quantum Constraint Satisfaction Problems

Ex 1: (2, 2, n, n-1)-qCSP on a line

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



$$H = \sum_j P_j = \sum_j \mathrm{id}_{1,\ldots,j-1} \otimes P_{j,j+1} \otimes \mathrm{id}_{j+2,\ldots,n}$$

Ex 2: (2, 2, n, m)-qCSP with diagonal projectors:

$$P_j = \sum_{x_{j_1}, x_{j_2}} C_j(x_{j_1}, x_{j_2}) |x_{j_1}, x_{j_2}\rangle\langle x_{j_1}, x_{j_2}|$$

$$\begin{aligned}
\mathrm{unsat}\left(\sum_j P_j\right) &= \min_{\{x_1,\ldots,x_n\}\in\{0,1\}^n} \sum_j \langle x_1,\ldots,x_n|P_j|x_1,\ldots,x_n\rangle / m \\
&= \min_{\{x_1,\ldots,x_n\}\in\{0,1\}^n} C_j(x_{j_1}, x_{j_2}) / m \\
&= \mathrm{unsat}(C)
\end{aligned}$$

PCP Theorem

PCP Theorem (Arora, Safra; Arora-Lund-Motwani-Sudan-Szegedy '98)
There is a $\varepsilon > 0$ s.t. it's NP-hard to determine whether for a CSP, unsat $= 0$ or unsat $> \varepsilon$

- Compare with Cook-Levin thm:
  It's NP-hard to determine whether unsat $= 0$ or unsat $> 1/m$.
- Equivalent to the existence of **P**robabilistically **C**heckable **P**roofs for NP.
- (Dinur '07) Combinatorial proof.
- Central tool in the theory of hardness of approximation.

Quantum Cook-Levin Thm

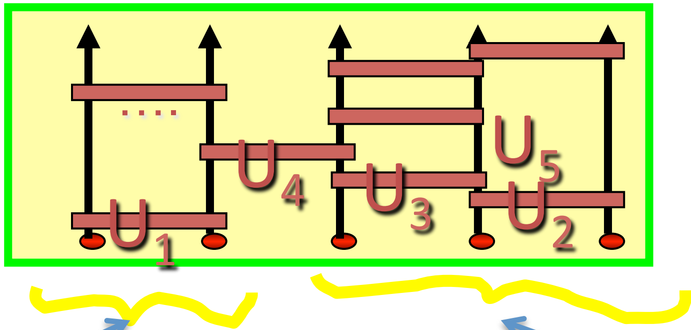
Local Hamiltonian Problem

locality local dim

Given a (k, d, n, m)-qcsp H with constant *k, d* and m = poly(n), decide if unsat(H)=0 or unsat(H)>Δ

Thm (Kitaev '99) The local Hamiltonian problem is QMA-complete for Δ = 1/poly(n)

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



input

proof

Quantum PCP?

The Quantum PCP conjecture: There is $\varepsilon > 0$ s.t. the following problem is QMA-complete: Given $(2, 2, n, m)$-qcsp H determine whether

locality local dim

(i) $\mathrm{unsat}(H)=0$ or (ii) $\mathrm{unsat}(H) > \varepsilon$.

- (Bravyi, DiVincenzo, Loss, Terhal '08) Equivalent to conjecture for (k, d, n, m)-qcsp for any constant k, d.
- At least **NP-hard** (by PCP Thm) and **inside QMA**
- Open *even* for commuting qCSP ($[P_i, P_j] = 0$)

Motivation of the Problem

- Hardness of approximation for QMA

Motivation of the Problem

- Hardness of approximation for QMA

- Quantum-hardness of computing *mean* groundenergy:
  no good ansatz for *any* low-energy state

  (caveat: interaction graph expander; not very physical)

Motivation of the Problem

- Hardness of approximation for QMA
- Quantum-hardness of computing *mean* groundenergy:
  no good ansatz for *any* low-energy state

  (caveat: interaction graph expander; not very physical)
- Sophisticated form of quantum error correction?

Motivation of the Problem

- Hardness of approximation for QMA

- Quantum-hardness of computing *mean* groundenergy: no good ansatz for *any* low-energy state

  (caveat: interaction graph expander; not very physical)

- Sophisticated form of quantum error correction?

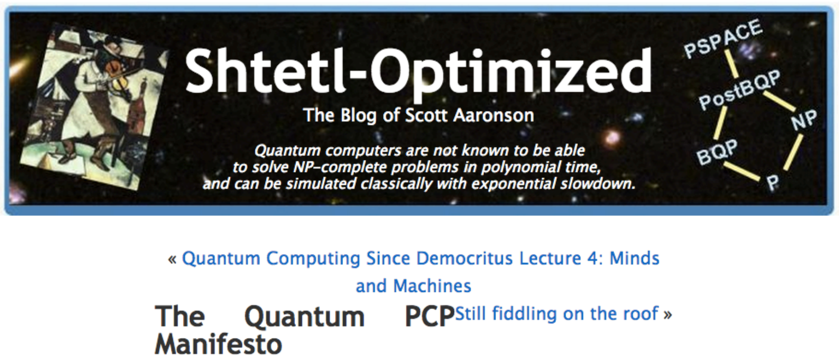
- For more motivation see review (Aharonov, Arad, Vidick '13) and Thomas recorded talk on bootcamp week

History of the Problem

- (Aharonov, Naveh '02) First mention

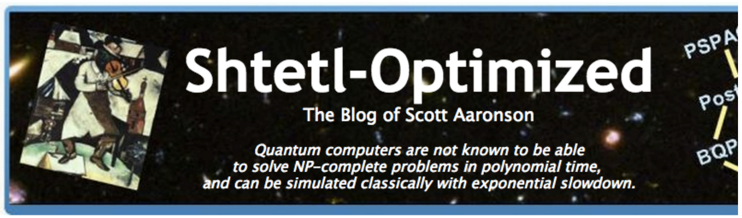
History of the Problem

- (Aharonov, Naveh ’02) First mention
- (Aaronson’ 06) “Quantum PCP manifesto”



History of the Problem

- (Aharonov, Naveh ’02) First mention
- (Aaronson’ 06) “Quantum PCP manifesto”



« Quantum Computing Since Democritus Lecture 4: Minds and Machines

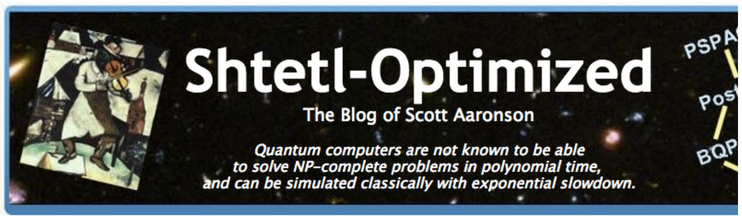
The Quantum PCP Manifesto

Still fiddling on the roof »

I’m 99% sure that this theorem (alright, conjecture) or something close to it is true. I’m 95% sure that the proof will require a difficult adaptation of classical PCP machinery (whether Iritean or pre-Iritean), in much the same way that the Quantum Fault-Tolerance Theorem required a difficult adaptation of classical fault-tolerance machinery. I’m 85% sure that the proof is achievable in a year or so, should enough people make it a priority. I’m 75% sure that the proof, once achieved, will open up heretofore undreamt-of vistas of understanding and insight. I’m 0.01% sure that I can prove it. And that is why I hereby bequeath the actual proving part to you, my readers.

History of the Problem

- (Aharonov, Naveh '02) First mention
- (Aaronson' 06) "Quantum PCP manifesto"



« Quantum Computing Since Democritus Lecture 4: Minds and Machines

The Quantum PCP Manifesto

Still fiddling on the roof »

I'm 99% sure that this theorem (alright, conjecture) or something close to it is true. I'm 95% sure that the proof will require a difficult adaptation of classical PCP machinery (whether Iritean or pre-Iritean), in much the same way that the Quantum Fault-Tolerance Theorem required a difficult adaptation of classical fault-tolerance machinery. I'm 85% sure that the proof is achievable in a year or so, should enough people make it a priority. I'm 75% sure that the proof, once achieved, will open up heretofore undreamt-of vistas of understanding and insight. I'm 0.01% sure that I can prove it. And that is why I hereby bequeath the actual proving part to you, my readers.

I'm quite certain that a Quantum PCP Theorem will require significant new ideas. Recently I spent a day or two studying Irit's proof of the classical PCP theorem (which I hadn't done before), and I found about 20 violations of the No-Cloning Theorem on every page. 😃

History of the Problem

- (Aharonov, Naveh '02) First mention
- (Aaronson' 06) "Quantum PCP manifesto"
- (Aharonov, Arad, Landau, Vazirani '08) Quantum version of gap amplification by random walk on expanders (quantizing Dinur?)

History of the Problem

- (Aharonov, Naveh ’02) First mention
- (Aaronson’ 06) “Quantum PCP manifesto”
- (Aharonov, Arad, Landau, Vazirani ‘08) Quantum version of gap amplification by random walk on expanders (quantizing Dinur?)
- (Arad ‘10) NP-approximation for 2-local (arity 2) almost commuting qCSP

History of the Problem

- (Aharonov, Naveh ’02) First mention
- (Aaronson’ 06) “Quantum PCP manifesto”
- (Aharonov, Arad, Landau, Vazirani ‘08) Quantum version of gap amplification by random walk on expanders (quantizing Dinur?)
- (Arad ‘10) NP-approximation for 2-local (arity 2) almost commuting qCSP
- (Hastings ’12; Hastings, Freedman ‘13) “No low-energy trivial states” conjecture and evidence for its validity

History of the Problem

- (Aharonov, Naveh ’02) First mention
- (Aaronson’ 06) “Quantum PCP manifesto”
- (Aharonov, Arad, Landau, Vazirani ‘08) Quantum version of gap amplification by random walk on expanders (quantizing Dinur?)
- (Arad ‘10) NP-approximation for 2-local (arity 2) almost commuting qCSP
- (Hastings ’12; Hastings, Freedman ‘13) “No low-energy trivial states” conjecture and evidence for its validity
- (Aharonov, Eldar ‘13) NP-approximation for *k*-local commuting qCSP on small set expanders and study of quantum locally testable codes

History of the Problem

- (Aharonov, Naveh '02) First mention
- (Aaronson' 06) "Quantum PCP manifesto"
- (Aharonov, Arad, Landau, Vazirani '08) Quantum version of gap amplification by random walk on expanders (quantizing Dinur?)
- (Arad '10) NP-approximation for 2-local (arity 2) almost commuting qCSP
- (Hastings '12; Hastings, Freedman '13) "No low-energy trivial states" conjecture and evidence for its validity
- (Aharonov, Eldar '13) NP-approximation for *k*-local commuting qCSP on small set expanders and study of quantum locally testable codes
- (B. Harrow '13) Approx. in NP for 2-local non-commuting qCSP

this talk

"Blowing up" maps

prop For every $t \geq 1$ there is an efficient mapping from $(2, \Sigma, n, m)$-csp C to $(2, \Sigma_t, n_t, m_t)$-csp C_t s.t.

(i) $n_t \leq n^{O(t)}$, $m_t \leq m^{O(t)}$

(ii) $\deg(C_t) \geq \deg(C)^t$

(iii) $|\Sigma_t| = |\Sigma|^t$

(iv) $\mathrm{unsat}(C_t) \geq \mathrm{unsat}(C)$

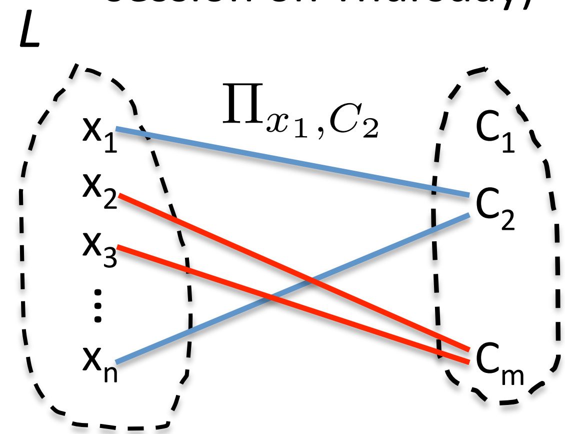
(v) $\mathrm{unsat}(C_t) = 0$ if $\mathrm{unsat}(C) = 0$

Example: Parallel Repetition (for kids)

(see parallel repetition session on Thursday)

1. write C as a *cover label instance* L on $G(V, W, E)$ with function $\Pi_{v,w} : [N] \rightarrow [M]$

Labeling $l : V \rightarrow [N], W \rightarrow [M]$ covers edge (v, w) if $\Pi_{v,w}(l(w)) = l(v)$



2. Define L_t on graph $G'(V', W', E')$ with $V' = V^t$, $W' = W^t$, $[N'] = [N]^t$, $[M'] = [M]^t$

Edge set: $(v' = \{v_{i_1}, \ldots, v_{i_t}\}, w' = \{w_{i_1}, \ldots . w_{t_t}\}) \in E$ iff $(v_{i_j}, w_{i_j}) \in E, \ \forall\, i \in [n], 0 \leq j \leq t$

Function: $\Pi_{v',w'}(b_1, \ldots, b_t) = \{\Pi_{v_1,w_1}, \ldots, \Pi_{v_t,w_t}\}$

Example: Parallel Repetition (for kids)

(see parallel repetition
ay)

1. write *C*
L on G(

Labeling
edge (v,

C_1
C_2
C_m

Easy to see:

(i) $n_t \leq n^{O(t)}$, $m^{O(t)}$

(ii) $\mathrm{Deg}(L_t) \geq \deg(C)^t$,

(iii) $\mathrm{unsat}(L_t) \geq \mathrm{unsat}(C)$,

(iv) $|\Sigma_t| = |\Sigma|^t$,

(v) $\mathrm{unsat}(L_t) = 0$ if $\mathrm{unsat}(C) = 0$

(vi) $\mathrm{unsat}(L_t) \geq \mathrm{unsat}(C)$

In fact: (Raz '95) If $\mathrm{unsat}(C) \geq \delta$, $\mathrm{unsat}(L_t) \geq 1 - \exp(-\Omega(\delta^3 t))$

2. Define
$V' = V^t$,

Edge set: $(v' = \{v_{i_1}, \ldots, v_{i_t}\}, w' = \{w_{i_1}, \ldots . w_{t_t}\}) \in E$

iff $(v_{i_j}, w_{i_j}) \in E,\ \forall\, i \in [n], 0 \leq j \leq t$

Function: $\Pi_{v',w'}(b_1, \ldots, b_t) = \{\Pi_{v_1,w_1}, \ldots, \Pi_{v_t,w_t}\}$

Quantum “Blowing up” maps + Quantum PCP?

Quantum "Blowing up" maps + Quantum PCP?

thm If for every $t \geq 1$ there is an efficient mapping from $(2, d, n, m)$-qcsp H to $(2, d_t, n_t, m_t)$-qcsp H_t s.t.

(i) $n_t \leq n^{O(t)}$, $m_t \leq m^{O(t)}$

(ii) $\mathrm{Deg}(H_t) \geq \deg(H)^t$

(iii) $|d_t| = |d|^t$

(iv) $\mathrm{unsat}(H_t) \geq \mathrm{unsat}(H)$

(v) $\mathrm{unsat}(H_t) = 0$ if $\mathrm{unsat}(H) = 0$

then the quantum PCP conjecture is *false*.

Formalizes difficulty of "quantizing" proofs of the PCP theorem

(e.g. Dinur's proof; see (Aharonov, Arad, Landau, Vazirani '08))

Obs: Apparently *not* related to parallel repetition for quantum games

(see session on Thursday)

Entanglement Monogamy…

…is the main idea behind the result.

Entanglement cannot be freely shared

Ex. 1 $\rho_{AB} = |\phi^+\rangle\langle\phi^+|_{AB}, \quad |\phi^+\rangle = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$, $\rho_{ABC} = \rho_{AB} \otimes \rho_C$

Entanglement Monogamy…

…is the main idea behind the result.

Entanglement cannot be freely shared

Ex. 1 $\rho_{AB} = |\phi^+\rangle\langle\phi^+|_{AB}, \quad |\phi^+\rangle = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$, $\rho_{ABC} = \rho_{AB} \otimes \rho_C$

Ex. 2 $|\mathrm{CAT}\rangle_{A_1,\ldots,A_n} = (|0,\ldots,0\rangle + |1,\ldots,1\rangle)/\sqrt{2}$

$$\rho_{A_i A_j} := \mathrm{tr}_{\backslash A_i A_j}(|\mathrm{CAT}\rangle\langle\mathrm{CAT}|) = (|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1|)/2$$

Entanglement Monogamy…

…is the main idea behind the result.

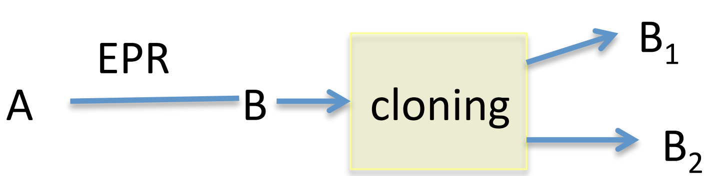
Entanglement cannot be freely shared

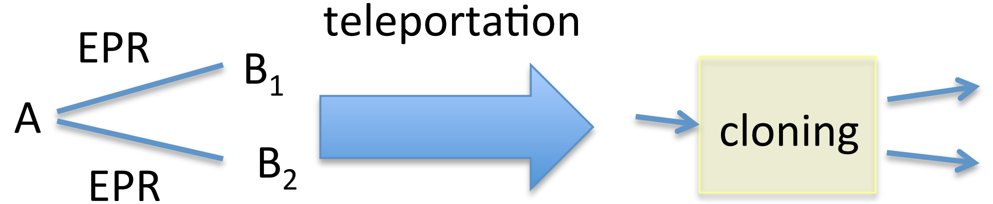
Ex. 1 $\rho_{AB} = |\phi^+\rangle\langle\phi^+|_{AB}, \quad |\phi^+\rangle = (|0,0\rangle + |1,1\rangle)/\sqrt{2},\ \ \rho_{ABC} = \rho_{AB} \otimes \rho_C$

Ex. 2 $|\mathrm{CAT}\rangle_{A_1,\ldots,A_n} = \left(|0,\ldots,0\rangle + |1,\ldots,1\rangle\right)/\sqrt{2}$

$$\rho_{A_i A_j} := \mathrm{tr}_{\setminus A_i A_j}\left(|\mathrm{CAT}\rangle\langle\mathrm{CAT}|\right) = (|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1|)/2$$

Monogamy vs cloning:



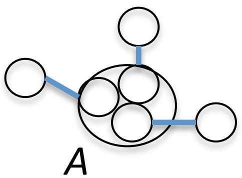


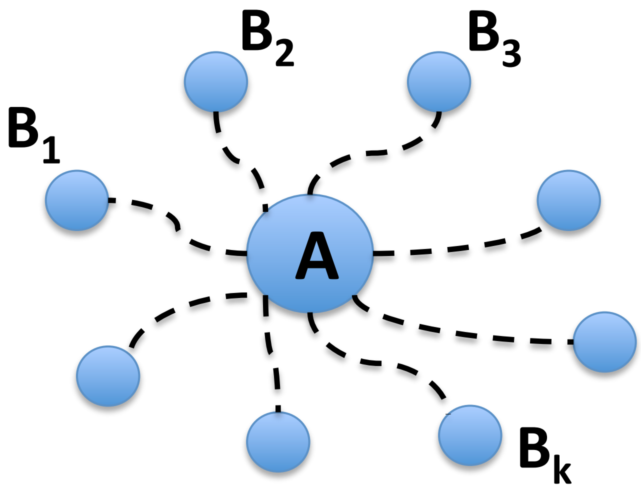
A maximally entangled with B_1 and B_2

Entanglement Monogamy…

…intuition:

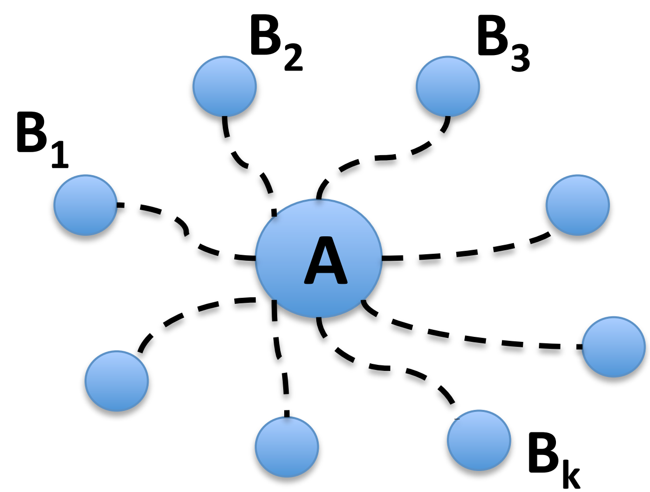
- *A* can only be substantially entangled with a few of the *B*s
- How entangled it can be depends on the *size* of *A*.

Ex. 

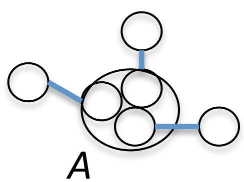


Entanglement Monogamy…

…intuition:



- *A* can only be substantially entangled with a few of the *B*s
- How entangled it can be depends on the *size* of *A.*

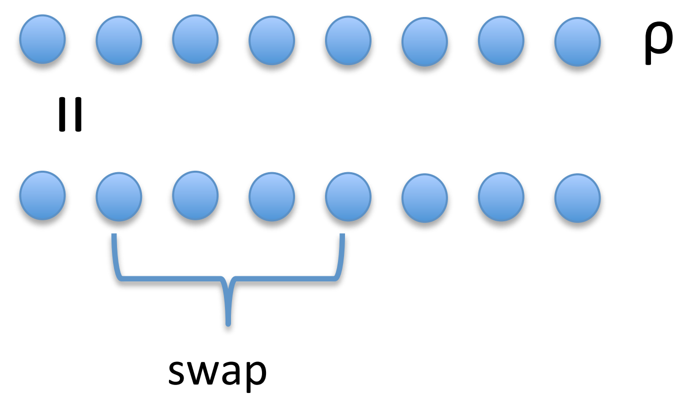
Ex. 

How to make it quantitative?

1. Study behavior of entanglement measures (distillable entanglement, squashed entanglement, …) (see Patrick's talk)
2. Study specific tasks (QKD, MIP*, …) (see sessions on MIP and device independent crypto)
3. Quantum de Finetti Theorems (see also Aram's talk)

Quantum de Finetti Theorems

Let $\rho_{1,\ldots,n}$ be permutation-symmetric, i.e.



Quantum de Finetti Thm:

$$\rho_{1,\ldots,l} \approx \sum_k p_k \rho_k^{\otimes l}$$

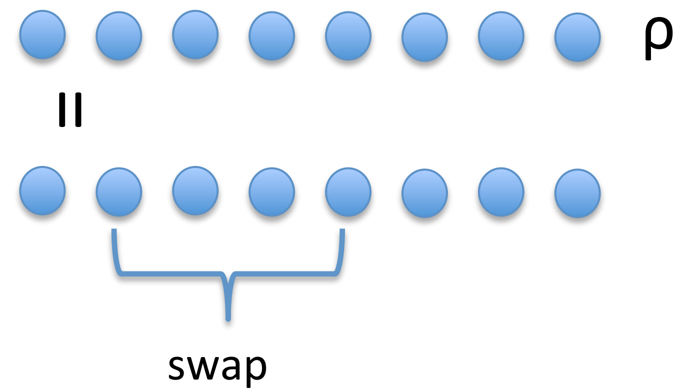
$$\frac{d^2 l}{n}$$

(Christandl, Koenig, Mitchson, Renner '05)

- In complete analogy with de Finetti thm for symmetric probability distributions
- But much more remarkable: *entanglement* is destroyed

Quantum de Finetti Theorems

Let $\rho_{1,\dots,n}$ be permutation-symmetric, i.e.



Quantum de Finetti Thm:

$$\rho_{1,\dots,l} \approx \sum_k p_k \rho_k^{\otimes l}$$

$$\frac{d^2 l}{n}$$

(Christandl, Koenig, Mitchson, Renner '05)

- In complete analogy with de Finetti thm for symmetric probability distributions
- But much more remarkable: *entanglement* is destroyed

- Final installment in a long sequence of works: (Hudson, Moody '76), (Stormer '69), (Raggio, Werner '89), (Caves, Fuchs, Schack '01), (Koenig, Renner '05), …
- Can we improve on the error? (see Aram's and Patrick's talk)
- Can we find a more general result, beyond permutation-invariant states?

General Quantum de Finetti

thm (B., Harrow '13) Let G = (V, E) be a D-regular graph with n = |V|. Let $\rho_{1,\dots,n}$ be a n-qudit state. Then there exists a *globally separable* state $\sigma_{1,\dots,n}$ such that

$$\mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \leq 12 \left(\frac{d^2 \ln(d)}{D} \right)^{1/3}$$

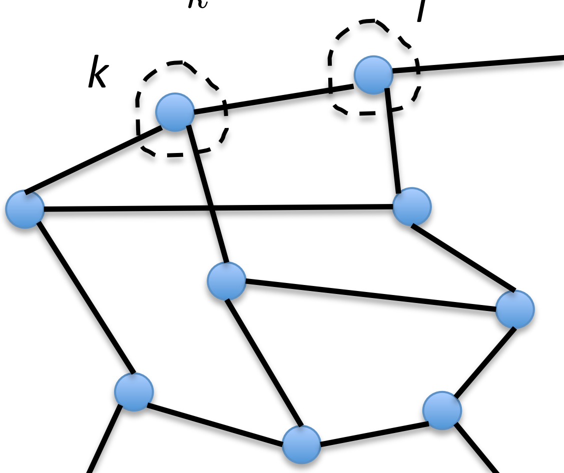
Globally separable (unentangled):

$$\rho_{ij} \approx \sigma_{ij} = \sum_k p_k \sigma_{k_i} \otimes \sigma_{k_j}$$

$$\sigma = \sum_k p_k \sigma_{k_1} \otimes \dots \otimes \sigma_{k_n}$$

probability distribution

local states



General Quantum de Finetti

thm (B., Harrow '13) Let G = (V, E) be a D-regular graph with n = |V|. Let $\rho_{1,\ldots,n}$ be a n-qudit state. Then there exists a *globally separable* state $\sigma_{1,\ldots,n}$ such that

$$\mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \leq 12 \left(\frac{d^2 \ln(d)}{D} \right)^{1/3}$$

Ex 1. "Local entanglement":

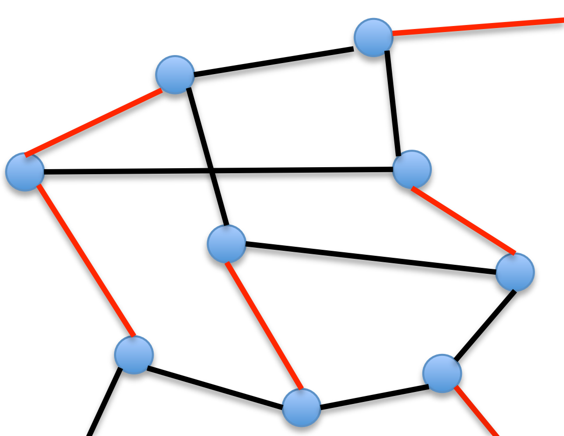
For (i, j) red: $\|\rho_{i,j} - \sigma_{i,j}\|_1 \geq 1/4$

EPR Separable

But for all other (i, j): $\rho_{i,j} = \rho_i \otimes \rho_j$

$\sigma = \rho_1 \otimes \ldots \otimes \rho_n$ gives good approx.

Red edge: EPR pair



General Quantum de Finetti

thm (B., Harrow '13) Let G = (V, E) be a D-regular graph with n = |V|. Let $\rho_{1,\ldots,n}$ be a n-qudit state. Then there exists a *globally separable* state $\sigma_{1,\ldots,n}$ such that

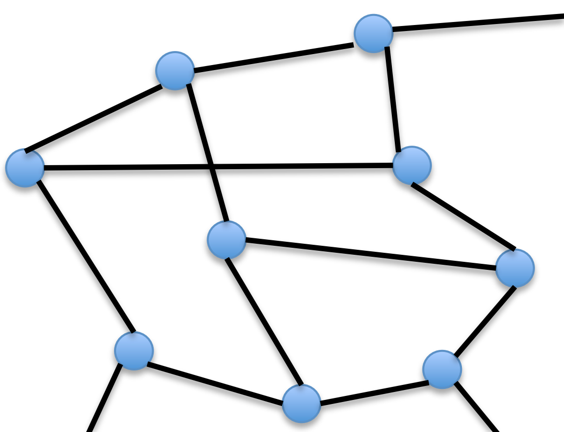
$$\mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \leq 12 \left(\frac{d^2 \ln(d)}{D} \right)^{1/3}$$

Ex 2. "Global entanglement":

Let ρ = |φ><φ| be a Haar random state

|φ> has a lot of entanglement (e.g. for every region *X*, S(X) ≈ number qubits in *X*)

But: $\rho_{i,j} \approx \frac{\mathrm{id} \otimes \mathrm{id}}{d^2}$



General Quantum de Finetti

thm (B., Harrow '13) Let $G = (V, E)$ be a D-regular graph with $n = |V|$. Let $\rho_{1,\ldots,n}$ be a n-qudit state. Then there exists a *globally separable* state $\sigma_{1,\ldots,n}$ such that

$$\mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \leq 12 \left(\frac{d^2 \ln(d)}{D} \right)^{1/3}$$

Ex 3.

Let $\rho = |CAT\rangle\langle CAT|$ with $|CAT\rangle = (|0, \ldots, 0\rangle + |1, \ldots, 1\rangle)/\sqrt{2}$

$$\rho_{i,j} = \frac{1}{2}|0,0\rangle\langle 0,0| + \frac{1}{2}|1,1\rangle\langle 1,1|$$

$$\sigma = \frac{1}{2}|0,\ldots,0\rangle\langle 0,\ldots,0| + \frac{1}{2}|1,\ldots,1\rangle\langle 1,\ldots,1|$$

gives a good approximation

Product-State Approximation

cor Let G = (V, E) be a D-regular graph with n = |V|. Let

$$H = \sum_{(i,j)\in E} P_{i,j}$$

Then there exists $|\phi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$ such that

$$\frac{2}{nD}\langle\phi|H|\phi\rangle \leq \text{unsat}(H) + 12\left(\frac{d^2\log(d)}{D}\right)^{1/3}$$

- The problem is in NP for $\varepsilon = O(d^2\log(d)/D)^{1/3}$ (φ is a classical witness)
- Limits the range of parameters for which quantum PCPs can exist
- For any constants c, α, β > 0 it's NP-hard to tell whether

  unsat = 0 or unsat ≥ c $|\Sigma|^{\alpha}/D^{\beta}$

Product-State Approximation

From **thm** to **cor**:

Let ρ be optimal assignment (aka groundstate) for $H = \sum_{(i,j)\in E} P_{i,j}$

By **thm**:

$$\exists\ \sigma = \sum_k p_k \sigma_{k_1} \otimes \ldots \otimes \sigma_{k_n} \quad \text{s.t.} \quad \mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \le 12 \left(\frac{d^2 \ln(d)}{D} \right)^{1/3}$$

Then

$$\frac{2}{nD}\mathrm{tr}(\sigma H) - \underbrace{\frac{2}{nD}\mathrm{tr}(\rho H)}_{\text{unsat}(H)} = \mathop{\mathbb{E}}_{(i,j)\in E} \mathrm{tr}(P_{i,j}(\sigma - \rho)) \le \mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1$$

Product-State Approximation

From **thm** to **cor**:

Let ρ be optimal assignment (aka groundstate) for $H = \sum_{(i,j)\in E} P_{i,j}$

By **thm**:

$$\exists\ \sigma = \sum_k p_k \sigma_{k_1} \otimes \ldots \otimes \sigma_{k_n} \quad \text{s.t.} \quad \mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1 \leq 12 \left(\frac{d^2 \ln(d)}{D}\right)^{1/3}$$

Then

$$\frac{2}{nD}\operatorname{tr}(\sigma H) - \underbrace{\frac{2}{nD}\operatorname{tr}(\rho H)}_{\text{unsat}(H)} = \mathop{\mathbb{E}}_{(i,j)\in E} \operatorname{tr}(P_{i,j}(\sigma - \rho)) \leq \mathop{\mathbb{E}}_{(i,j)\in E} \|\rho_{i,j} - \sigma_{i,j}\|_1$$

So

$$\frac{2}{nD}\sum_k p_k \operatorname{tr}(\sigma_{k_1} \otimes \ldots \otimes \sigma_{k_n} H) = \frac{2}{nD}\operatorname{tr}(\sigma H) \leq \text{unsat}(H) + 12\left(\frac{d^2\ln(d)}{D}\right)^{1/3}$$

Coming back to quantum "blowing up" maps + qPCP

thm If for every $t \geq 1$ there is an efficient mapping from $(2, d, n)$-qcsp H to $(2, d_t, n_t)$-qcsp H_t s.t.

(i) $n_t \leq n^{O(t)}$
(ii) $\mathrm{Deg}(H_t) \geq \deg(H)^t$
(iii) $|d_t| = |d|^t$
(iv) $\mathrm{unsat}(H_t) \geq \mathrm{unsat}(H)$
(v) $\mathrm{unsat}(H_t) = 0$ if $\mathrm{unsat}(H) = 0$

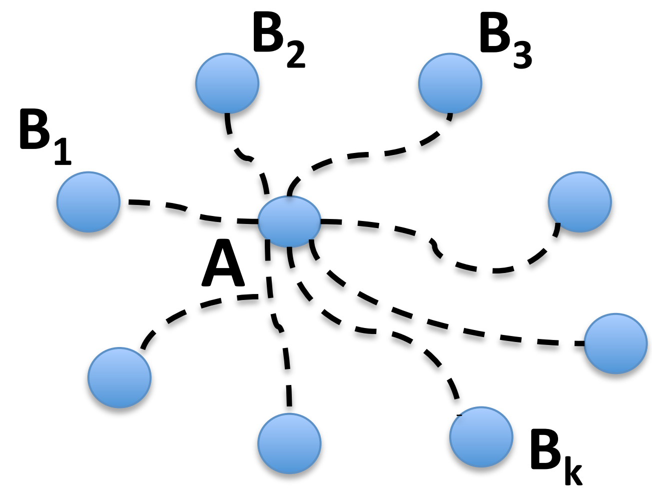
then the quantum PCP conjecture is *false*.

Suppose w.l.o.g. $d^2\log(d)/D < ½$ for C. Then there is a product state φ s.t.

$$\frac{2}{n_t D_t}\langle\phi|H_t|\phi\rangle \leq \mathrm{unsat}(H_t) + 12\left(\frac{d_t^2\log(d_t)}{D_t}\right)^{1/3} \leq \mathrm{unsat}(H_t) + 12\left(\frac{d^2\log(d)}{D}\right)^{t/3}$$

Proving de Finetti Approximation

For simplicity let's consider a *star* graph



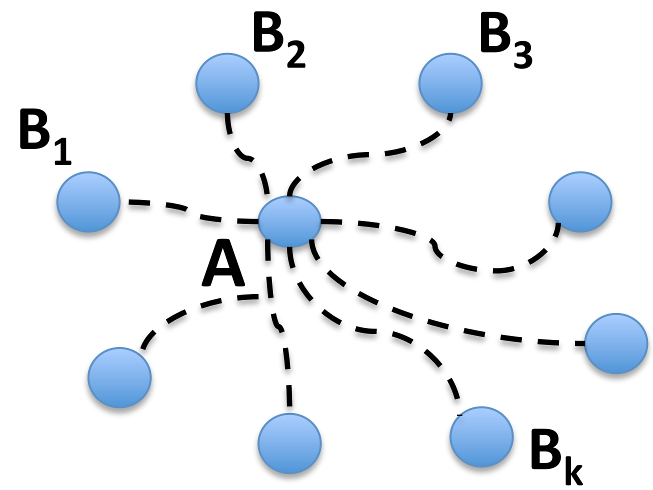
Want to show: there is a state

$$\sigma_{AB_1,\ldots,B_D} = \sum_k p_k \sigma_{A,k} \otimes \sigma_{B_1,k} \otimes \ldots \otimes \sigma_{B_D,k}$$

s.t. $\mathbb{E}_i \|\rho_{AB_i} - \sigma_{AB_i}\|_1 \leq 12 \left(\frac{d^2 ln(d)}{D} \right)^{1/3}$

Proving de Finetti Approximation

For simplicity let's consider a *star* graph



Want to show: there is a state

$$\sigma_{AB_1,\ldots,B_D} = \sum_k p_k \sigma_{A,k} \otimes \sigma_{B_1,k} \otimes \ldots \otimes \sigma_{B_D,k}$$

s.t. $\mathop{\mathbb{E}}_i \|\rho_{AB_i} - \sigma_{AB_i}\|_1 \leq 12 \left(\frac{d^2 ln(d)}{D} \right)^{1/3}$

Idea: Use *information theory*. Consider $\mathop{\mathbb{E}}_{i_1,\ldots,i_D} I(A : B_{i_1}, \ldots, B_{i_D})$

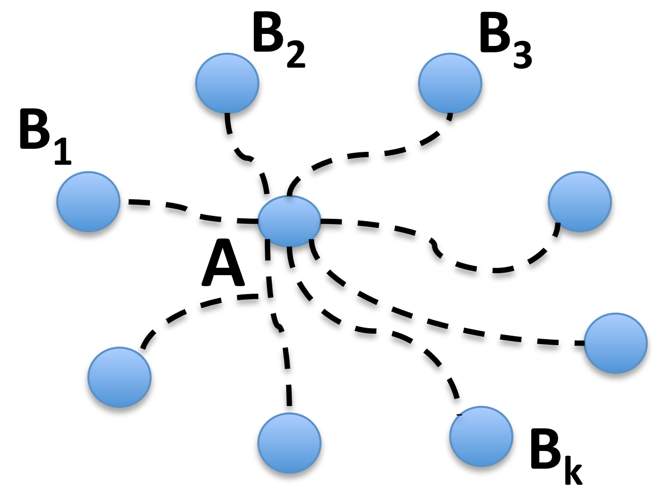
mutual info:
I(X:Y) = H(X) + H(Y) – H(XY)

(i) $I(A : B_{i_1}, \ldots, B_{i_D}) \leq 2 \log(d)$

(ii) $I(A : B_{i_1}, \ldots, B_{i_D}) = I(A : B_{i_1}) + \ldots + I(A : B_{i_D} : B_{i_1} \ldots B_{i_{D-1}})$

Proving de Finetti Approximation

For simplicity let's consider a *star* graph



Want to show: there is a state

$$\sigma_{AB_1,\dots,B_D} = \sum_k p_k \sigma_{A,k} \otimes \sigma_{B_1,k} \otimes \dots \otimes \sigma_{B_D,k}$$

s.t. $\mathop{\mathbb{E}}_i \|\rho_{AB_i} - \sigma_{AB_i}\|_1 \leq 12 \left(\frac{d^2 ln(d)}{D} \right)^{1/3}$

Idea: Use *information theory*. Consider $\mathop{\mathbb{E}}_{i_1,\dots,i_D} I(A : B_{i_1}, \dots, B_{i_D})$

mutual info:
I(X:Y) = H(X) + H(Y) – H(XY)

(i) $I(A : B_{i_1}, \dots, B_{i_D}) \leq 2\log(d)$

(ii) $I(A : B_{i_1}, \dots, B_{i_D}) = I(A : B_{i_1}) + \dots + I(A : B_{i_D} : B_{i_1} \dots B_{i_{D-1}})$

$$\exists\, s \leq D : \mathop{\mathbb{E}}_{i_1,\dots,i_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s} | B_{i_1} \dots B_{i_{s-1}}) \leq \frac{2\log(d)}{D}$$

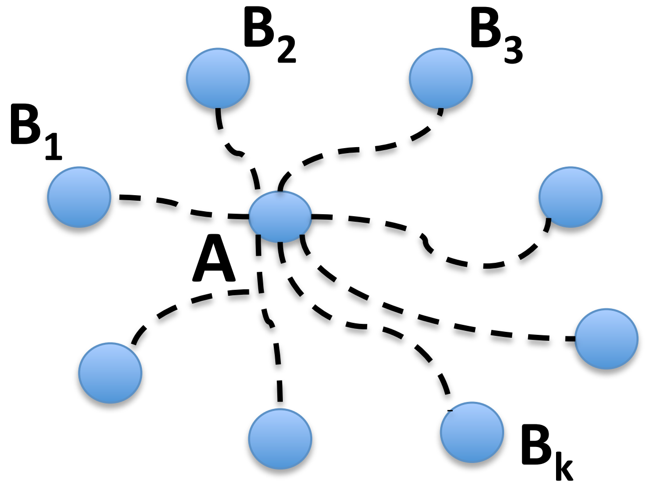
What small conditional mutual info implies?

$$\exists\, s \leq D : \mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s} | B_{i_1} \ldots B_{i_{s-1}}) \leq \frac{2\log(d)}{D}$$

For X, Y, Z random variables

$$I(X:Y|Z)_p = \mathbb{E}_z I(X:Y)_{p_z}$$

$$p_z(x,y) = p(x,y,z)/p(z)$$



No similar interpretation is known for I(X:Y|Z) with *quantum* Z

Solution: Measure sites $i_1, \ldots, i_{s-1}$

Proof Sktech

Consider a measurement $\Lambda(X) := \sum_k \mathrm{tr}(M_k X)|k\rangle\langle k|$

and $\pi = \mathrm{id}_A \otimes \Lambda^{\otimes D}(\rho)$

POVM

Proof Sktech

Consider a measurement $\Lambda(X) := \sum_k \mathrm{tr}(M_k X)|k\rangle\langle k|$

and $\pi = \mathrm{id}_A \otimes \Lambda^{\otimes D}(\rho)$

POVM

There exists s ≤ D s.t. $\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s} | B_{i_1} \ldots B_{i_{s-1}})_{\pi_r} \leq \frac{2\log(d)}{D}$

So $\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s})_{\pi_r} \leq \frac{2\log(d)}{D}$

with π_r the postselected state conditioned on outcomes *(r_1, ..., r_{s-1})*.

Proof Sktech

Consider a measurement $\Lambda(X) := \sum_k \mathrm{tr}(M_k X)|k\rangle\langle k|$

and $\pi = \mathrm{id}_A \otimes \Lambda^{\otimes D}(\rho)$

POVM

There exists s ≤ D s.t. $\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s} | B_{i_1} \ldots B_{i_{s-1}})_{\pi_r} \leq \frac{2\log(d)}{D}$

So $\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} I(A : B_{i_s})_{\pi_r} \leq \frac{2\log(d)}{D}$

with π_r the postselected state conditioned on outcomes *(r_1, …, r_{s-1})*. Thus:

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \|(\pi_r)_{AB_{i_s}} - (\pi_r)_A \otimes (\pi_r)_{B_{i_s}}\|_1 \leq \left(\frac{4\ln(2)\log(d)}{D}\right)^{1/2}$$

(by Pinsker inequality)

Proof Sktech

Again:

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \| (\pi_r)_{AB_{i_s}} - (\pi_r)_A \otimes (\pi_r)_{B_{i_s}} \|_1 \leq \left(\frac{4 \ln(2) \log(d)}{D} \right)^{1/2}$$

But $(\pi_r)_{A,B_i} = \mathrm{id}_A \otimes \Lambda_{B_i}(\rho_r)$. Choosing Λ an **informationally-complete** measurement:

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \| (\rho_r)_{AB_{i_s}} - (\rho_r)_A \otimes (\rho_r)_{B_{i_s}} \|_1 \leq 12 \left(\frac{d^2 \log(d)}{D} \right)^{1/2}$$

Conversion factor from info-complete meas.

Proof Sktech

Again:

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \|(\pi_r)_{AB_{i_s}} - (\pi_r)_A \otimes (\pi_r)_{B_{i_s}}\|_1 \leq \left(\frac{4\ln(2)\log(d)}{D}\right)^{1/2}$$

But $(\pi_r)_{A,B_i} = \mathrm{id}_A \otimes \Lambda_{B_i}(\rho_r)$. Choosing Λ an **informationally-complete** measurement:

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \|(\rho_r)_{AB_{i_s}} - (\rho_r)_A \otimes (\rho_r)_{B_{i_s}}\|_1 \leq 12\left(\frac{d^2\log(d)}{D}\right)^{1/2}$$

Conversion factor from info-complete meas.

Separable state: $\sigma = \mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} (\rho_{\vec{r},\vec{i}})_A \otimes \left(\bigotimes_{k\in[D]} (\rho_{\vec{r},\vec{i}})_{B_k}\right)$

Finally:

$$\mathop{\mathbb{E}}_{i} \|\rho_{AB_i} - \sigma_{AB_i}\|_1 \leq \mathop{\mathbb{E}}_{i_1,\ldots,i_{s-1}} \mathop{\mathbb{E}}_{r_1,\ldots,r_{s-1}} \mathop{\mathbb{E}}_{i_s} \|(\rho_s)_{AB_{i_s}} - (\rho_r)_A \otimes (\rho_r)_{B_{i_s}}\|_1$$

$$\leq 12\left(\frac{d^2\log(d)}{D}\right)$$

Product-State Approximation: General Theorem

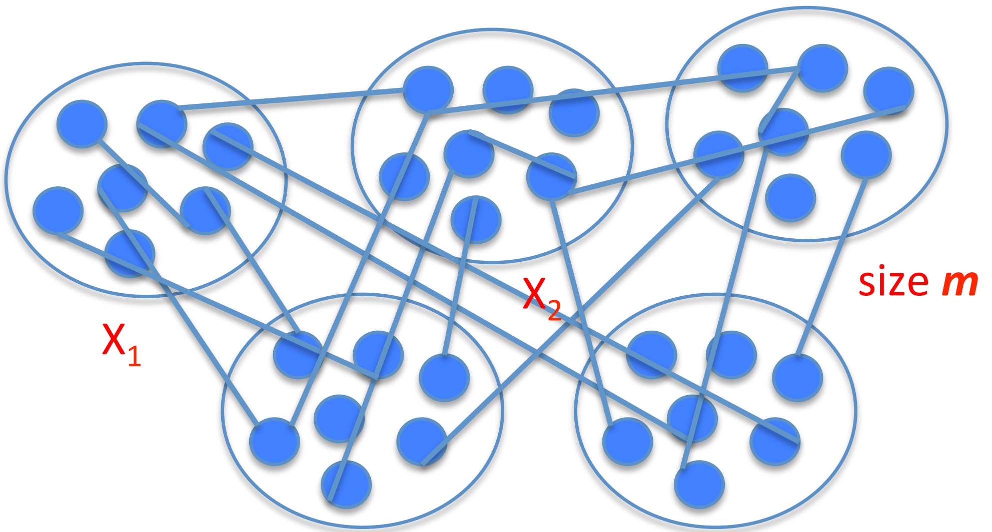
thm Let H be a 2-local Hamiltonian on qudits with D-regular interaction graph G(V, E) and |E| local terms.

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

$$\frac{2}{nD}\langle\phi_1,\ldots,\phi_{n/m}|H|\phi_1,\ldots,\phi_{n/m}\rangle \leq \text{unsat}(H) + 9\left(\frac{d^2\ln(d)\Phi_G}{D}\frac{\mathbb{E}_i S(X_i)}{m}\right)^{1/6}$$

Φ_G : average expansion

$S(X_i)$: entropy of groundstate in X_i



Product-State Approximation: General Theorem

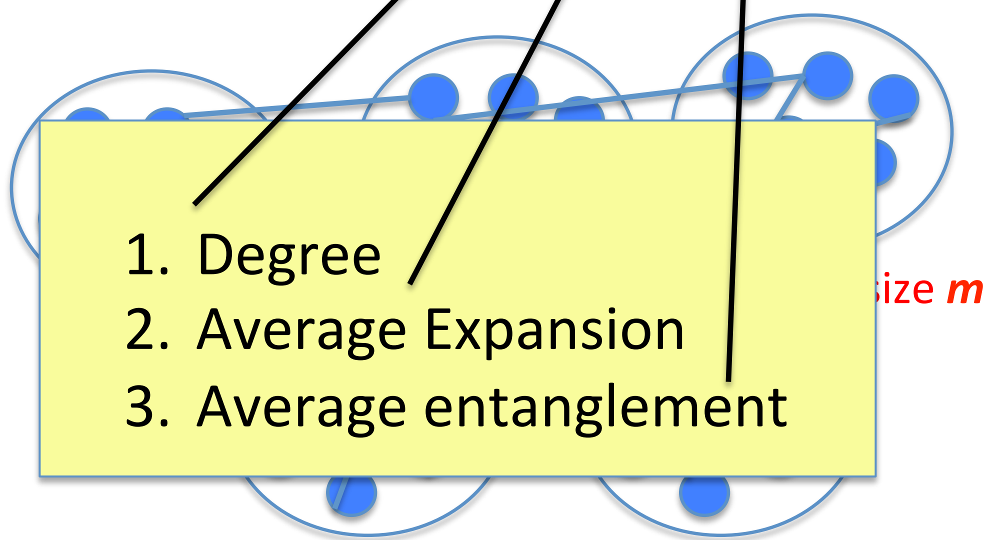
thm Let H be a 2-local Hamiltonian on qudits with D-regular interaction graph $G(V, E)$ and $|E|$ local terms.

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

$$\frac{2}{nD}\langle \phi_1,\ldots,\phi_{n/m}|H|\phi_1,\ldots,\phi_{n/m}\rangle \leq \mathrm{unsat}(H) + 9\left(\frac{d^2\ln(d)\Phi_G}{D}\frac{\mathbb{E}_i S(X_i)}{m}\right)^{1/6}$$

Φ_G : average expansion

$S(X_i)$: entropy of groundstate in X_i



1. Degree
2. Average Expansion
3. Average entanglement

Summary and Open Questions

Summary:

Entanglement monogamy puts limitations on quantum PCPs *and* on approaches for proving them.

Open questions:

- Can we combine (BH '13) with (Aharonov, Eldar '13)? I.e. approximation for highly expanding non-commuting *k*-local models?
  (Needs to go beyond both product-state approximations and Bravyi-Vyalyi)
- Relate quantum "blowing up" maps to quantum games?
- Improved clock-constructions for better gap? (Daniel's talk)
- Understand better power of tensor network states (product states 1st level)
- (dis)prove quantum PCP conjecture!

Summary and Open Questions

Summary:

Entanglement monogamy puts limitations on quantum PCPs
and on approaches for proving them.

Open questions:

- Can we combine (BH '13) with (Aharonov, Eldar '13)? I.e. approximation for highly expanding non-commuting *k*-local models?
  (Needs to go beyond both product-state approximations and Bravyi-Vyalyi)
- Relate quantum "blowing up" maps to quantum games?
- Improved clock-constructions for better gap? (Daniel's talk)
- Understand better power of tensor network states (product states 1st level)
- (dis)prove quantum PCP conjecture!

Thanks!