Limitations on quantum PCPs

Aram Harrow
based on joint work with Fernando G.S.L. Brandão (ETHZ->Imperial)

PCP theorem

Classical k-CSPs:
Given constraints $C=\{C_i\}$, choose an assignment σ mapping n variables to an alphabet Σ to minimize the fraction of unsatisfied constraints.

$$\text{UNSAT}(C) = \min_{\sigma} \Pr_i [\sigma \text{ fails to satisfy } C_i]$$

Example: 3-SAT:
NP-hard to determine if $\text{UNSAT}(C)=0$ or $\text{UNSAT}(C) \geq 1/n^3$

PCP (probabilistically checkable proof) theorem:
NP-hard to determine if $\text{UNSAT}(C)=0$ or $\text{UNSAT}(C) \geq 0.1$

quantum background

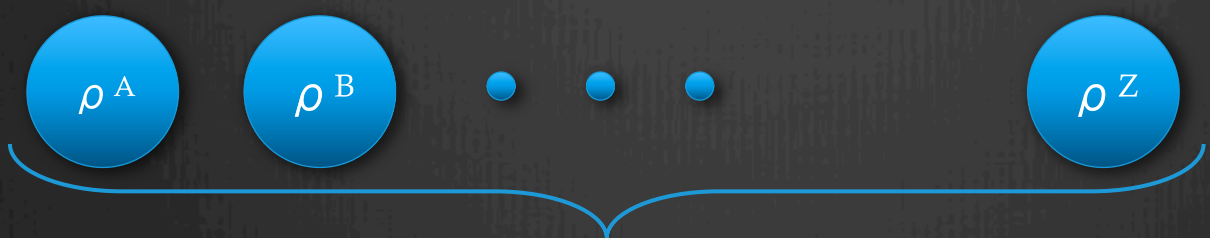
Density matrices

A quantum state on n qubits is described by a $2^n \times 2^n$ [density] matrix ρ satisfying $\rho \geq 0$ and $\mathrm{tr}\,\rho = 1$.

Classical analogue:

Diagonal density matrices $\cong$ probability distributions

Tensor product:



$$\rho^A \otimes \rho^B \otimes \ldots \otimes \rho^Z$$

$$(\rho^{X_1} \otimes \cdots \otimes \rho^{X_n})_{(i_1,\ldots,i_n),(j_1,\ldots,j_n)} = \rho^{X_1}_{i_1,j_1} \rho^{X_2}_{i_2,j_2} \cdots \rho^{X_n}_{i_n,j_n}$$

Local Hamiltonian problem

LOCAL-HAM: k-local Hamiltonian ground-state energy estimation

Let $H = \mathbb{E}_i H_i$, with each H_i acting on k qubits, and $\|H_i\| \leq 1$

i.e. $H_i = H_{i,1} \otimes H_{i,2} \otimes \ldots \otimes H_{i,n}$, with $\#\{j : H_{i,j} \neq I\} \leq k$

Goal:

Estimate $E_0 = \min_\rho \operatorname{tr} H\rho$

Hardness

- Includes k-CSPs, so ±0.1 error is NP-hard by PCP theorem.
- QMA-complete with 1/poly(n) error [Kitaev '99]

  QMA = quantum proof, bounded-error polytime quantum verifier

Quantum PCP conjecture

LOCAL-HAM is QMA-hard for some constant error $\varepsilon > 0$.

Can assume k=2 WLOG [Bravyi, DiVincenzo, Terhal, Loss '08]

high-degree in NP

Theorem

It is NP-complete to estimate E_0 for n qudits on a D-regular graph ($k=2$) to additive error $\sim d / D^{1/8}$.

Idea: use product states

$E_0 \approx \min \operatorname{tr} H(\rho_1 \otimes \ldots \otimes \rho_n) - O(d/D^{1/8})$

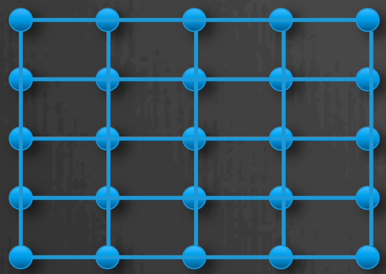
By constrast

2-CSPs are NP-hard to approximate to error $|\Sigma|^\alpha/D^\beta$ for any $\alpha,\beta>0$

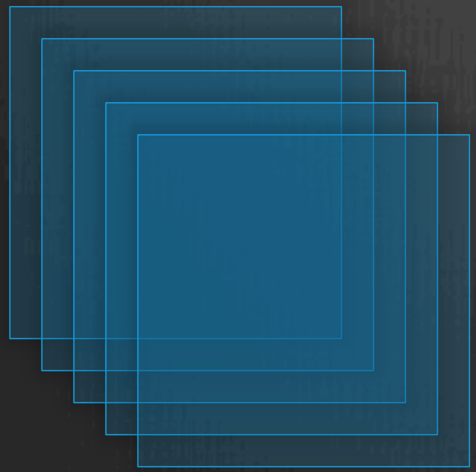
mean-field theory

1-D

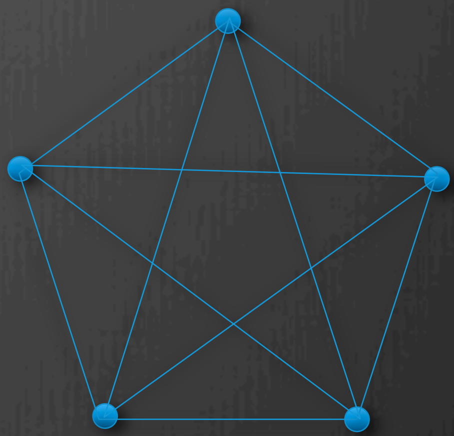
2-D



3-D



∞-D



<u>Folk theorem</u>

high-degree interaction graph

→ symmetric ground state

≈ tensor power ground state

quantum de Finetti theorem

Theorem [Christandl, Koenig, Mitchison, Renner '06]

Given a state $\rho^{AB_1\ldots B_n}$, there exists μ such that

$$\left\| \mathop{\mathbb{E}}_{i_1,\ldots,i_k} \rho^{AB_{i_1}\ldots B_{i_k}} - \int \mu(\mathrm{d}\sigma)\rho_\sigma \otimes \sigma^{\otimes k} \right\|_1 \leq \frac{d^2 k}{n}$$

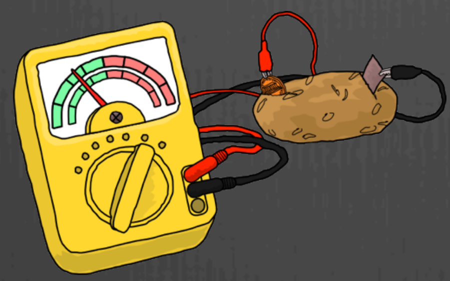
builds on work by [Størmer '69], [Hudson, Moody '76], [Raggio, Werner '89] [Caves, Fuchs, Sachs '01], [Koenig, Renner '05]

Proof idea:

Perform an informationally complete measurement of n-k B systems.

QUANTUM → **measurement** → CLASSICAL

ρ →



$\Pr[1] = \mathrm{tr}\ \rho M_1$ → 1

$\Pr[2] = \mathrm{tr}\ \rho M_2$ → 2

$\Pr[k] = \mathrm{tr}\ \rho M_k$ → k

$\{M_1, \ldots, M_k\}$

<u>Density matrix</u>

$\mathrm{tr}\ \rho = 1$

$\rho \geq 0$

<u>Measurement</u>

$M_1 + \ldots + M_k = I$

$M_i \geq 0, \ \forall i$

M is <u>informationally complete</u> $\Leftrightarrow$ M is injective

information theory tools

1. Mutual information:

$$I(X:Y)_p = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} = D(p^{XY} \| p^X \otimes p^Y)$$

2. Pinsker's inequality:

$$I(X:Y)_p \geq \frac{1}{2 \ln 2} \| p^{XY} - p^X \otimes p^Y \|_1^2$$

3. Conditional mutual information:

$I(X:Y|Z) = I(X:YZ) - I(X:Z)$

4. Chain rule:

$I(X:Y_1 \ldots Y_k) = I(X:Y_1) + I(X:Y_2|Y_1) + \ldots + I(X:Y_k|Y_1 \ldots Y_{k-1})$

→ $I(X:Y_t|Y_1 \ldots Y_{t-1}) \leq \log(|X|)/k$ for some $t \leq k$.

conditioning decouples

Idea that almost works: [c.f. Raghavendra-Tan '11]

1. Choose $i, j_1, \ldots, j_k$ at random from {1, …, n}

Then there exists $t<k$ such that

$$\mathop{\mathbb{E}}_{i,j,j_1,\ldots,j_t} I(X_i : X_j | X_{j_1} \ldots X_{j_t}) \leq \frac{\log(d)}{k}$$

2. Discarding systems $j_1,\ldots,j_t$ causes error $\leq k/n$ and leaves a distribution q for which

$$\mathop{\mathbb{E}}_{i,j} I(X_i : X_j)_q \leq \frac{\log(d)}{k}$$

$$\mathop{\mathbb{E}}_{i\sim j} I(X_i : X_j)_q \leq \frac{n}{D}\frac{\log(d)}{k}$$

$$\mathop{\mathbb{E}}_{i\sim j} \|q^{XY} - q^X \otimes q^Y\|_1 \leq \sqrt{\frac{1}{2\ln 2}\frac{n}{D}\frac{\log(d)}{k}}$$

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.

a physicist

Good news

- $I(A:B)$, $I(A:B|C)$, etc. still defined
- Pinsker, chain rule, etc. still hold
- $I(A:B|C)_\rho = 0 \leftrightarrow \rho$ is separable

Bad news

- Only definition of $I(A:B)_\rho$ is as $H(A)_\rho + H(B)_\rho - H(AB)_\rho$.
- Can't condition on quantum information.
- $I(A:B|C)_\rho \approx 0$ doesn't imply ρ is approximately separable [Ibinson, Linden, Winter '08]

Good news we can use:

Informationally-complete measurement M satisfies

$$d^{-3} \| \rho - \sigma \|_1 \leq \| M(\rho) - M(\sigma) \|_1 \leq \| \rho - \sigma \|_1$$

proof overview

1. Measure εn qudits and condition on outcomes. Incur error ε.

2. Most pairs of other qudits would have mutual information $\leq \log(d) / \varepsilon D$ if measured.

3. ∴ their state is within distance $d^3(\log(d) / \varepsilon D)^{1/2}$ of product.

4. Witness is a global product state. Total error is $\varepsilon + d^3(\log(d) / \varepsilon D)^{1/2}$.
   Choose ε to balance these terms.

other applications

PTAS for Dense k-local Hamiltonians
improves on $1/d^{k-1} + \varepsilon$ approximation from [Gharibian-Kempe '11]

PTAS for planar graphs
Builds on [Bansal, Bravyi, Terhal '07] PTAS for bounded-degree planar graphs

Algorithms for graphs with low threshold rank
Extends result of [Barak, Raghavendra, Steurer '11].
run-time for ε-approximation is
$\exp(\log(n)\ \mathrm{poly}(d/\varepsilon) \cdot \#\{\text{eigs of adj. matrix} \geq \mathrm{poly}(\varepsilon/d)\})$

quantum Lasserre

Previously proposed by [Barthel-Hübener '11], [Baumgartz-Plenio '11] building on [Erdahl '78], [Yasuda-Nakatsuji '97], [Nakatsuji-Yasuda '04], [Mazziotti '04]

$$\operatorname{tr} H\rho = \mathop{\mathbb{E}}_i \operatorname{tr} H_i \rho = \mathop{\mathbb{E}}_i \operatorname{tr} H_i^{S_i} \rho^{S_i}$$

S_i = set of ≤k systems acted on by H_i

First attempt:
Variables are r-body marginals ρ^S with $|S| \le k$.
Enforce consistency constraints on overlapping S_1, S_2.

Global PSD constraint:
For k/2 – local Hermitian operators X, Y, define $\langle X,Y \rangle := \operatorname{tr} \rho XY$.
Require that $\langle \cdot , \cdot \rangle$ be PSD.
(Classical analogue = covariance matrix.)

BRS11 analysis + local measurement ⇒ suffices to take
$r \geq \text{poly}(d/\varepsilon) \cdot \#\{\text{eigs of adj. matrix} \geq \text{poly}(\varepsilon/d)\}$

Open questions

1. <u>The Quantum PCP conjecture!</u>
   Gap amplification, commuting case, thermal states
   Better ansatzes

2. Quantum Lasserre for analogue of unique games?

3. <u>better de Finetti/monogamy-of-entanglement theorems</u>
   hoping to prove
   a) QMA(2 provers, m qubits) ⊆ QMA(1 prover, m^2 qubits)
   b) MIP* ⊆ NEXP. [cf. Ito-Vidick '12]
   c) exp(polylog(n)) algorithm for small-set expansion

de Finetti without symmetry

Theorem [Christandl, Koenig, Mitchison, Renner '05]

Given a state $\rho^{AB_1\ldots B_n}$, there exists μ such that

$$\left\| \mathop{\mathbb{E}}_{i_1,\ldots,i_k} \rho^{AB_{i_1}\ldots B_{i_k}} - \int \mu(\mathrm{d}\sigma)\rho_\sigma \otimes \sigma^{\otimes k} \right\|_1 \leq \frac{d^2 k}{n}$$

Theorem

For ρ a state on $A_1A_2\ldots A_n$ and any $t \leq n-k$, there exists $m \leq t$ such that

$$\mathop{\mathbb{E}}_{i_1,\ldots,i_k} \mathop{\mathbb{E}}_{\substack{j_1,\ldots,j_m \\ a_1,\ldots,a_m}} \left\| \sigma^{A_{i_1}\cdots A_{i_k}} - \sigma^{A_{i_1}} \otimes \cdots \otimes \sigma^{A_{i_k}} \right\|_1 \lesssim \frac{d^k}{n-k}$$

where σ is the state resulting from measuring $j_1,\ldots,j_m$ and obtaining outcomes $a_1,\ldots,a_m$.

QC de Finetti theorems

Idea

Everything works if at most one system is quantum.
Or if all systems are non-signalling (NS) boxes.

Theorem

If ρ^{AB} has an extension $\tilde{\rho}^{AB_1\ldots B_n}$ that is symmetric on the $B_1,\ldots,B_n$ systems, and $\{\Lambda_{A,m}\}_m$ is a distribution over maps with a d-dimensional output, then

$$\min_{\sigma\in\mathrm{Sep(A:B)}} \max_{M_B} \mathbb{E}_m \left\|(\Lambda_{A,m}\otimes M_B)(\rho^{AB}-\sigma^{AB})\right\|_1 \leq \sqrt{\frac{2\ln d}{n}}$$

Corollary [cf Brandao-Christandl-Yard '10]

$$\|\rho^{AB}-\sigma^{AB}\|_{\text{1-LOCC}} \leq \sqrt{\frac{2\ln|A|}{n}}$$

QCC…C de Finetti

Theorem

If $\rho^{A_1,\ldots,A_n}$ is permutation symmetric then for every k there exists μ s.t.

$$\max_{M_2,\ldots,M_k} \left\| (\mathrm{id} \otimes M_2 \otimes \cdots \otimes M_k)(\rho^{A_1\ldots A_k} - \int \mu(\sigma)\sigma^{\otimes k} \right\|_1 \leq \sqrt{\frac{2k^2 \ln |A|}{n-k}}$$

Applications

- QMA = QMA with multiple provers and Bell measurements
- free non-local games are easy
- convergence of sum-of-squares hierarchy for polynomial optimization
- Aaronson's pretty-good tomography with symmetric states