de Finetti theorems
and
PCP conjectures

Aram Harrow (MIT)
DAMTP, 26 Mar 2013

joint work with Fernando Brandão (UCL)
Symmetric States

Let \( \rho_{AB_1 \ldots B_n} \) be a state defined over the subsystems \( A \) and \( B \). It is permutation symmetric in the \( B \) subsystems if for every permutation \( \pi \),

\[
\rho_{AB_1 \ldots B_n} = \rho_{AB_{\pi(1)} \ldots B_{\pi(n)}}
\]

This means that the state does not change under permutations of the \( B \) subsystems. The diagram illustrates the symmetry across the subsystems.

The state can be represented as:

\[
\begin{align*}
\rho_{AB_1 \ldots B_n} & \quad A \quad B_1 \quad B_2 \quad B_{n-1} \quad B_4 \quad B_3 \quad B_n \\
\rho_{AB_1 \ldots B_n} & \quad A \quad B_1 \quad B_2 \quad B_3 \quad B_4 \quad B_{n-1} \quad B_n
\end{align*}
\]

The equality shows that the state is symmetric under permutations of the \( B \) subsystems.
Quantum de Finetti Theorem

**Theorem** [Christandl, Koenig, Mitchison, Renner ‘06]

Given a state $\rho^{AB_1\ldots B_n}$ symmetric under exchange of $B_1\ldots B_n$, there exists $\mu$ such that

$$\left\| \rho^{AB_1\ldots B_k} - \int \mu(d\sigma) \rho_\sigma \otimes \sigma^{\otimes k} \right\|_1 \leq \frac{d^2k}{n}$$

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

**Proof idea:**
Perform an informationally complete measurement of $n-k$ B systems.

**Applications:**
- **information theory:** tomography, QKD, hypothesis testing
- **algorithms:** approximating separable states, mean-field theory
Quantum de Finetti Theorem as Monogamy of Entanglement

**Definition:** $\rho_{AB}$ is **$n$-extendable** if there exists an extension $\rho_{AB_1...B_n}$ with $\rho_{AB} = \rho_{AB_i}$ for each $i$.

- all quantum states (= 1-extendable)
- 2-extendable
- 100-extendable
- separable = $\infty$-extendable

**Algorithms:** Can search/optimize over $n$-extendable states in time $d^{O(n)}$.

**Question:** How close are $n$-extendable states to separable states?
**Quantum de Finetti theorem**

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

Given a state $\rho_{AB_1\ldots B_n}$ symmetric under exchange of $B_1\ldots B_n$, there exists $\mu$ such that

$$
\|\rho^{AB_1\ldots B_k} - \int \mu(d\sigma) \rho_{\sigma} \otimes \sigma^{\otimes k}\|_1 \leq \frac{d^2 k}{n}
$$

**Difficulty:**
1. Parameters are, in many cases, too weak.
2. They are also essentially tight.

**Way forward:**
1. Change definitions (of error or i.i.d.)
2. Obtain better scaling
relaxed/improved versions

Two examples known:

1. **Exponential de Finetti Theorem**: [Renner ’07]
   
   error term \( \exp(-\Omega(n-k)) \).
   
   Target state convex combination of “almost i.i.d.” states.

2. **measure error in 1-LOCC norm**: [Brandão, Christandl, Yard ’10]
   
   For error \( \varepsilon \) and \( k=1 \), requires \( n \sim \varepsilon^{-2} \log|A| \).

**This talk**

improved de Finetti theorems for local measurements
**main idea**

**use information theory**

\[
\log |A| \geq \\
I(A:B_1...B_n) = I(A:B_1) + I(A:B_2|B_1) + ... + I(A:B_n|B_1...B_{n-1})
\]

repeatedly uses chain rule: \( I(A:BC) = I(A:B) + I(A:C|B) \)

\[\Rightarrow I(A:B_1|B_1...B_{t-1}) \leq \log(|A|)/n \text{ for some } t \leq n.\]

If \( B_1...B_n \) were classical, then we would have

\[
\rho_{AB} = \rho_{AB_t} = \sum_i \pi_i \rho_i \approx \text{separable}
\]

\( \approx \)product state (cf. Pinsker ineq.)

**Question:**
How to make \( B_{1...n} \) classical?
Answer: measure!

Fix a measurement $M: B \to Y$.
$I(A: B_t | B_1 \ldots B_{t-1}) \leq \varepsilon$ for the measured state $(\text{id} \otimes M^n)(\rho)$.

Then
- $\rho^{AB}$ is hard to distinguish from $\sigma \in \text{Sep}$ if we first apply $(\text{id} \otimes M)$
- $\| (\text{id} \otimes M)(\rho - \sigma) \| \leq \text{small}$ for some $\sigma \in \text{Sep}$.

**Theorem**
Given a state $\rho^{A B_1 \ldots B_n}$ symmetric under exchange of $B_1 \ldots B_n$, and $\{\Lambda_r\}$ a collection of operations from $A \to X$,

$$\min_{\sigma \in \text{Sep}} \max_M \mathbb{E}_r \| (\Lambda_r^A \otimes M^B) (\rho^{AB} - \sigma^{AB}) \|_1 \leq \sqrt{\frac{2 \ln |X|}{n}}$$

**Cor:** setting $\Lambda = \text{id}$ recovers [Brandão, Christandl, Yard ’10] 1-LOCC result.
\[ \pi XY_1 \ldots Y_n R = \mathbb{E}_{\pi}(A^X \times M^B_1 \times Y_1 \times \ldots \times M^B_n \times Y_n)(\rho^{AB} \times \ldots \times \rho^{AB}) \times |r\rangle\langle r|^{R} \]

\[ \log |X| \geq \max_{M_1, \ldots, M_n} I(X : Y_1 \ldots Y_n | R)_{\pi} \]

\[ = \max_{M_1, \ldots, M_n} \left( I(X : Y_1 | R)_{\pi} + \cdots + I(X : Y_n | Y_1 \ldots Y_{n-1} R)_{\pi} \right) \]

\[ = \max_{M_1, \ldots, M_{n-1}} \left( I(X : Y_1 | R)_{\pi} + \cdots + I(X : Y_{n-1} | Y_1 \ldots Y_{n-2} R)_{\pi} \right) \]

\[ + \max_{M_n} I(X : Y_n | Y_1 \ldots Y_{n-1} R)_{\pi} \]

\[ = \max_{M_n} \mathbb{E}_{r} \mathbb{E}_{y=(y_1, \ldots, y_{n-1})} I(X : Y_n)_{\pi_{r, y}} \]

\[ \geq \max_{M} \mathbb{E}_{r} \mathbb{E}_{y} \frac{1}{2} \left\| (\Lambda^r \otimes M)(\rho^{AB} - \rho^{A|y} \otimes \rho^{B|y}) \right\|_{1}^{2} \]

\[ \geq \min_{\sigma \in \text{Sep}} \max_{M} \mathbb{E}_{r} \frac{1}{2} \left\| (\Lambda^r \otimes M)(\rho^{AB} - \sigma^{AB}) \right\|_{1}^{2} \]
advantages/extensions

**Theorem**

Given a state $\rho^{AB_1\ldots B_n}$ symmetric under exchange of $B_1\ldots B_n$, and $\{\Lambda_r\}$ a collection of operations from $A \rightarrow X$,

\[
\min_{\sigma \in \text{Sep}} \max_{M} \max_{r} \mathbb{E} \left\| (\Lambda_r^A \otimes M^B)(\rho^{AB} - \sigma^{AB}) \right\|_1 \leq \sqrt{\frac{2 \ln |X|}{n}}
\]

1. Simpler proof and better constants
2. Bound depends on $|X|$ instead of $|A|$ (A can be $\infty$-dim)
3. Applies to general non-signalling distributions
4. There is a multipartite version (multiply error by $k$)
5. Efficient “rounding” (i.e. $\sigma$ is explicit)
6. Symmetry isn’t required
applications

• nonlocal games
  Adding symmetric provers “immunizes” against entanglement / non-signalling boxes. (Caveat: needs uncorrelated questions.) Conjectured improvement would yield NP-hardness for 4 players.

• $\text{BellQMA}(\text{poly}) = \text{QMA}$
  Proves Chen-Drucker SAT $\subseteq \text{BellQMA}_{\log(n)}(\sqrt{n})$ protocol is optimal.

• pretty good tomography [Aaronson ’06]
  on permutation-symmetric states (instead of product states)

• convergence of Lasserre hierarchy for polynomial optimization
  see also 1205.4484 for connections to small-set expansion
non-local games

$|\psi\rangle$

Alice

$r$

$x$

$y$

$q$

Bob
non-local games

Non-Local Game $G(\pi, V)$:

$\pi(r, q)$: distribution on $R \times Q$

$V(x, y| r, q)$: predicate on $X \times Y \times R \times Q$

Classical value:

$$\omega_c(G) = \max_{x, y} \mathbb{E}_{(r, q) \sim \pi} V(x(r), y(q)| r, q)$$

Quantum value:

$$\omega_e(G) = \sup_{(r, q) \sim \pi} \mathbb{E} \sum_{x, y} V(x(r), y(q)| r, q) \langle \psi | L_x^r \otimes M_y^q | \psi \rangle$$

$$\sum_x L_x^r = I \quad \sum_y M_y^q = I$$

sup over measurements and $|\psi\rangle$ of unbounded dim
previous results

- [Bell ’64]
  There exist $G$ with $\omega_e(G) > \omega_c(G)$

- PCP theorem [Arora et al ‘98 and Raz ‘98]
  For any $\varepsilon > 0$, it is NP-complete to determine whether
  $\omega_c < \varepsilon$ or $\omega_c > 1 - \varepsilon$ (even for XOR games).

- [Cleve, Høyer, Toner, Watrous ‘04]
  Poly-time algorithm to compute $\omega_e$ for two-player XOR games.

- [Kempe, Kobayashi, Matsumoto, Toner, Vidick ‘07]
  NP-hard to distinguish $\omega_e(G) = 1$ from $\omega_e(G) < 1 - 1/poly(|G|)$

- [Ito-Vidick ‘12 and Vidick ‘13]
  NP-hard to distinguish $\omega_e(G) > 1 - \varepsilon$ from $\omega_e(G) < \frac{1}{2} + \varepsilon$
  for three-player XOR games
immunizing against entanglement
Cor: Let $G(\pi, V)$ be a 2-player free game with questions in $R \times Q$ and answers in $X \times Y$, where $\pi = \pi_R \otimes \pi_Q$. Then there exists an $(n+1)$-player game $G'(\pi', V')$ with questions in $R \times (Q_1 \times \ldots \times Q_n)$ and answers in $X \times (Y_1 \times \ldots \times Y_n)$, such that

$$\omega_c(G) \leq \omega_e(G') \leq \omega_c(G) + \sqrt{\frac{\ln |X|}{2n}}$$

Implies:
1. an $\exp(\log(|X|) \log(|Y|))$ algo for approximating $\omega_c$
2. $\omega_e$ is hard to approximate for free games.
why free games?

**Theorem**
Given a state $\rho^{ABB_1...B_n}$ symmetric under exchange of $B_1...B_n$, and $\{\Lambda_r\}$ a collection of operations from $A \rightarrow X$, 

$$\min_{\sigma \in \text{Sep}} \max_M \mathbb{E}_r \left\| (\Lambda_r^A \otimes M^B) (\rho^{AB} - \sigma^{AB}) \right\|_1 \leq \sqrt{\frac{2 \ln |X|}{n}}$$

$\exists \sigma \forall q$ for most $r$ $\rho$ and $\sigma$ give similar answers

**Conjecture**
Given a state $\rho^{ABB_1...B_n}$ symmetric under exchange of $B_1...B_n$, and $\{\Lambda_r\}$ a collection of operations from $A \rightarrow X$, 

$$\min_{\sigma \in \text{Sep}} \mathbb{E} \max_r \max_M \left\| (\Lambda_r^A \otimes M^B) (\rho^{AB} - \sigma^{AB}) \right\|_1 \leq \sqrt{\frac{2 \ln |X|}{n}}$$

- Would give alternate proof of Vidick result.
- FALSE for non-signalling distributions.
Theorem

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

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

Applications

- QMA = QMA with multiple provers and Bell measurements
- convergence of sum-of-squares hierarchy for polynomial optimization
- Aaronson's pretty-good tomography with symmetric states
de Finetti without symmetry

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

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

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

**Theorem**

For $\rho$ a state on $A_1 A_2 \ldots A_n$ and any $t \leq n - k$, there exists $m \leq t$ such that

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

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

Classical $k$-CSPs:
Given constraints $C=\{C_i\}$, choose an assignment $\sigma$ mapping $n$ variables to an alphabet $\Sigma$ 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 $\text{UNSAT}(C) \geq 0.1$
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 $E_0 = \min_\psi \langle \psi | H | \psi \rangle = \min_\rho \text{tr} \, H \, \rho$

**Hardness**

- Includes $k$-CSPs, so $\pm 0.1$ error is NP-hard by PCP theorem.
- **QMA-complete** with $1/\text{poly(n)}$ 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]
Theorem
It is **NP-complete** to estimate $E_0$ for $n$ qudits on a $D$-regular graph to additive error $\sim d / D^{1/8}$.

Idea: use product states
$E_0 \approx \min \text{ tr } H(\psi_1 \otimes \ldots \otimes \psi_n) - O(d/D^{1/8})$

By contrast
2-CSPs are NP-hard to approximate to error $|\Sigma|^{\alpha/D^\beta}$ for any $\alpha, \beta > 0$
intuition: mean-field theory
Proof of PCP no-go theorem

1. Measure $\varepsilon n$ qudits and condition on outcomes. Incur error $\varepsilon$.

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

3. Thus 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 $\varepsilon$ 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 $\varepsilon$-approximation is
$\exp(\log(n) \cdot \text{poly}(d/\varepsilon) \cdot \#\{\text{eigs of adj. matrix } \geq \text{poly}(\varepsilon/d)\})$
open questions

• Is QMA(2) = QMA? Is $\text{SAT} \in \text{QMA}_{1/\sqrt{n}(2)}^{1,1/2}$ optimal? (Would follow from replacing 1-LOCC with SEP-YES.)

• Can we reorder our quantifiers to get a dimension-independent bound for correlated local measurements?

• (Especially if your name is Graeme Mitchison) Representation theory results $\rightarrow$ de Finetti theorems
What about the other direction?

• The usual de Finetti questions:
  • better counter-examples
  • how much does it help to add PPT constraints?

• The unique games conjecture is $\approx$equivalent to determining whether $\max \{\text{tr } M \rho : \rho \in \text{Sep} \} \geq c_1/d$ or $\leq c_2/d$ for $c_1 \gg c_2 \gg 1$ and $M$ a LO measurement. Can we get an algorithm for this using de Finetti?

• Weak additivity? The Quantum PCP conjecture?

arXiv:1210.6367