Quantum de Finetti theorems under local measurements

Aram Harrow (MIT)
QIP 2013

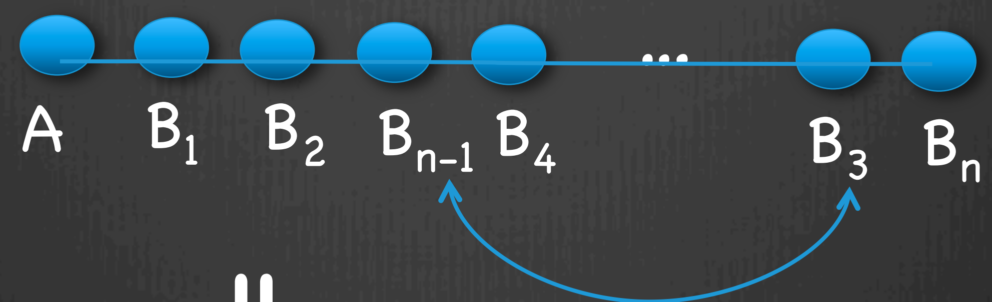
based on arXiv:1210.6367
joint work with Fernando Brandão (ETH)

Symmetric States

$\rho^{AB_1 \ldots B_n}$ is permutation symmetric in the B subsystems if for every permutation π,

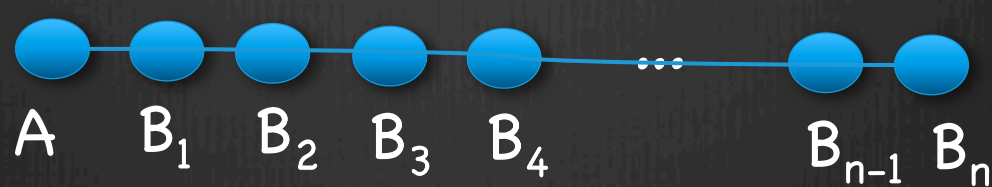
$$\rho^{AB_1 \ldots B_n} = \rho^{AB_{\pi(1)} \ldots B_{\pi(n)}}$$

$\rho^{AB_1 \ldots B_n}$



=

$\rho^{AB_1 \ldots B_n}$



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 μ such that

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

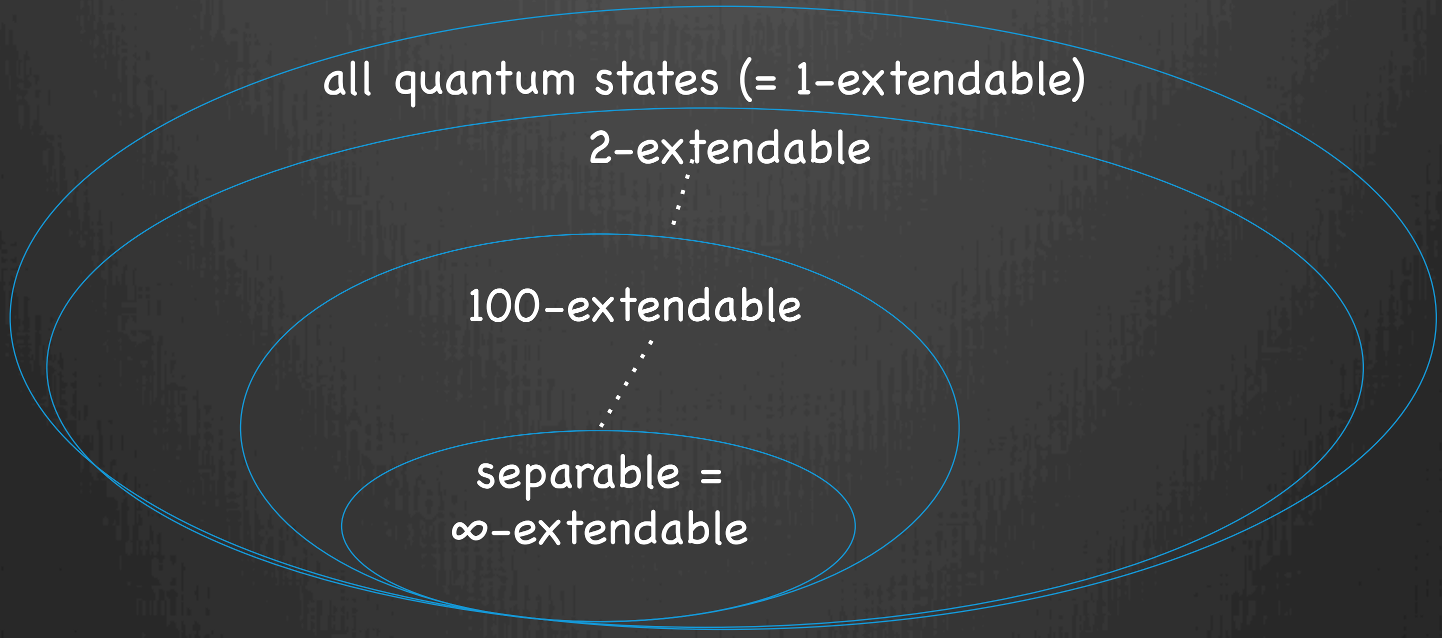
builds on work by [Størmer '69], [Hudson, Moody '76], [Raggio, Werner '89] [Caves, Fuchs, Schack '01], [Koenig, Renner '05]

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: ρ^{AB} is n-extendable if there exists an extension $\rho^{AB_1 \ldots B_n}$ with $\rho^{AB} = \rho^{AB_i}$ for each i.



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 μ such that

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

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 ε 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| ≥
$I(A:B_1 \ldots B_n) = I(A:B_1) + I(A:B_2|B_1) + \ldots + I(A:B_n|B_1 \ldots B_{n-1})$

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

→ $I(A:B_t|B_1 \ldots B_{t-1}) \leq \log(|A|)/n$ for some $t \leq n$.

If $B_1 \ldots B_n$ were classical, then we would have

$$\rho^{AB} = \rho^{AB_t} = \sum_i \pi_i \rho_i^{AB}$$ ≈separable

distribution on $B_1 \ldots B_{t-1}$

≈product state (cf. Pinsker ineq.)

Question:
How to make $B_{1 \ldots n}$ 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 $(\mathrm{id} \otimes M^{\otimes n})(\rho)$.

Then

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

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

$$\min_{\sigma \in \mathrm{Sep}} \max_{M} \mathbb{E}_{i} \left\| (\Lambda_i^A \otimes M^B)(\rho^{AB} - \sigma^{AB}) \right\|_1 \leq \sqrt{\frac{2 \ln |X|}{n}}$$

Cor: setting $\Lambda = \mathrm{id}$ recovers [Brandão, Christandl, Yard '10] 1-LOCC result.

advantages/extensions

Theorem

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

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

1. Simpler proof and better constants
2. Bound depends on |X| instead of |A| (can be ∞ dim)
3. Applies to general non-signalling distributions
4. There is a multipartite version (multiply error by k)
5. Efficient "rounding" (i.e. σ is explicit)
6. Symmetry isn't required (see Fernando's talk on Thursday)

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.

- BellQMA(poly) = QMA
  Proves Chen-Drucker SAT $\in$ $\mathrm{BellQMA}_{\log(n)}(\sqrt{n})$ 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

open questions

- Is QMA(2) = QMA? Is SAT $\in$ QMA$_{\sqrt{n}}(2)_{1,1/2}$ optimal? (Would follow from replacing 1-LOCC with SEP-YES.)
- Can we reorder our quantifiers to obtain

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

(no-signalling analogue is FALSE assuming P≠NP)

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

arXiv:1210.6367