Faithful Squashed Entanglement

with applications to separability testing and quantum Merlin-Arthur games

Fernando G.S.L. Brandão[1]

Matthias Christandl[2]

Jon Yard[3]

1. Universidade Federal de Minas Gerais, Brazil

2. ETH Zürich, Switzerland

3. Los Alamos Laboratory, USA

Mutual Information vs Conditional Mutual Information

Mutual Information: Measures the correlations of **A** and **B** in ρ_{AB}

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$$

Mutual Information vs Conditional Mutual Information

Mutual Information: Measures the correlations of **A** and **B** in ρ_{AB}

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$$

Always positive: $I(A:B)_\rho \geq 0$ (subadditivity of entropy)

Mutual Information vs Conditional Mutual Information

Mutual Information: Measures the correlations of **A** and **B** in ρ_{AB}

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$$

Always positive: $I(A:B)_\rho \geq 0$ (subadditivity of entropy)

When does it vanish? $I(A:B)_\rho = 0$ **iff** $\rho_{AB} = \rho_A \otimes \rho_B$

Mutual Information vs Conditional Mutual Information

Mutual Information: Measures the correlations of **A** and **B** in ρ_{AB}

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$$

Always positive: $I(A:B)_\rho \geq 0$ (subadditivity of entropy)

When does it vanish? $I(A:B)_\rho = 0$ **iff** $\rho_{AB} = \rho_A \otimes \rho_B$

Approximate version? **Pinsker's inequality:**

$$I(A:B) \geq \frac{1}{2\ln 2} \left\| \rho_{AB} - \rho_A \otimes \rho_B \right\|_1^2$$

Remark: **dimension-independent!** Useful in many application in QIT (e.g. decoupling, QKD, …)

Mutual Information vs Conditional Mutual Information

Conditional Mutual Information: Measures the correlations of **A** and **B** relative to **E** in ρ_{ABE}

$$I(A:B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$$

Mutual Information vs Conditional Mutual Information

Conditional Mutual Information: Measures the correlations of **A** and **B** relative to **E** in $\boldsymbol{\rho_{ABE}}$

$$I(A{:}B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$$

Always positive: $I(A{:}B|E)_\rho \geq 0$ (strong-subadditivity of entropy)

(Lieb, Ruskai '73)

Mutual Information vs Conditional Mutual Information

Conditional Mutual Information: Measures the correlations of **A** and **B** relative to **E** in $\boldsymbol{\rho_{ABE}}$

$$I(A{:}B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$$

Always positive: $I(A{:}B|E)_\rho \geq 0$ (strong-subadditivity of entropy)

(Lieb, Ruskai '73)

When does it vanish?

$I(A{:}B|E)_\rho = 0$ **iff** ρ_{ABE} is a **"Quantum Markov Chain State"**

(Hayden, Jozsa, Petz, Winter '04)

E.g. $$\rho_{ABE} = \sum_k p_k \rho_k^A \otimes \rho_k^B \otimes |k\rangle^E \langle k|$$

Mutual Information vs Conditional Mutual Information

Conditional Mutual Information: Measures the correlations of **A** and **B** relative to **E** in ρ_{ABE}

$$I(A:B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$$

Always positive: $I(A:B|E)_\rho \geq 0$ (strong-subadditivity of entropy)

(Lieb, Ruskai '73)

When does it vanish?

$I(A:B|E)_\rho = 0$ **iff** ρ_{ABE} is a **"Quantum Markov Chain State"**

(Hayden, Jozsa, Petz, Winter '04)

E.g. $$\rho_{ABE} = \sum_k p_k \rho_k^A \otimes \rho_k^B \otimes |k\rangle^E \langle k|$$

Approximate version??? ………

Outline

- **I(A:B|E)≈0 (partial) characterization**
- **Applications:**
  - **Squashed Entanglement**
  - **de Finetti-type bounds**
  - **Algorithm for Separability**
  - **A new characterization of QMA**
- **Proof**

No-Go For Approximate Version

A naïve guess for approximate version (à la Pinsker):

$$I(A:B|E) \overset{?}{\geq} \Omega\left(\min_{\sigma=\sum_k p_k \sigma_A^k \otimes \sigma_B^k \otimes |k\rangle_E\langle k|} \left\| \rho_{ABE} - \sigma_{ABE} \right\|_1^2 \right) \geq \Omega\left(\min_{\sigma=\sum_k p_k \sigma_A^k \otimes \sigma_B^k} \left\| \rho_{AB} - \sigma_{AB} \right\|_1^2 \right)$$

No-Go For Approximate Version

A naïve guess for approximate version (à la Pinsker):

$$I(A:B|E) \overset{?}{\geq} \Omega\left(\min_{\sigma=\sum_k p_k \sigma_A^k \otimes \sigma_B^k \otimes |k\rangle_E\langle k|} \left\| \rho_{ABE} - \sigma_{ABE} \right\|_1^2 \right) \geq \Omega\left(\min_{\sigma=\sum_k p_k \sigma_A^k \otimes \sigma_B^k} \left\| \rho_{AB} - \sigma_{AB} \right\|_1^2 \right)$$

|| (left) … **||** (right)

$O(|A|^{-1})$ **It fails badly!** **$\Omega(1)$**

E.g. Antisymmetric Werner state **(Christandl, Schuch, Winter ’08)**

Main Result

Thm: (B., Christandl, Yard '10)

$$I(A:B|E) \geq \Omega\left(\min_{\sigma \in SEP} \left\|\rho_{AB} - \sigma_{AB}\right\|^2\right)$$

Main Result

Thm: (B., Christandl, Yard '10)

$$I(A:B|E) \geq \Omega\left(\min_{\sigma \in SEP} \left\|\rho_{AB} - \sigma_{AB}\right\|^2\right)$$

(Euclidean norm or LOCC norm)

Main Result

Thm: (B., Christandl, Yard '10)

$$I(A:B|E) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\|^2\right)$$

(Euclidean norm or LOCC norm)

The Euclidean (Frobenius) norm: $||X||_2 = \mathrm{tr}(X^T X)^{1/2}$

The trace norm: $||X||_1 = ½ + ½ \max_{0 \leq A \leq I} |\mathrm{tr}(AX)|$

$||\rho-\sigma||_1$: optimal bias

The LOCC norm:

$||X||_{LOCC} = ½ + ½ \max_{0 \leq A \leq I} |\mathrm{tr}(AX)|$: {A, I-A} in LOCC

$||\rho-\sigma||_{LOCC}$: optimal bias by LOCC

The Power of LOCC

Thm: (B., Christandl, Yard '10)

$$I(A:B|E) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\|^2\right)$$

(Euclidean norm or LOCC norm)

(Matthews, Wehner, Winter '09) For X in $A \otimes B$

$$\|X\|_1 \geq \|X\|_{LOCC} \geq \Omega\left(\|X\|_2\right) \geq \Omega\left(\left(|A||B|\right)^{-1/2} \|X\|_1\right)$$

Interesting one, uses a covariant random local measurement

Squashed Entanglement

(Christandl, Winter '04) **Squashed entanglement**:

$E_{sq}(\rho_{AB}) = \inf_\pi \{ \frac{1}{2} I(A:B|E)_\pi \; : \; tr_E(\pi_{ABE}) = \rho_{AB} \}$

Open question: **Is it faithful?**

i.e. Is $E_{sq}(\rho_{AB}) > 0$ for every entangled ρ_{AB}?

Squashed Entanglement

(Christandl, Winter '04) **Squashed entanglement**:

$E_{sq}(\rho_{AB}) = \inf_\pi \{ \frac{1}{2} I(A:B|E)_\pi \; : \; tr_E(\pi_{ABE}) = \rho_{AB} \}$

Open question: **Is it faithful?**

i.e. Is $E_{sq}(\rho_{AB}) > 0$ for every entangled ρ_{AB}?

Corollary: $E_{sq}(\rho_{AB}) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho - \sigma\|_{LOCC}^2 \right)$

Squashed Entanglement

(Christandl, Winter '04) **Squashed entanglement**:

$E_{sq}(\rho_{AB}) = \inf_\pi \{ \tfrac{1}{2} I(A:B|E)_\pi \ : \ tr_E(\pi_{ABE}) = \rho_{AB} \}$

Corollary $$E_{sq}(\rho_{AB}) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho - \sigma\|^2_{LOCC} \right)$$

Proof:

From $$I(A:B|E) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho_{AB} - \sigma_{AB}\|^2_{LOCC} \right)$$

Follows: $$E_{sq}(\rho_{AB}) \geq \Omega\left(\min_{\sigma \in SEP} \|\rho - \sigma\|^2_{LOCC} \right)$$

Entanglement Zoo

Measure	E_{sq}	E_D	K_D	E_C	E_F	E_R	E_R^∞	E_N
normalisation	y	y	y	y	y	y	y	y
faithfulness	y	n	?	y	y	y	y	n
LOCC monotonicity	y	y	y	y	y	y	y	y
asymptotic continuity	y	?	?	?	y	y	y	n
convexity	y	?	?	?	y	y	y	n
strong superadditivity	y	y	y	?	n	n	?	?
subadditivity	y	?	?	y	y	y	y	y
monogamy	y	?	?	n	n	n	n	?

Entanglement Zoo

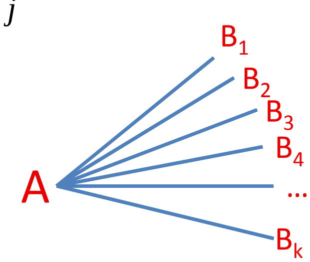
Measure	E_{sq}	E_D	K_D	E_C	E_F	E_R	E_R^∞	E_N
normalisation	y	y	y	y	y	y	y	y
faithfulness	y	n	?	y	y	y	y	n
LOCC monotonicity	y	y	y	y	y	y	y	y
asymptotic continuity	y	?	?	?	y	y	y	n
convexity	y	?	?	?	y	y	y	n
strong superadditivity	y	y	y	?	n	n	?	?
subadditivity	y	?	?	y	y	y	y	y
monogamy	y	?	?	n	n	n	n	?

Entanglement Monogamy

Classical correlations are shareable:

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

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



Separable states are k-extendible for every k.

Entanglement Monogamy

Quantum correlations are non-shareable:

ρ_{AB} separable iff ρ_{AB} k-extendible for all 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 Wernerstate is not *d*-extendible

Entanglement Monogamy

Quantitative version: For any *k*-extendible ρ_{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)

Entanglement Monogamy

Quantitative version: For any k-extendible ρ_{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 a state ρ_{AB} s.t. $\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \geq \Omega\left(\frac{|B|}{k}\right)$
(guess which? ☺)

For other norms ($||*||_2$, $||*||_{LOCC}$, …) no better bound known.

Exponentially Improved de Finetti type bound

Corollary For any k-extendible ρ_{AB}, with $||*||$ equals $||*||_2$ or $||*||_{LOCC}$

$$\min_{\sigma \in SEP} \|\rho - \sigma\| \leq O\left(\frac{\log|A|}{k}\right)^{\frac{1}{2}}$$

Bound proportional to the (square root) of the number of qubits: exponential improvement over previous bound

Exponentially Improved de Finetti type bound

Corollary For any *k*-extendible ρ_{AB}, with $||*||$ equals $||*||_2$ or $||*||_{LOCC}$

$$\min_{\sigma \in SEP} \|\rho - \sigma\| \leq O\left(\frac{\log|A|}{k}\right)^{\frac{1}{2}}$$

Proof: E_{sq} satisfies monogamy relation (Koashi, Winter '05)

$$E_{sq}(\rho_{A:B\bar{B}}) \geq E_{sq}(\rho_{A:B}) + E_{sq}(\rho_{A:\bar{B}})$$

For ρ_{AB} *k*-extendible:

$$\log|A| \geq E_{sq}(\rho_{A:B_1\ldots B_k}) \geq kE_{sq}(\rho_{A:B}) \geq kO\left(\min_{\sigma \in SEP} \|\rho - \sigma\|^2\right)$$

Exponentially Improved de Finetti type bound

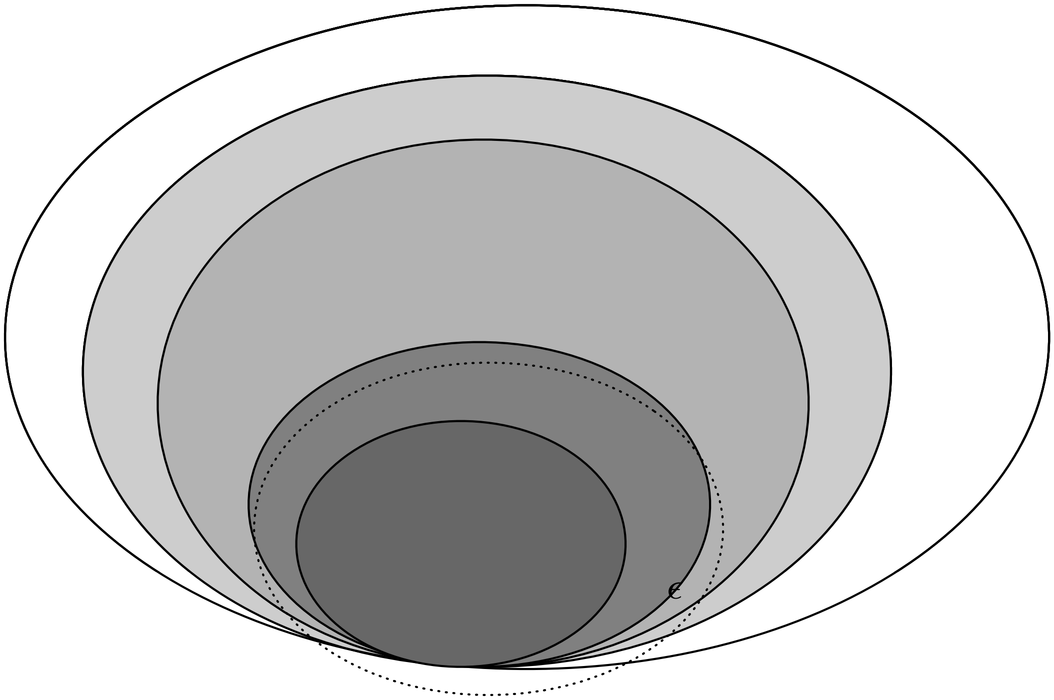
Corollary For any *k*-extendible ρ_{AB}, with $||*||$ equals $||*||_2$ or $||*||_{LOCC}$

$$\min_{\sigma \in SEP} \|\rho - \sigma\| \leq O\left(\frac{\log|A|}{k}\right)^{\frac{1}{2}}$$

(Close-to-Optimal) There is *k*-extendible state ρ_{AB} s.t.

$$\min_{\sigma \in SEP} \|\rho - \sigma\|_{LOCC} \geq \Omega\left(\frac{\log|A|}{k}\right)$$

Exponentially Improved de Finetti type bound



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

Hardness results:

(Gurvits '02) NP-hard with $\varepsilon=1/\exp((|A||B|)^{1/2})$

(Gharibian '08, Beigi '08) NP-hard with $\varepsilon=1/\mathrm{poly}((|A||B|)^{1/2})$

(Beigi&Shor '08) Favorite separability tests fail

(Harrow&Montanaro '10) No $\exp(O(|A|^{1-\nu}|A|^{1-\mu}))$ time algorithm for membership in any convex set within $\varepsilon=\Omega(1)$ trace distance to SEP and any $\nu+\mu>0$, unless ETH fails

ETH (Exponential Time Hypothesis): SAT cannot be solved in $2^{o(n)}$ time (Impagliazzo&Paruti '99)

Quasi-polynomial Algorithm

Corollary There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for deciding separability (in $||*||_2$ or $||*||_{LOCC}$)

Quasi-polynomial Algorithm

Corollary There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for deciding separability (in $||*||_2$ or $||*||_{LOCC}$)

The idea (Doherty, Parrilo, Spedalieri '04)

Search for a $k=O(\log|A|/\varepsilon^2)$ extension of ρ_{AB} by SDP

$$\exists \ \pi_{AB_1,\ldots,B_k} \geq 0 : \pi_{AB_j} = \rho_{AB} \quad \forall \quad j \in [k]$$

Complexity SDP of size

$|A|^2|B|^{2k} = \exp(O(\varepsilon^{-2}\log|A|\log|B|))$

Quasi-polynomial Algorithm

Corollary There is a $\exp(O(\varepsilon^{-2}\log|A|\log|B|))$ time algorithm for deciding separability (in $||*||_2$ or $||*||_{LOCC}$)

NP-hardness for $\varepsilon = 1/\text{poly}(d)$ is shown using $||*||_2$

From corollary: the problem in $||*||_2$ cannot be NP-hard for $\varepsilon = 1/\text{polylog}(d)$, unless ETH fails

Best Separable State Problem

BSS(ε) Problem: Given X, approximate $\max_{|a\rangle,|b\rangle} \langle a,b|X|a,b\rangle$ to additive error ε

Corollary There is a $\exp(O(\varepsilon^{-2} \log|A| \log|B| (||X||_2)^2))$ time algorithm for BSS(ε)

Best Separable State Problem

BSS(ε) Problem: Given X, approximate $\max_{|a\rangle,|b\rangle} \langle a,b|X|a,b\rangle$ to additive error ε

Corollary There is a $\exp(O(\varepsilon^{-2} \log|A| \log|B| (||X||_2)^2))$ time algorithm for BSS(ε)

The idea Optimize over $k=O(\log|A|\varepsilon^{-2}(||X||_2)^2)$ extension of ρ_{AB} by SDP

$$\min_{\pi} tr(\pi X) : \pi_{AB_1,\ldots,B_k} \geq 0, \quad \pi_{AB_j} = \rho_{AB} \quad \forall \quad j \in [k]$$

Best Separable State Problem

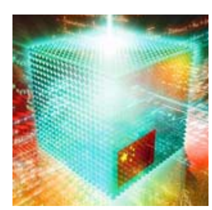
BSS(ε) Problem: Given X, approximate $\max_{|a\rangle,|b\rangle} \langle a,b|X|a,b\rangle$ to additive error ε

Corollary There is a $\exp(O(\varepsilon^{-2} \log|A| \log|B| (||X||_2)^2))$ time algorithm for BSS(ε)

(Harrow and Montanaro '10): BSS(ε) for $\varepsilon=\Omega(1)$ and $||X||_\infty \leq 1$ cannot be solved in $\exp(O(\log^{1-\nu}|A| \log^{1-\mu}|B|))$ time for any $\nu + \mu > 0$ unless ETH fails

QMA

$|\Psi\rangle$



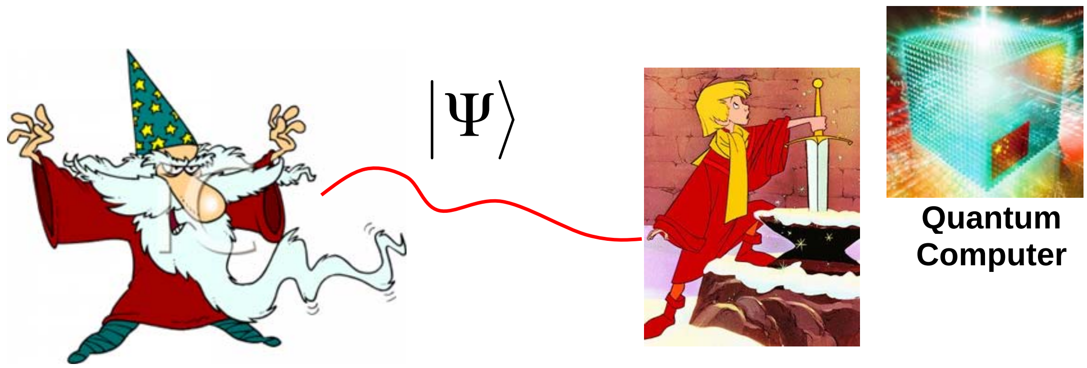
Quantum Computer

A language **L** is in QMA if for every x in **L**:

QMA:

- YES instance: Merlin can convince Arthur with probability > 2/3

QMA



A language **L** is in QMA if for every x in **L**:

QMA:
- YES instance: Merlin can convince Arthur with probability > 2/3
- NO instance: Merlin cannot convince Arthur with probability > 1/3

QMA

- Quantum analogue of NP (or MA)
- Local Hamiltonian Problem, …

Is QMA a robust complexity class?

(Aharonov, Regev ‘03) superverifiers doesn’t help

(Marriott, Watrous ‘05) Exponential amplification with fixed proof size

(Beigi, Shor, Watrous ‘09) logarithmic size interaction doesn’t help

New Characterization QMA

Corollary QMA doesn't change allowing k = O(1) different proofs if the verifier can only apply LOCC measurements in the k proofs

New Characterization QMA

Corollary QMA doesn't change allowing k = O(1) different proofs if the verifier can only apply LOCC measurements in the k proofs

Def $QMA_m(k)$: analogue of QMA with k proofs and proof size m

New Characterization QMA

Corollary QMA doesn't change allowing $k = O(1)$ different proofs if the verifier can only apply LOCC measurements in the k proofs

Def $QMA_m(k)$: analogue of QMA with k proofs and proof size m

Def $LOCCQMA_m(k)$: analogue of QMA with k proofs, proof size m and LOCC verification procedure along the k proofs.

New Characterization QMA

Corollary **$QMA = LOCCQMA(k)$, $k = O(1)$**

$LOCCQMA_m(2)$ contained in $QMA_{O(m^2)}$

Contrast: **$QMA_m(2)$ not in $QMA_{O(m^{2-\delta})}$**

for any $\delta>0$ unless Quantum ETH* fails

(Harrow and Montanaro '10) -- based on Aaronson et al '08

And: **SAT has a $LOCCQMA_{O(\log(n))}(n^{0.5})$ protocol**

(Chen and Drucker '10)

* Quantum ETH: SAT cannot be solved in $2^{o(n)}$ quantum time

New Characterization QMA

Corollary QMA = LOCCQMA(k), k = O(1)

$LOCCQMA_m(2)$ contained in $QMA_{O(m^2)}$

Idea to simulate $LOCCQMA_m(2)$ in QMA:

- Arthur asks for proof ρ on $AB_1B_{2\ldots}B_k$ with $k = m\varepsilon^{-2}$
- He symmetrizes the *B* systems and applies the original verification prodedure to AB_1

Correcteness

de Finetti bound implies: $\min_{\sigma \in SEP} \left\| \rho_{AB_1} - \sigma \right\|_{LOCC} \leq \sqrt{\frac{m}{k}} = \varepsilon$

Proof

Relative Entropy of Entanglement

The proof is largely based on the properties of a *different* entanglement measure:

Def Relative Entropy of Entanglement (Vedral, Plenio '99)

$$E_R^\infty(\rho_{AB}) := \lim_{n\to\infty} \frac{E_R(\rho_{AB}^{\otimes n})}{n} \qquad E_R(\rho_{AB}) := \min_{\sigma \in SEP} S(\rho \| \sigma)$$

$$S(\rho \| \sigma) := tr(\rho(\log \rho - \log \sigma))$$

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB}, what's the optimal probability of distinguishing it from a separable state?

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB}, what's the optimal probability of distinguishing it from a separable state?

Def Rate Function: $D(\rho_{AB})$ is maximum number r s.t. there exists $\{M_n, I-M_n\}$, $0 < M_n < I$,

$$\min_{\sigma \in SEP} tr(M_n \sigma) \leq 2^{-nr}, \quad tr(M \rho_{AB}^{\otimes n}) \geq \Omega(1)$$

$D_{LOCC}(\rho_{AB})$: defined analogously, but now {M, I-M} must be LOCC

Entanglement Hypothesis Testing

Given (many copies) of ρ_{AB}, what's the optimal probability of distinguishing it from a separable state?

Def Rate Function: $D(\rho_{AB})$ is maximum number r s.t there exists $\{M_n, I-M_n\}$, $0 < M_n < I$,

$$\min_{\sigma \in SEP} tr(M_n \sigma) \leq 2^{-nr}, \quad tr(M \rho_{AB}^{\otimes n}) \geq \Omega(1)$$

$D_{LOCC}(\rho_{AB})$: defined analogously, but now {M, I-M} must be LOCC

(B., Plenio '08) $D(\rho_{AB}) = E_R^{\infty}(\rho_{AB})$

Obs: *Equivalent* to reversibility of entanglement under non-entangling operations

Proof in 1 Line

$$I(A:B|E)_{\rho_{ABE}} \overset{(i)}{\geq} E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \overset{(ii)}{\geq} D_{LOCC}(\rho_{A:B}) \overset{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \|\rho_{A:B} - \sigma\|_{LOCC}^2\right)$$

Proof in 1 Line

$$I(A:B|E)_{\rho_{ABE}} \overset{(i)}{\geq} E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \overset{(ii)}{\geq} D_{LOCC}(\rho_{A:B}) \overset{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \|\rho_{A:B} - \sigma\|_{LOCC}^2\right)$$

Relative entropy of Entanglement plays a triple role:

(i) Quantum Shannon Theory: State redistribution Protocol
(Devetak and Yard '07)

(ii) Large Deviation Theory: Entanglement Hypothesis Testing
(B. and Plenio '08)

(iii) Entanglement Theory: Faithfulness bounds

First Inequality

$$I(A:B|E)_{\rho_{ABE}} \overset{(i)}{\geq} E_R^{\infty}(\rho_{A:BE}) - E_R^{\infty}(\rho_{A:E})$$

Non-lockability: $E_R(\rho_{A:BE}) \leq E_R(\rho_{A:E}) + 2\log|B|$

(Horodecki[3] and Oppenheim '04)

State Redistribution: How much does it cost to redistribute a quantum system? ½ I(A:B|E)

A | BE | F ⟶ A | E | BF $\qquad |\psi\rangle_{A:BE:F}^{\otimes n} \rightarrow |\psi\rangle_{A:E:BF}^{\otimes n}$

Proof (i):

Apply non-lockability to $\rho_{A:BE}^{\otimes n}$ and use state redistribution to trace out B at a rate of ½ I(A:B|E) qubits per copy

Second Inequality

$$E_R^{\infty}(\rho_{A:BE}) - E_R^{\infty}(\rho_{A:E}) \overset{(ii)}{\geq} D_{LOCC}(\rho_{A:B})$$

Equivalent to: $D(\rho_{A:BE}) \geq D(\rho_{A:E}) + D_{LOCC}(\rho_{A:B})$

Monogamy relation for entanglement hypothesis testing

Proof (ii)

Use optimal measurements for ρ_{AE} and ρ_{AB} achieving $D(\rho_{AE})$ and $D_{LOCC(1)}(\rho_{AB})$, resp., to construct a measurement for $\rho_{A:BE}$ achieving $D(\rho_{A:BE})$

Third Inequality

$$D_{LOCC}(\rho_{A:B}) \overset{(iii)}{\geq} \Omega\left(\min_{\sigma \in SEP} \left\| \rho_{A:B} - \sigma \right\|_{LOCC}^2 \right)$$

Pinsker type inequality for entanglement hypothesis testing

Proof (iii)

minimax theorem + martingale like property of the set of separable states

Summary

- New Pinsker type lower bound for I(A:B|E) and E_{sq}
- LOCC norm is fundamental
- Testing separability is rather easy
- QMA is (once more) robust
- Entanglement measures rulez

Open Problems

- Can we prove a lower bound on I(A:B|E) in terms of distance to "markov quantum chain states"?
- Can we close the LOCC norm vs. trace norm gap in the results? (hardness vs. algorithm, LOCCQMA(k) vs QMA(k))
- Are there more applications of the bound on the convergence of the SDP relaxation?
- Can we put new problems in QMA using QMA = LOCCQMA(k)?
- Are there more application of the main inequality?

Thank you!