Faithful Squashed Entanglement
with applications to separability testing and quantum Merlin-Arthur games

Fernando G.S.L. Brandão¹
Matthias Christandl²
Jon Yard³

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 $\rho_{AB}$

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$$
Mutual Information vs Conditional Mutual Information

**Mutual Information**: Measures the correlations of $A$ and $B$ in $\rho_{AB}$

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

**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 $\rho_{AB}$

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

**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:

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

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

---

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

\[
I(A:B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho
\]
Mutual Information vs Conditional Mutual Information

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

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

**Always positive**: \( I(A:B|E)_{\rho} \geq 0 \) (strong-subadditivity of entropy)  
(Lieb, Ruskai ’73)

**When does it vanish?**

\[
I(A:B|E)_{\rho} = 0 \text{ iff } \rho_{ABE} \text{ is a “Quantum Markov Chain State”}
\]
(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 \( \rho_{ABE} \)

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

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

**When does it vanish?**

\[
I(A:B|E)_\rho = 0 \text{ iff } \rho_{ABE} \text{ is a “Quantum Markov Chain State”}
\]

(Lieb, Ruskai ‘73)

**E.g.** \( \rho_{ABE} = \sum_k p_k \rho^A_k \otimes \rho^B_k \otimes |k⟩⟨k|_E \)

Outline

- \( I(A:B|E) \approx 0 \) (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):

$$I(A : B | E) \geq \Omega \left( \min_{\sigma = \sum p_k \sigma_i^A \otimes \sigma_j^B \otimes |k\rangle \langle k|} \| \rho_{ABE} - \sigma_{ABE} \|_1^2 \right) \geq \Omega \left( \min_{\sigma = \sum p_k \sigma_i^A \otimes \sigma_j^B} \| \rho_{AB} - \sigma_{AB} \|_1^2 \right)$$

It fails badly!

$O(|A|^{-1})$ \hspace{1cm} $\Omega(1)$

E.g. Antisymmetric Werner state \hspace{1cm} (Christandl, Schuch, Winter ’08)
Main Result

Thm: (B., Christandl, Yard ’10)

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

(Euclidean norm or LOCC norm)
Main Result

**Thm: (B., Christandl, Yard ’10)**

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

(Euclidean norm or LOCC norm)

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

The trace norm: \[ \| X \|_1 = \frac{1}{2} + \frac{1}{2} \max_{0 \leq A \leq I} | \text{tr}(AX) | \]

\[ \| \rho - \sigma \|_1 : \text{optimal bias} \]

The LOCC norm:

\[ \| X \|_{\text{LOCC}} = \frac{1}{2} + \frac{1}{2} \max_{0 \leq A \leq I} | \text{tr}(AX) | : \{ A, I-A \} \text{ in LOCC} \]

\[ \| \rho - \sigma \|_{\text{LOCC}} : \text{optimal bias by LOCC} \]

The Power of LOCC

**Thm: (B., Christandl, Yard ’10)**

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

(Euclidean norm or LOCC norm)

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

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

**Interesting one, uses a covariant random local measurement**
(Christandl, Winter ‘04) Squashed entanglement:

\[ E_{sq}(\rho_{AB}) = \inf_\pi \left\{ \frac{1}{2} I(A:B|E)_\pi : \text{tr}_E(\pi_{ABE}) = \rho_{AB} \right\} \]

Open question: Is it faithful? i.e. Is \( E_{sq}(\rho_{AB}) > 0 \) for every entangled \( \rho_{AB} \)?

Corollary:

\[ E_{sq}(\rho_{AB}) \geq \Omega \left( \min_{\sigma \in \text{SEP}} \left\| \rho - \sigma \right\|_{LOCC}^2 \right) \]
Squashed Entanglement

(Christandl, Winter ’04) Squashed entanglement:

\[ E_{sq}(\rho_{AB}) = \inf_{\pi} \left\{ \frac{1}{2} I(A:B|E)_{\pi} : \text{tr}_E(\pi_{AB}) = \rho_{AB} \right\} \]

**Corollary**

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

**Proof:**

From

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

Follows:

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

Entanglement Zoo

<table>
<thead>
<tr>
<th>Measure</th>
<th>( E_{sq} )</th>
<th>( E_D )</th>
<th>( K_D )</th>
<th>( E_C )</th>
<th>( E_F )</th>
<th>( E_R )</th>
<th>( E_R^\infty )</th>
<th>( E_N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>normalisation</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>faithfulness</td>
<td>y</td>
<td>n</td>
<td>?</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>LOCC monotonicity</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>asymptotic continuity</td>
<td>y</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>convexity</td>
<td>y</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>strong superadditivity</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>?</td>
<td>n</td>
<td>n</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>subadditivity</td>
<td>y</td>
<td>?</td>
<td>?</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>monogamy</td>
<td>y</td>
<td>?</td>
<td>?</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>?</td>
</tr>
</tbody>
</table>
## Entanglement Zoo

<table>
<thead>
<tr>
<th>Measure</th>
<th>$E_{sq}$</th>
<th>$E_D$</th>
<th>$K_D$</th>
<th>$E_C$</th>
<th>$E_F$</th>
<th>$E_R$</th>
<th>$E_R^\infty$</th>
<th>$E_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>normalisation</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>y</td>
</tr>
<tr>
<td>faithfulness</td>
<td>℣</td>
<td>n</td>
<td>℣</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>LOCC monotonicity</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>y</td>
</tr>
<tr>
<td>asymptotic continuity</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>n</td>
</tr>
<tr>
<td>convexity</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>y</td>
</tr>
<tr>
<td>strong superadditivity</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>℣</td>
</tr>
<tr>
<td>subadditivity</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>y</td>
</tr>
<tr>
<td>monogamy</td>
<td>℣</td>
<td>℣</td>
<td>℣</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>℣</td>
</tr>
</tbody>
</table>

### Def. $\rho_{AB}$ is $k$-extendible if there is $\rho_{AB_1...B_k}$

s.t for all $j$ in $[k]$ $\text{tr}_{B_j}(\rho_{AB_1...B_k}) = \rho_{AB}$

Separable states are $k$-extendible for every $k$.  

### Entanglement Monogamy

Classical correlations are shareable:

$$\sigma_{AB_1,...,B_k} = \sum_j p_j \sigma_{A,j} \otimes \sigma_{B,j}$$
Entanglement Monogamy

Quantum correlations are non-shareable:
\[ \rho_{AB} \text{ separable iff } \rho_{AB} \text{ k-extendible for all } k \]

- 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 \( d \times d \) antisymmetric Werner state is not \( d \)-extendible

Quantitative version: For any \( k \)-extendible \( \rho_{AB} \),
\[ \min_{\sigma \in \text{SEP}} \| \rho - \sigma \|_1 \leq O\left( \frac{|B|^2}{k} \right) \]

- Follows from: **finite quantum de Finetti Theorem** (Christandl, König, Mitchson, Renner ‘05)
Entanglement Monogamy

Quantitative version: For any $k$-extendible $\rho_{AB}$,

$$\min_{\sigma \in SEP} \|\rho - \sigma\|_1 \leq O\left(\frac{|B|^2}{k}\right)$$

- Follows from: finite quantum de Finetti Theorem (Christandl, König, Mitchson, Renner ‘05)

Close to optimal: there is a state $\rho_{AB}$ 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 $\rho_{AB}$, 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 $\rho_{AB}$, with $\|*\|$ equals $\|*\|_2$ or $\|*\|_{\text{LOCC}}$

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

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

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

For $\rho_{AB}$ $k$-extendible:

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

Exponentially Improved de Finetti type bound

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

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

(Close-to-Optimal) There is $k$-extendible state $\rho_{AB}$ s.t.

$$\min_{\sigma \in \text{SEP}} \|\rho - \sigma\|_{\text{LOCC}} \geq \Omega\left(\frac{\log |A|}{k}\right)$$
Exponentially Improved de Finetti type bound

The Separability Problem

When is $\rho_{AB}$ entangled?
- Decide if $\rho_{AB}$ is separable or $\epsilon$-away from separable

Beautiful theory behind it (PPT, entanglement witnesses, symmetric extensions, etc)

Horribly expensive algorithms

State-of-the-art: $2^{O(|A| \log (1/\epsilon))}$ time complexity

(Doherty, Parrilo, Spedalieri ‘04)
The Separability Problem

When is $\rho_{AB}$ entangled?
- Decide if $\rho_{AB}$ is separable or $\varepsilon$-away from separable

**Hardness results:**

- (Gurvits ’02) NP-hard with $\varepsilon=1/\exp(|A| |B|^{1/2})$
- (Gharibian ’08, Beigi ’08) NP-hard with $\varepsilon=1/\text{poly}(|A| |B|^{1/2})$
- (Beigi&Shor ’08) Favorite separability tests fail
- (Harrow&Montanaro ’10) No $\exp(O(|A|^{-\nu} |A|^{-\mu}))$ 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 \( \|*\|_{\text{LOCC}} \))

**The idea** (Doherty, Parrilo, Spedalieri ’04)

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

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

**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 \( \|*\|_{\text{LOCC}} \))

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 $\epsilon$.

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

---

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

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

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

(Harrow and Montanaro ’10): BSS(ε) for $\epsilon=\Omega(1)$ 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**

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 \( L \):
- YES instance: Merlin can convince Arthur with probability \( > \frac{2}{3} \)
- NO instance: Merlin cannot convince Arthur with probability \( > \frac{1}{3} \)

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

**Def** $\text{QMA}_m(k)$: 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** \( \text{QMA}_m(k) \): analogue of QMA with \( k \) proofs and proof size \( m \)

**Def** \( \text{LOCCQMA}_m(k) \): analogue of QMA with \( k \) proofs, proof size \( m \) and LOCC verification procedure along the \( k \) proofs.

**New Characterization QMA**

**Corollary** \[ \text{QMA} = \text{LOCCQMA}(k), \quad k = O(1) \]

\( \text{LOCCQMA}_m(2) \) contained in \( \text{QMA}_{O(m^2)} \)

**Contrast:** \( \text{QMA}_m(2) \) not in \( \text{QMA}_{O(m^{2-\delta})} \)

for any \( \delta > 0 \) unless Quantum ETH* fails

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

**And:** SAT has a \( \text{LOCCQMA}_{O(\log(n))}(n^{0.5}) \) protocol

(Chen and Drucker ’10)

* Quantum ETH: SAT cannot be solved in \( 2^{o(n)} \) quantum time
New Characterization QMA

Corollary \( \text{QMA} = \text{LOCCQMA}(k), \quad k = O(1) \)

\( \text{LOCCQMA}_m(2) \) contained in \( \text{QMA}_{O(m^2)} \)

Idea to simulate \( \text{LOCCQMA}_m(2) \) in QMA:

- Arthur asks for proof \( \rho \) on \( AB_1B_2...B_k \) with \( k = m\epsilon^{-2} \)
- He symmetrizes the \( B \) systems and applies the original verification procedure to \( AB_1 \)

Correcteness

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

Proof
Relative Entropy of Entanglement

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

\[
E_R^\infty(\rho_{AB}) := \lim_{n \to \infty} \frac{E_R(\rho_{AB}^\otimes n)}{n} \quad E_R(\rho_{AB}) := \min_{\sigma \in SEp} S(\rho \| \sigma)
\]

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

Entanglement Hypothesis Testing

Given (many copies) of \(\rho_{AB}\), what’s the optimal probability of distinguishing it from a separable state?
Entanglement Hypothesis Testing

Given (many copies) of $\rho_{AB}$, 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

\[ I(A : B \mid E)_{\rho_{ABE}} \geq E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \geq D_{\text{LOCC}}(\rho_{A:B}) \geq \Omega \left( \min_{\sigma \in \text{SEP}} \| \rho_{A:B} - \sigma \|_{\text{LOCC}}^2 \right) \]

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

\[ I(A : B | E)_{\rho_{ABE}}^{(i)} \geq E^\infty_R(\rho_{A:BE}) - E^\infty_R(\rho_{A:E}) \]

Non-lockability: \[ E^\infty_R(\rho_{A:BE}) \leq E^\infty_R(\rho_{A:E}) + 2 \log |B| \]

(Horodecki\(^3\) and Oppenheim ‘04)

State Redistribution: How much does it cost to redistribute a quantum system? \( \frac{1}{2} I(A:B|E) \)

\[ \begin{array}{c|c|c} & A & E \rightarrow A \mid BF \\ \hline & \psi^{\otimes n}_{A:B:E:F} \rightarrow \psi^{\otimes n}_{A:E:BF} \end{array} \]

Proof (i):
Apply non-lockability to \( \rho^{\otimes n}_{A:BE} \) and use state redistribution to trace out B at a rate of \( \frac{1}{2} I(A:B|E) \) qubits per copy

Second Inequality

\[ E^\infty_R(\rho_{A:BE}) - E^\infty_R(\rho_{A:E})^{(ii)} \geq D_{LOCC}(\rho_{A:B}) \]

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 \( \rho_{AE} \) and \( \rho_{AB} \) achieving \( D(\rho_{AE}) \) and \( D_{LOCC}(\rho_{AB}) \), resp., to construct a measurement for \( \rho_{A:BE} \) achieving \( D(\rho_{A:BE}) \)
Third Inequality

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

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!