Soundness gap amplification of $\mathrm{QMA}(2)$ protocols by parallel repetition

The possible role of de Finetti reductions and entanglement measure theory

Based on arXiv:1605.09013, joint work with Andreas Winter

Cécilia Lancien

Université Claude Bernard Lyon 1 & Universitat Autónoma de Barcelona

$\mathrm{QMA}(2)$ Workshop - QuICS - August 4th 2016

QMA(2) protocols and related problems

A verifier requires states α, β from two (unentangled) provers and performs a binary POVM (M^+, M^-) on the state $\alpha \otimes \beta$. The provers pass the test iff the verifier obtains outcome $+$.
$\rightarrow$ **Goal of the provers :** Maximize their passing probability $\mathrm{Tr}(M^+ \alpha \otimes \beta)$.

QMA(2) protocols and related problems

A verifier requires states α, β from two (unentangled) provers and performs a binary POVM (M^+, M^-) on the state $\alpha \otimes \beta$. The provers pass the test iff the verifier obtains outcome $+$.
$\rightarrow$ **Goal of the provers :** Maximize their passing probability $\mathrm{Tr}(M^+ \alpha \otimes \beta)$.

Equivalent formulation : Given a Hermitian M on $\mathrm{A} \otimes \mathrm{B}$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$, determine its maximum overlap with $\mathcal{S}(\mathrm{A:B})$, the set of separable states on $\mathrm{A} \otimes \mathrm{B}$, i.e.

$$h_{sep}(M) := \max_{\sigma \in \mathcal{S}(\mathrm{A:B})} \mathrm{Tr}(M\sigma).$$

Remark : In the case where $M = VV^*$ for $V : \mathrm{C} \hookrightarrow \mathrm{A} \otimes \mathrm{B}$ an isometry, define the quantum channel $\mathcal{N} : \rho \in \mathcal{D}(\mathrm{C}) \mapsto \mathrm{Tr}_{\mathrm{B}}(V\rho V^*) \in \mathcal{D}(\mathrm{A})$. Then,

$$S_\infty^{\min}(\mathcal{N}) = -\log h_{sep}(M), \text{ where } S_\infty^{\min}(\mathcal{N}) := \min_{\rho \in \mathcal{D}(\mathrm{C})} -\log \|\mathcal{N}(\rho)\|_\infty.$$

QMA(2) protocols and related problems

A verifier requires states α, β from two (unentangled) provers and performs a binary POVM (M^+, M^-) on the state $\alpha \otimes \beta$. The provers pass the test iff the verifier obtains outcome $+$.
$\rightarrow$ **Goal of the provers :** Maximize their passing probability $\mathrm{Tr}(M^+ \alpha \otimes \beta)$.

Equivalent formulation : Given a Hermitian M on $\mathrm{A} \otimes \mathrm{B}$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$, determine its maximum overlap with $\mathcal{S}(\mathrm{A{:}B})$, the set of separable states on $\mathrm{A} \otimes \mathrm{B}$, i.e.

$$h_{sep}(M) := \max_{\sigma \in \mathcal{S}(\mathrm{A:B})} \mathrm{Tr}(M\sigma).$$

Remark : In the case where $M = VV^*$ for $V : \mathrm{C} \hookrightarrow \mathrm{A} \otimes \mathrm{B}$ an isometry, define the quantum channel $\mathcal{N} : \rho \in \mathcal{D}(\mathrm{C}) \mapsto \mathrm{Tr}_{\mathrm{B}}(V\rho V^*) \in \mathcal{D}(\mathrm{A})$. Then,

$$S_\infty^{\min}(\mathcal{N}) = -\log h_{sep}(M), \text{ where } S_\infty^{\min}(\mathcal{N}) := \min_{\rho \in \mathcal{D}(\mathrm{C})} -\log \|\mathcal{N}(\rho)\|_\infty.$$

Many other related problems (Harrow/Montanaro) :

- Determine $\|\psi\|_{\mathrm{inj}}$ for $\psi \in \mathrm{A} \otimes \mathrm{B} \otimes \mathrm{C}$ s.t. $\|\psi\|_2 \leqslant 1$, i.e. $\max_{\alpha \in \mathrm{A}, \beta \in \mathrm{B}, \gamma \in \mathrm{C}} \dfrac{\langle \psi | \alpha \otimes \beta \otimes \gamma \rangle}{\|\alpha\|_2 \|\beta\|_2 \|\gamma\|_2}$.
- Determine $\|T\|_{2\to 4}$ for $T : \mathrm{C} \to \mathrm{A} \otimes \mathrm{B}$ s.t. $\|T\|_\infty \leqslant 1$, i.e. $\max_{\varphi \in \mathrm{C}} \dfrac{\|T\varphi\|_4}{\|\varphi\|_2}$.

Parallel repetition of QMA(2) protocols

If two provers cannot pass 1 instance of a given test with probability 1, does their probability of passing simultaneously n instances of it go to 0 exponentially with n ?
More generally, does their probability of passing t amongst the n instances already decay exponentially as soon as t/n is larger than their 1-instance passing probability ?
And if so, at which rate ?

Parallel repetition of QMA(2) protocols

If two provers cannot pass 1 instance of a given test with probability 1, does their probability of passing simultaneously n instances of it go to 0 exponentially with n ?
More generally, does their probability of passing t amongst the n instances already decay exponentially as soon as t/n is larger than their 1-instance passing probability ?
And if so, at which rate ?

Equivalent question : Does h_{sep}, resp. $S_\infty^{\min}$, exhibit a multiplicative, resp. additive, behavior under tensoring ?
Clearly, for any $n \in \mathbf{N}$, $(h_{sep}(M))^n \leqslant h_{sep}(M^{\otimes n}) \leqslant h_{sep}(M)$, but what is the true asymptotic behavior of $h_{sep}(M^{\otimes n})$ as $n \to +\infty$?

Parallel repetition of $\mathrm{QMA}(2)$ protocols

If two provers cannot pass 1 instance of a given test with probability 1, does their probability of passing simultaneously n instances of it go to 0 exponentially with n ?
More generally, does their probability of passing t amongst the n instances already decay exponentially as soon as t/n is larger than their 1-instance passing probability ?
And if so, at which rate ?

Equivalent question : Does h_{sep}, resp. $S_\infty^{\min}$, exhibit a multiplicative, resp. additive, behavior under tensoring ?
Clearly, for any $n \in \mathbf{N}$, $(h_{sep}(M))^n \leqslant h_{sep}(M^{\otimes n}) \leqslant h_{sep}(M)$, but what is the true asymptotic behavior of $h_{sep}(M^{\otimes n})$ as $n \to +\infty$?

Known : In general, h_{sep} is strictly super-multiplicative (Holevo/Werner).
However, all known extreme examples s.t. $h_{sep}(M^{\otimes 2}) \simeq h_{sep}(M) \gg (h_{sep}(M))^2$, namely M projector onto either the anti-symmetric subspace (Grudka/Horodecki/Pankowski) or a random subspace (Hayden/Winter), are also s.t. $h_{sep}(M^{\otimes n}) \leqslant (h_{sep}(M))^{\lambda n}$, for some $0 < \lambda < 1$ (Christandl/Schuch/Winter, Montanaro).
$\to$ Does such multiplicativity without dimensional dependence actually hold for any M ?

If this were true : Possibility of amplifying the soundness gap of any $\mathrm{QMA}(2)$ protocol from δ to $1 - e^{-\delta\lambda n}$ by performing it n times in parallel.

Outline

1. Multiplicativity of h_{sep} under tensoring via de Finetti approach
2. Multiplicativity of h_{sep} under tensoring via entanglement measure approach
3. Further comments and generalizations

Outline

1. Multiplicativity of h_{sep} under tensoring via de Finetti approach
2. Multiplicativity of h_{sep} under tensoring via entanglement measure approach
3. Further comments and generalizations

De Finetti reductions (aka Post-selection techniques)

Motivation : Reduce the study of an exchangeable scenario to that of i.i.d. ones, in a setting where being able to upper bound a permutation-invariant object by product ones is enough.

De Finetti reductions (aka Post-selection techniques)

Motivation : Reduce the study of an exchangeable scenario to that of i.i.d. ones, in a setting where being able to upper bound a permutation-invariant object by product ones is enough.

Theorem [Universal quantum de Finetti reduction (Christandl/König/Renner)]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{|\mathrm{H}|^2} \int_\sigma \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

De Finetti reductions (aka Post-selection techniques)

Motivation : Reduce the study of an exchangeable scenario to that of i.i.d. ones, in a setting where being able to upper bound a permutation-invariant object by product ones is enough.

Theorem [Universal quantum de Finetti reduction (Christandl/König/Renner)]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{|\mathrm{H}|^2} \int_\sigma \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

Drawback : All permutation-invariant states are upper bounded by the same mixture of tensor power states. $\rightarrow$ Any additional information on $\rho^{(n)}$ is lost.

De Finetti reductions (aka Post-selection techniques)

Motivation : Reduce the study of an exchangeable scenario to that of i.i.d. ones, in a setting where being able to upper bound a permutation-invariant object by product ones is enough.

Theorem [Universal quantum de Finetti reduction (Christandl/König/Renner)]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{|\mathrm{H}|^2} \int_\sigma \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

Drawback : All permutation-invariant states are upper bounded by the same mixture of tensor power states. $\rightarrow$ Any additional information on $\rho^{(n)}$ is lost.

Theorem [Flexible quantum de Finetti reduction]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{3|\mathrm{H}|^2} \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

De Finetti reductions (aka Post-selection techniques)

Motivation : Reduce the study of an exchangeable scenario to that of i.i.d. ones, in a setting where being able to upper bound a permutation-invariant object by product ones is enough.

Theorem [Universal quantum de Finetti reduction (Christandl/König/Renner)]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{|\mathrm{H}|^2} \int_\sigma \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

Drawback : All permutation-invariant states are upper bounded by the same mixture of tensor power states. $\to$ Any additional information on $\rho^{(n)}$ is lost.

Theorem [Flexible quantum de Finetti reduction]

Let $\rho^{(n)}$ be a permutation-invariant state on $\mathrm{H}^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{3|\mathrm{H}|^2} \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\mu(\sigma), \quad \mu : \text{uniform p.d. over the set of states on } \mathrm{H}.$$

Advantage : State-dependent upper bound. $\to$ Amongst states of the form $\sigma^{\otimes n}$, only those which have a high fidelity with $\rho^{(n)}$ (hence “similar properties”) are given an important weight.

Filtered by measurements distance measures

M a set of POVMs, $\mathcal{K}$ a set of states on H.
For any state ρ on H, its measured by **M** fidelity and trace-norm distance to $\mathcal{K}$ are

$$F_{\mathbf{M}}(\rho,\mathcal{K}) := \sup_{\sigma\in\mathcal{K}} \inf_{\mathcal{M}\in\mathbf{M}} F\left(\mathcal{M}(\rho),\mathcal{M}(\sigma)\right) \text{ and } \|\rho-\mathcal{K}\|_{\mathbf{M}} := \inf_{\sigma\in\mathcal{K}} \sup_{\mathcal{M}\in\mathbf{M}} \left\|\mathcal{M}(\rho)-\mathcal{M}(\sigma)\right\|_1 .$$

Observation : $F_{\mathbf{ALL}}(\rho,\mathcal{K}) = F(\rho,\mathcal{K})$ and $\|\rho-\mathcal{K}\|_{\mathbf{ALL}} = \|\rho-\mathcal{K}\|_1$.

Relationship between both : $1-F_{\mathbf{M}}(\rho,\mathcal{K}) \leqslant \frac{1}{2}\|\rho-\mathcal{K}\|_{\mathbf{M}} \leqslant \left(1-F_{\mathbf{M}}(\rho,\mathcal{K})^2\right)^{1/2}$.

Filtered by measurements distance measures

M a set of POVMs, $\mathcal{K}$ a set of states on H.
For any state ρ on H, its measured by **M** fidelity and trace-norm distance to $\mathcal{K}$ are

$$F_{\mathbf{M}}(\rho,\mathcal{K}) := \sup_{\sigma\in\mathcal{K}} \inf_{\mathcal{M}\in\mathbf{M}} F(\mathcal{M}(\rho),\mathcal{M}(\sigma)) \text{ and } \|\rho-\mathcal{K}\|_{\mathbf{M}} := \inf_{\sigma\in\mathcal{K}} \sup_{\mathcal{M}\in\mathbf{M}} \left\|\mathcal{M}(\rho)-\mathcal{M}(\sigma)\right\|_1 .$$

Observation : $F_{\mathbf{ALL}}(\rho,\mathcal{K}) = F(\rho,\mathcal{K})$ and $\|\rho-\mathcal{K}\|_{\mathbf{ALL}} = \|\rho-\mathcal{K}\|_1$.

Relationship between both : $1 - F_{\mathbf{M}}(\rho,\mathcal{K}) \leqslant \frac{1}{2}\|\rho-\mathcal{K}\|_{\mathbf{M}} \leqslant \left(1-F_{\mathbf{M}}(\rho,\mathcal{K})^2\right)^{1/2}$.

Theorem [Distinguishing power of separable POVMs]

For any Hermitian Δ on $\mathrm{A}\otimes\mathrm{B}$, we have

$$\|\Delta\|_{\mathbf{SEP}(\mathrm{A:B})} \geqslant \|\Delta\|_2 .$$

Theorem [Weakly multiplicative behavior of $F(\cdot,\mathcal{S})$ under tensoring]

For any state ρ on $\mathrm{A}\otimes\mathrm{B}$, we have

$$F\left(\rho^{\otimes n},\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)\right) \leqslant F_{\mathbf{SEP}(\mathrm{A:B})}\left(\rho,\mathcal{S}(\mathrm{A:B})\right)^n .$$

Multiplicativity of h_{sep} under tensoring

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$, and set $r := \|M\|_2$. Then,

$$h_{sep}(M) \leqslant 1-\delta \;\Rightarrow\; \forall\, n\in\mathbf{N},\; h_{sep}(M^{\otimes n}) \leqslant \left(1-\frac{\delta^2}{5r^2}\right)^n \leqslant \left(1-\frac{\delta^2}{5|\mathrm{A}||\mathrm{B}|}\right)^n .$$

Multiplicativity of h_{sep} under tensoring

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant \mathrm{Id}$, and set $r:=\|M\|_2$. Then,

$$h_{sep}(M)\leqslant 1-\delta \ \Rightarrow\ \forall\, n\in\mathbf{N},\ h_{sep}(M^{\otimes n})\leqslant\left(1-\frac{\delta^2}{5r^2}\right)^n\leqslant\left(1-\frac{\delta^2}{5|\mathrm{A}||\mathrm{B}|}\right)^n.$$

Main steps in the proof :

Let $\rho\in\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)$, w.l.o.g. permutation-invariant so that $\rho\leqslant \mathrm{poly}(n)\int_\sigma F\left(\rho,\sigma^{\otimes n}\right)^2\sigma^{\otimes n}\,\mathrm{d}\mu(\sigma)$.
Hence, $\mathrm{Tr}\left(M^{\otimes n}\rho\right)\leqslant \mathrm{poly}(n)\displaystyle\int_\sigma F\left(\rho,\sigma^{\otimes n}\right)^2\mathrm{Tr}(M\sigma)^n\,\mathrm{d}\mu(\sigma)$.
Fix $0<\varepsilon<1$ and set $\mathcal{K}_\varepsilon:=\{\sigma\ :\ \|\sigma-\mathcal{S}(\mathrm{A}{:}\mathrm{B})\|_2\leqslant\varepsilon/r\}$.
Then, $\sigma\in\mathcal{K}_\varepsilon\ \Rightarrow\ \mathrm{Tr}(M\sigma)\leqslant 1-\delta+\varepsilon$ and $\sigma\notin\mathcal{K}_\varepsilon\ \Rightarrow\ F\left(\rho,\sigma^{\otimes n}\right)^2\leqslant\left(1-\varepsilon^2/4r^2\right)^n$.
Thus, $\mathrm{Tr}\left(M^{\otimes n}\rho\right)\leqslant\mathrm{poly}(n)\left((1-\delta+\varepsilon)^n+\left(1-\varepsilon^2/4r^2\right)^n\right)$.
So choosing $\varepsilon=2r^2\left((1+\delta/r^2)^{1/2}-1\right)$, we get $h_{sep}(M^{\otimes n})\leqslant\mathrm{poly}(n)\left(1-\delta^2/5r^2\right)^n$.

To remove the polynomial pre-factor :
Assume that $\exists\ N\in\mathbf{N}, C>0:\ h_{sep}(M^{\otimes N})\geqslant C\left(1-\delta^2/5r^2\right)^N$.
Then, $\forall\ n\in\mathbf{N}$, $h_{sep}\left(M^{\otimes Nn}\right)\geqslant C^n\left(1-\delta^2/5r^2\right)^{Nn}$ and $h_{sep}\left(M^{\otimes Nn}\right)\leqslant\mathrm{poly}(Nn)\left(1-\delta^2/5r^2\right)^{Nn}$.
$C\leqslant 1$ is the only option to make these two inequalities compatible as $n\to+\infty$.

Is the relaxation to filtered by measurements quantities truly needed to get multiplicativity ?

Question : Does there exist a universal function f s.t., for any state ρ on $\mathrm{A}\otimes\mathrm{B}$,

$$F\big(\rho,\mathcal{S}(\mathrm{A{:}B})\big) \leqslant 1-\delta \;\Rightarrow\; \forall\, n\in\mathbf{N},\; F\big(\rho^{\otimes n},\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)\big) \leqslant (1-f(\delta))^n \text{ ?}$$

Is the relaxation to filtered by measurements quantities truly needed to get multiplicativity ?

Question : Does there exist a universal function f s.t., for any state ρ on $\mathrm{A}\otimes\mathrm{B}$,

$$F\big(\rho,\mathcal{S}(\mathrm{A}{:}\mathrm{B})\big)\leqslant 1-\delta \;\Rightarrow\; \forall\, n\in\mathbf{N},\; F\big(\rho^{\otimes n},\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)\big)\leqslant (1-f(\delta))^n \;?$$

Known :

- Perfect multiplicativity of $F(\cdot,\mathcal{S})$ for pure states.
- Dimension-free multiplicativity of $F(\cdot,\mathcal{S})$ for the anti-symmetric state (Christandl/Schuch/Winter).
  $\rightarrow$ Does it generalize to any entangled Werner state ?

Is the relaxation to filtered by measurements quantities truly needed to get multiplicativity ?

Question : Does there exist a universal function f s.t., for any state ρ on $\mathrm{A}\otimes\mathrm{B}$,

$$F\big(\rho,\mathcal{S}(\mathrm{A{:}B})\big)\leqslant 1-\delta \;\Rightarrow\; \forall\, n\in\mathbf{N},\; F\big(\rho^{\otimes n},\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)\big)\leqslant (1-f(\delta))^n \text{ ?}$$

Known :

- Perfect multiplicativity of $F(\cdot,\mathcal{S})$ for pure states.
- Dimension-free multiplicativity of $F(\cdot,\mathcal{S})$ for the anti-symmetric state (Christandl/Schuch/Winter).
  $\to$ Does it generalize to any entangled Werner state ?

Would be enough : If this were true w.h.p. for uniformly distributed mixed states...
Difficulty : Understanding properties of random tensor power states is hard, because they form a random matrix model with less invariances and less concentration (cf. Ambainis/Harrow/Hastings).

Outline

1. Multiplicativity of h_{sep} under tensoring via de Finetti approach
2. Multiplicativity of h_{sep} under tensoring via entanglement measure approach
3. Further comments and generalizations

Squashed entanglement

Squashed entanglement (Christandl/Winter) :

$$E_{sq}(\rho_{\mathrm{AB}}) := \inf\left\{ \frac{1}{2} I(\mathrm{A}{:}\mathrm{B}|\mathrm{E})_\rho \ : \ \mathrm{Tr}_{\mathrm{E}}(\rho_{\mathrm{ABE}}) = \rho_{\mathrm{AB}} \right\}$$

Theorem [Weak faithfulness property of squashed entanglement (Li/Winter)]

For any state ρ on $\mathrm{A}\otimes\mathrm{B}$ and any $\varepsilon \geqslant 0$, we have

$$E_{sq}(\rho) \leqslant \varepsilon \ \Rightarrow \ \|\rho - \mathcal{S}(\mathrm{A}{:}\mathrm{B})\|_1 \leqslant (128 \ln 2)^{1/4} \min(|\mathrm{A}|, |\mathrm{B}|)\, \varepsilon^{1/4}.$$

Squashed entanglement

Squashed entanglement (Christandl/Winter) :

$$E_{sq}(\rho_{AB}) := \inf\left\{ \frac{1}{2} I(A{:}B|E)_\rho \ : \ \mathrm{Tr}_E(\rho_{ABE}) = \rho_{AB} \right\}$$

Theorem [Weak faithfulness property of squashed entanglement (Li/Winter)]

For any state ρ on $A\otimes B$ and any $\varepsilon \geqslant 0$, we have

$$E_{sq}(\rho) \leqslant \varepsilon \ \Rightarrow\ \|\rho - \mathcal{S}(A{:}B)\|_1 \leqslant (128\ln 2)^{1/4} \min(|A|,|B|)\,\varepsilon^{1/4}.$$

Theorem [Disturbance induced by a global measurement on a product state]

Let M_{AB} be a Hermitian on $A\otimes B$, satisfying $0 \leqslant M_{AB} \leqslant \mathrm{Id}$, and let $\alpha_{A^n}, \beta_{B^n}$ be states on $A^{\otimes n}, B^{\otimes n}$ respectively. Next, fix $1 \leqslant k \leqslant n-1$, and define

$$p_k := \mathrm{Tr}_{A^nB^n}\left[M_{AB}^{\otimes k}\otimes \mathrm{Id}_{AB}^{\otimes n-k}\,\alpha_{A^n}\otimes\beta_{B^n}\right],\ \tau^{(k)}_{A^{n-k}B^{n-k}} := \frac{1}{p_k}\mathrm{Tr}_{A^kB^k}\left[M_{AB}^{\otimes k}\otimes \mathrm{Id}_{AB}^{\otimes n-k}\,\alpha_{A^n}\otimes\beta_{B^n}\right].$$

Then, $\displaystyle\sum_{j=k+1}^{n} E_{sq}\left(\tau^{(k)}_{A_jB_j}\right) \leqslant \frac{1}{2}\log\frac{1}{p_k}$.

Multiplicativity of h_{sep} under tensoring

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$. Then,

$$h_{sep}(M) \leqslant 1-\delta \Rightarrow \forall\, n\in\mathbf{N},\ h_{sep}\left(M^{\otimes n}\right) \leqslant \left(1-\frac{\delta^4}{512\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4}\right)^n.$$

Multiplicativity of h_{sep} under tensoring

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant \mathrm{Id}$. Then,

$$h_{sep}(M)\leqslant 1-\delta \Rightarrow \forall\, n\in\mathbf{N},\ h_{sep}\left(M^{\otimes n}\right)\leqslant\left(1-\frac{\delta^4}{512\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4}\right)^n.$$

Main steps in the proof :

Let $\rho\in\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)$, w.l.o.g. of the form $\alpha_{\mathrm{A}^n}\otimes\beta_{\mathrm{B}^n}$.
Set $p_0=1$, $\tau^{(0)}_{\mathrm{A}^n\mathrm{B}^n}=\alpha_{\mathrm{A}^n}\otimes\beta_{\mathrm{B}^n}$. Then, given $I_k\subset[n]$ s.t. $|I_k|=k$, define $M^{(I_k)}_{\mathrm{A}^n\mathrm{B}^n}:=M_{\mathrm{AB}}^{\otimes I_k}\otimes\mathrm{Id}_{\mathrm{AB}}^{\otimes I_k^c}$,
and build recursively $p_k=\mathrm{Tr}_{\mathrm{A}^n\mathrm{B}^n}\left[M^{(I_k)}_{\mathrm{A}^n\mathrm{B}^n}\alpha_{\mathrm{A}^n}\otimes\beta_{\mathrm{B}^n}\right]$, $\tau^{(k)}_{\mathrm{A}_{I_k^c}\mathrm{B}_{I_k^c}}=\mathrm{Tr}_{\mathrm{A}_{I_k}\mathrm{B}_{I_k}}\left[M^{(I_k)}_{\mathrm{A}^n\mathrm{B}^n}\alpha_{\mathrm{A}^n}\otimes\beta_{\mathrm{B}^n}\right]/p_k$,
where $I_k=I_{k-1}\cup\{i_k\}$ with i_k chosen in I_{k-1}^c s.t. $E_{sq}\left(\tau^{(k-1)}_{\mathrm{A}_{i_k}\mathrm{B}_{i_k}}\right)\leqslant\frac{1}{n-k+1}\,\frac{1}{2}\log\frac{1}{p_{k-1}}$.

The p_k's are related by the recursion formula $p_{k+1}=p_k\,\mathrm{Tr}_{\mathrm{A}_{i_{k+1}}\mathrm{B}_{i_{k+1}}}\left(M_{\mathrm{A}_{i_{k+1}}\mathrm{B}_{i_{k+1}}}\tau^{(k)}_{\mathrm{A}_{i_{k+1}}\mathrm{B}_{i_{k+1}}}\right)$.
So $p_{k+1}\leqslant p_k\left[\left(\frac{128\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4}{n-k}\log\frac{1}{p_k}\right)^{1/4}+h_{sep}(M_{\mathrm{AB}})\right]$.
It follows that $\mathrm{Tr}\left(M_{\mathrm{AB}}^{\otimes n}\alpha_{\mathrm{A}^n}\otimes\beta_{\mathrm{B}^n}\right)=p_n\leqslant\left(1-\frac{(1-h_{sep}(M_{\mathrm{AB}}))^4}{512\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4}\right)^n$.

In search of a "'magical" measure of entanglement (cf. Aaronson/Beigi/Drucker/Fefferman/Shor)

Question : Does there exist a measure of entanglement E satisfying the two properties :

1. $E(\rho_{\mathrm{A:B}}) + E(\rho_{\mathrm{A':B'}}) \leqslant I(\mathrm{AA'}:\mathrm{BB'})_\rho$ (monogamy-type),
2. $E(\rho) \leqslant \varepsilon \Rightarrow \|\rho - \mathcal{S}(\mathrm{A:B})\|_1 \leqslant g(\varepsilon)$, with g a universal function (strong faithfulness) ?

The existence of such "'magical" measure of entanglement E would imply that, for any Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$,

$$h_{sep}(M) \leqslant 1-\delta \Rightarrow \forall\, n \in \mathbf{N},\ h_{sep}(M^{\otimes n}) \leqslant \left(1 - \frac{g^{-1}(\delta)}{4}\right)^n .$$

In search of a "'magical" measure of entanglement (cf. Aaronson/Beigi/Drucker/Fefferman/Shor)

Question : Does there exist a measure of entanglement E satisfying the two properties :

1. $E(\rho_{A:B}) + E(\rho_{A':B'}) \leqslant I(AA':BB')_\rho$ (monogamy-type),
2. $E(\rho) \leqslant \varepsilon \Rightarrow \|\rho - \mathcal{S}(A:B)\|_1 \leqslant g(\varepsilon)$, with g a universal function (strong faithfulness) ?

The existence of such "'magical" measure of entanglement E would imply that, for any Hermitian M on $A \otimes B$, satisfying $0 \leqslant M \leqslant \mathrm{Id}$,

$$h_{sep}(M) \leqslant 1 - \delta \Rightarrow \forall\, n \in \mathbf{N},\ h_{sep}(M^{\otimes n}) \leqslant \left(1 - \frac{g^{-1}(\delta)}{4}\right)^n.$$

Difficulty : Monogamy and faithfulness are two features of entanglement measures which usually exclude one another (Adesso/Di Martino/Huber/Lancien/Piani/Winter)

Candidate : Conditional entanglement of mutual information (Horodecki/Wang/Yang)

$$E_I(\rho_{AB}) := \inf\left\{ \frac{1}{2}\left(I(AA':BB')_\rho - I(A':B')_\rho \right) \ :\ \mathrm{Tr}_{A'B'}(\rho_{ABA'B'}) = \rho_{AB} \right\}$$

E_I satisfies (1), like E_{sq}, and may satisfy (2), unlike E_{sq}. To show the latter : make use of "small conditional mutual information $\Rightarrow$ existence of good recovery map"... ?

Outline

1. Multiplicativity of h_{sep} under tensoring via de Finetti approach
2. Multiplicativity of h_{sep} under tensoring via entanglement measure approach
3. Further comments and generalizations

Cases where these results are already interesting as they are

Cases where these results are already interesting as they are

- **De Finetti approach :**

  For any Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, we have

$$\forall\, n\in\mathbf{N},\ h_{sep}(M^{\otimes n})\leqslant\left(1-\frac{(1-h_{sep}(M))^2}{5\,\mathrm{rk}(\mathrm{M})}\right)^n.$$

$\rightarrow$ Interesting for low-rank M's.

Cases where these results are already interesting as they are

- **De Finetti approach :**

  For any Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, we have

$$\forall\, n\in\mathbf{N},\ h_{sep}(M^{\otimes n})\leqslant\left(1-\frac{(1-h_{sep}(M))^2}{5\,\mathrm{rk}(\mathrm{M})}\right)^n.$$

  $\rightarrow$ Interesting for low-rank M's.

- **Entanglement measure approach :**

  For each $q\in\mathbf{N}$, denote by $\mathcal{E}_q(\mathrm{A{:}B})$ the set of q-extendible states on $\mathrm{A}\otimes\mathrm{B}$. We know that

$$E_{sq}(\rho)\leqslant\varepsilon\ \Rightarrow\ \forall\, q\in\mathbf{N},\ \|\rho-\mathcal{E}_q(\mathrm{A{:}B})\|_1\leqslant q\sqrt{2\ln 2\,\varepsilon}.$$

  Consequently, for any Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, for each $q\in\mathbf{N}$, we have

$$\forall\, n\in\mathbf{N},\ h_{sep}\left(M^{\otimes n}\right)\leqslant\left(1-\frac{(1-h_{q-ext}(M))^2}{8\ln 2\, q^2}\right)^n.$$

  $\rightarrow$ Interesting for M's s.t. $h_{q-ext}(M)\simeq h_{sep}(M)$ for small q's.

Concentration bound

Question : What is the probability that the two unentangled provers pass at least t amongst the n instances of the test that the verifier is subjecting them to ?

Equivalently, given a Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant \mathrm{Id}$, how does $h_{sep}\left(M^{(t/n)}\right)$ behave, where $M^{(t/n)} := \sum_{I\subset[n],|I|\geqslant t} M^{\otimes I}\otimes(\mathrm{Id}-M)^{\otimes I^c}$?

Clearly, if $t/n < h_{sep}(M)$, then $h_{sep}\left(M^{(t/n)}\right)$ is asymptotically 1. But what about the case $t/n > h_{sep}(M)$, does $h_{sep}\left(M^{(t/n)}\right)$ go exponentially to 0 with n, like in the extreme case $t=n$?

Concentration bound

Question : What is the probability that the two unentangled provers pass at least t amongst the n instances of the test that the verifier is subjecting them to ?
Equivalently, given a Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant \mathrm{Id}$, how does $h_{sep}\left(M^{(t/n)}\right)$ behave, where $M^{(t/n)}:=\sum_{I\subset[n],|I|\geqslant t} M^{\otimes I}\otimes(\mathrm{Id}-M)^{\otimes I^c}$?

Clearly, if $t/n<h_{sep}(M)$, then $h_{sep}\left(M^{(t/n)}\right)$ is asymptotically 1. But what about the case $t/n>h_{sep}(M)$, does $h_{sep}\left(M^{(t/n)}\right)$ go exponentially to 0 with n, like in the extreme case $t=n$?

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant \mathrm{Id}$. If $h_{sep}(M)\leqslant 1-\delta$, then for any $n,t\in\mathbf{N}$ s.t. $t\geqslant(1-\delta+\alpha)n$, we have

$$h_{sep}\left(M^{(t/n)}\right)\leqslant \exp\left(-n\frac{\alpha^2}{5|\mathrm{A}||\mathrm{B}|}\right) \text{ and } h_{sep}\left(M^{(t/n)}\right)\leqslant\left(1-\frac{\alpha^5}{2048\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4(2\delta-\alpha)}\right)^n.$$

Concentration bound

Question : What is the probability that the two unentangled provers pass at least t amongst the n instances of the test that the verifier is subjecting them to ?
Equivalently, given a Hermitian M on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant\mathrm{Id}$, how does $h_{sep}\left(M^{(t/n)}\right)$ behave, where $M^{(t/n)} := \sum_{I\subset[n],|I|\geqslant t} M^{\otimes I}\otimes(\mathrm{Id}-M)^{\otimes I^c}$?

Clearly, if $t/n < h_{sep}(M)$, then $h_{sep}\left(M^{(t/n)}\right)$ is asymptotically 1. But what about the case $t/n > h_{sep}(M)$, does $h_{sep}\left(M^{(t/n)}\right)$ go exponentially to 0 with n, like in the extreme case $t=n$?

Theorem

Let M be a Hermitian on $\mathrm{A}\otimes\mathrm{B}$, satisfying $0\leqslant M\leqslant\mathrm{Id}$. If $h_{sep}(M)\leqslant 1-\delta$, then for any $n,t\in\mathbf{N}$ s.t. $t\geqslant(1-\delta+\alpha)n$, we have

$$h_{sep}\left(M^{(t/n)}\right)\leqslant\exp\left(-n\frac{\alpha^2}{5|\mathrm{A}||\mathrm{B}|}\right) \text{ and } h_{sep}\left(M^{(t/n)}\right)\leqslant\left(1-\frac{\alpha^5}{2048\ln 2\,\min(|\mathrm{A}|,|\mathrm{B}|)^4(2\delta-\alpha)}\right)^n.$$

Key ingredients in the proofs :

- **De Finetti reduction approach :** Hoeffding's inequality.
- **Entanglement measure approach :** Conditioned on the event "the provers have already passed k instances of the test", the probability is high that they do not pass in most (and not just 1) of the $n-k$ remaining instances.

Multiplicativity under tensoring of support functions of other sets of states

Sequence of convex sets of states $\mathcal{K}^{(n)}$ on $\mathrm{H}^{\otimes n}$, $n \in \mathbf{N}$, s.t.

$$\mathcal{K}^{(n)} \supset \left(\mathcal{K}^{(1)}\right)^{\hat{\otimes} n} := \mathrm{conv}\left\{\rho_1 \otimes \cdots \otimes \rho_n \ : \ \rho_1, \ldots, \rho_n \in \mathcal{K}^{(1)}\right\}.$$

Assumptions : Stability under permutation and partial trace.

Simplest example : $\mathcal{K}$ set of states on H, and for each $n \in \mathbf{N}$, $\mathcal{K}^{(n)} = \mathcal{K}^{\hat{\otimes} n}$.

Multiplicativity under tensoring of support functions of other sets of states

Sequence of convex sets of states $\mathcal{K}^{(n)}$ on $\mathrm{H}^{\otimes n}$, $n \in \mathbf{N}$, s.t.

$$\mathcal{K}^{(n)} \supset \left(\mathcal{K}^{(1)}\right)^{\hat{\otimes} n} := \mathrm{conv}\left\{\rho_1 \otimes \cdots \otimes \rho_n \ : \ \rho_1, \ldots, \rho_n \in \mathcal{K}^{(1)}\right\}.$$

Assumptions : Stability under permutation and partial trace.

Simplest example : $\mathcal{K}$ set of states on H, and for each $n \in \mathbf{N}$, $\mathcal{K}^{(n)} = \mathcal{K}^{\hat{\otimes} n}$.

In that case, (quantitative) equivalence between the multiplicative behavior under tensoring of (a) the maximum fidelity function $F\left(\cdot, \mathcal{K}^{(n)}\right)$ and (b) the support function $h_{\mathcal{K}^{(n)}}(\cdot)$.

- To show $(a) \Rightarrow (b)$: use the flexible de Finetti reduction.
- To show $(b) \Rightarrow (a)$: design a discrimination test whose failure probability decays exponentially under parallel repetition.

Multiplicativity under tensoring of support functions of other sets of states

Sequence of convex sets of states $\mathcal{K}^{(n)}$ on $\mathrm{H}^{\otimes n}$, $n \in \mathbf{N}$, s.t.

$$\mathcal{K}^{(n)} \supset \left(\mathcal{K}^{(1)}\right)^{\hat{\otimes} n} := \mathrm{conv}\left\{\rho_1 \otimes \cdots \otimes \rho_n \ : \ \rho_1, \ldots, \rho_n \in \mathcal{K}^{(1)}\right\}.$$

Assumptions : Stability under permutation and partial trace.

Simplest example : $\mathcal{K}$ set of states on H, and for each $n \in \mathbf{N}$, $\mathcal{K}^{(n)} = \mathcal{K}^{\hat{\otimes} n}$.

In that case, (quantitative) equivalence between the multiplicative behavior under tensoring of (a) the maximum fidelity function $F\left(\cdot, \mathcal{K}^{(n)}\right)$ and (b) the support function $h_{\mathcal{K}^{(n)}}(\cdot)$.

- To show $(a) \Rightarrow (b)$: use the flexible de Finetti reduction.
- To show $(b) \Rightarrow (a)$: design a discrimination test whose failure probability decays exponentially under parallel repetition.

Question : How differently do $\mathcal{S}(\mathrm{A}^n{:}\mathrm{B}^n)$ and $\mathcal{S}(\mathrm{A{:}B})^{\hat{\otimes} n}$ behave from the point of view of maximum fidelity or support functions, on tensor power inputs ?

References

- **S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, P. Shor**, “The power of unentanglement”.
- **G. Adesso, S. Di Martino, M. Huber, C. Lancien, M. Piani, A. Winter**, “Should entanglement measures be monogamous or faithful ?”.
- **A. Ambainis, A.W. Harrow, M.B. Hastings**, “Random tensor theory : extending random matrix theory to random product states”.
- **M. Christandl, R. König, R. Renner**, “Post-selection technique for quantum channels with applications to quantum cryptography”.
- **M. Christandl, N. Schuch, A. Winter**, “Entanglement of the antisymmetric state”.
- **M. Christandl, A. Winter**, “Squashed entanglement - An additive entanglement measure”.
- **A. Grudka, M. Horodecki, L. Pankowski**, “Constructive counterexamples to additivity of minimum output Rényi entropy of quantum channels for all $p > 2$”.
- **A.W. Harrow, A. Montanaro**, “Testing product states, quantum Merlin-Arthur games and tensor optimisation”.
- **P. Hayden, A. Winter**, “Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$”.
- **A.S. Holevo, R.F. Werner**, “Counterexample to an additivity conjecture for output purity of quantum channels”.
- **M. Horodecki, Z.D. Wang, D. Yang**, “An additive and operational entanglement measure : conditional entanglement of mutual information”.
- **C. Lancien, A. Winter**, “Flexible constrained de Finetti reductions and applications”.
- **K. Li, A. Winter**, “Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps”.
- **A. Montanaro**, “Weak multiplicativity for random quantum channels”.