Weak multiplicativity for random quantum channels

Ashley Montanaro

Centre for Quantum Information and Foundations,
Department of Applied Mathematics and Theoretical Physics,
University of Cambridge

arXiv:1112.5271
CMP, to appear

Engineering and Physical Sciences Research Council

Maximum output p-norms

For a quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$, i.e. CPTP map, the maximum output p-norm of $\mathcal{N}$ is

$$\|\mathcal{N}\|_{1\to p} := \max\{\|\mathcal{N}(\rho)\|_p,\ \rho \geqslant 0,\ \operatorname{tr}\rho = 1\},$$

where $\|X\|_p := (\operatorname{tr}|X|^p)^{1/p}$ is the Schatten p-norm.

Maximum output p-norms

For a quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$, i.e. CPTP map, the maximum output p-norm of $\mathcal{N}$ is

$$\|\mathcal{N}\|_{1\to p} := \max\{\|\mathcal{N}(\rho)\|_p,\ \rho \geqslant 0,\ \operatorname{tr}\rho = 1\},$$

where $\|X\|_p := (\operatorname{tr}|X|^p)^{1/p}$ is the Schatten p-norm.

The following is a reasonable conjecture:

Multiplicativity Conjecture [Amosov, Holevo and Werner '00]

For any channels $\mathcal{N}_1$, $\mathcal{N}_2$, and any $p > 1$,

$$\|\mathcal{N}_1 \otimes \mathcal{N}_2\|_{1\to p} = \|\mathcal{N}_1\|_{1\to p}\|\mathcal{N}_2\|_{1\to p}.$$

Maximum output p-norms

For a quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$, i.e. CPTP map, the maximum output p-norm of $\mathcal{N}$ is

$$\|\mathcal{N}\|_{1\to p} := \max\{\|\mathcal{N}(\rho)\|_p,\ \rho \geqslant 0,\ \operatorname{tr}\rho = 1\},$$

where $\|X\|_p := (\operatorname{tr}|X|^p)^{1/p}$ is the Schatten p-norm.

The following is a reasonable conjecture:

Multiplicativity Conjecture [Amosov, Holevo and Werner '00]

For any channels $\mathcal{N}_1$, $\mathcal{N}_2$, and any $p > 1$,

$$\|\mathcal{N}_1 \otimes \mathcal{N}_2\|_{1\to p} = \|\mathcal{N}_1\|_{1\to p}\|\mathcal{N}_2\|_{1\to p}.$$

For any $\mathcal{N}_1$, $\mathcal{N}_2$, the $\geqslant$ direction of this equality is immediate (just take a product input to $\mathcal{N}_1 \otimes \mathcal{N}_2$), but in general the $\leqslant$ direction is far from immediate.

Why care about multiplicativity?

The multiplicativity conjecture would imply at least two "operational" conjectures:

Additivity conjecture

The Holevo capacity, entanglement of formation and minimum output von Neumann entropy are all additive.

QMA(2) parallel repetition conjecture

The success probability in quantum Merlin-Arthur proof systems with two provers can be amplified by parallel repetition.

The additivity conjecture

- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

$$H_p^{\min}(\mathcal{N}) := \frac{1}{1-p} \log \|\mathcal{N}\|_{1\to p}^p,$$

  the minimum output Rènyi p-entropy of $\mathcal{N}$.

The additivity conjecture

- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

$$H_p^{\min}(\mathcal{N}) := \frac{1}{1-p} \log \|\mathcal{N}\|_{1\to p}^p,$$

  the minimum output Rènyi p-entropy of $\mathcal{N}$.
- Multiplicativity of maximum output p-norms is equivalent to additivity of minimum output Rényi p-entropies.

The additivity conjecture

- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

$$H_p^{\min}(\mathcal{N}) := \frac{1}{1-p} \log \|\mathcal{N}\|_{1\to p}^p,$$

  the minimum output Rènyi p-entropy of $\mathcal{N}$.
- Multiplicativity of maximum output p-norms is equivalent to additivity of minimum output Rényi p-entropies.
- The minimum output von Neumann entropy $H^{\min}(\mathcal{N})$ is obtained by taking the limit $p \to 1$.

The additivity conjecture

- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

$$H_p^{\min}(\mathcal{N}) := \frac{1}{1-p} \log \|\mathcal{N}\|_{1\to p}^p,$$

  the minimum output Rènyi p-entropy of $\mathcal{N}$.
- Multiplicativity of maximum output p-norms is equivalent to additivity of minimum output Rényi p-entropies.
- The minimum output von Neumann entropy $H^{\min}(\mathcal{N})$ is obtained by taking the limit $p \to 1$.
- [Shor '03] showed that additivity of this quantity is equivalent to other additivity conjectures in quantum information theory, e.g.:
  - Additivity of Holevo capacity of quantum channels ($\max_{p_i, |v_i\rangle} H(\mathcal{N}(\sum_i p_i v_i)) - \sum_i p_i H(\mathcal{N}(v_i))$)
  - Additivity of entanglement of formation ($\min_{p_i, |v_i\rangle} \sum_i p_i H(\mathrm{tr}_B\, v_i)$)

The QMA(2) parallel repetition conjecture

- For any quantum channel $\mathcal{N}$, $\mathcal{N}(\rho) = \operatorname{tr}_E V\rho V^\dagger$ for some isometry $V : \mathbb{C}^{d_A} \to \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.

The QMA(2) parallel repetition conjecture

- For any quantum channel $\mathcal{N}$, $\mathcal{N}(\rho) = \operatorname{tr}_E V\rho V^\dagger$ for some isometry $V : \mathbb{C}^{d_A} \to \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.
- Define the support function of the separable states

$$h_{\mathrm{SEP}}(M) := \max_{\rho \in \mathrm{SEP}} \operatorname{tr} M\rho,$$

where SEP is the set of separable quantum states, i.e. states ρ which can be written as

$$\rho = \sum_i p_i \rho_i \otimes \sigma_i.$$

The QMA(2) parallel repetition conjecture

- For any quantum channel $\mathcal{N}$, $\mathcal{N}(\rho) = \operatorname{tr}_E V\rho V^\dagger$ for some isometry $V : \mathbb{C}^{d_A} \to \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.
- Define the support function of the separable states

$$h_{\text{SEP}}(M) := \max_{\rho \in \text{SEP}} \operatorname{tr} M\rho,$$

where SEP is the set of separable quantum states, i.e. states ρ which can be written as

$$\rho = \sum_i p_i \rho_i \otimes \sigma_i.$$

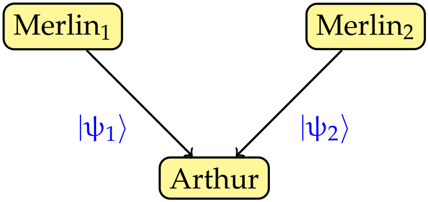
Fact

Let $\mathcal{N}$ be a quantum channel with corresponding isometry V, and set $M = VV^\dagger$. Then

$$h_{\text{SEP}}(M) = \|\mathcal{N}\|_{1\to\infty}.$$

An interpretation of h_{SEP}

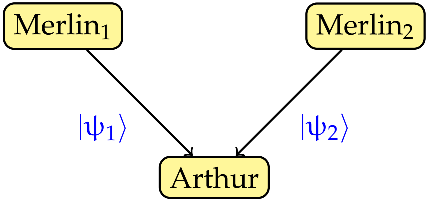
h_{SEP} has a natural interpretation in terms of QMA(2) protocols.



- This is a computational model where a computationally bounded verifier (Arthur) wishes to solve a decision problem, given access to two unentangled "proofs" from Merlin A and Merlin B [Kobayashi et al '03].

An interpretation of h_{SEP}

h_{SEP} has a natural interpretation in terms of QMA(2) protocols.



- This is a computational model where a computationally bounded verifier (Arthur) wishes to solve a decision problem, given access to two unentangled "proofs" from Merlin A and Merlin B [Kobayashi et al '03].
- The Merlins are all-powerful but Arthur cannot trust them.

An interpretation of h_{SEP}

- Consider a QMA(2) protocol with soundness error s, i.e. on inputs which Arthur should reject, for all proofs $|\psi_1\rangle$, $|\psi_2\rangle$, Arthur accepts with probability at most s.

- Let Arthur's measurement operator which corresponds to "reject" be M.

An interpretation of h_{SEP}

- Consider a QMA(2) protocol with soundness error s, i.e. on inputs which Arthur should reject, for all proofs $|\psi_1\rangle$, $|\psi_2\rangle$, Arthur accepts with probability at most s.

- Let Arthur's measurement operator which corresponds to "reject" be M.

- Then the maximum probability with which the Merlins can convince him to (incorrectly) accept is $h_{\text{SEP}}(M) = s$.

An interpretation of h_{SEP}

- Consider a QMA(2) protocol with soundness error s, i.e. on inputs which Arthur should reject, for all proofs $|\psi_1\rangle$, $|\psi_2\rangle$, Arthur accepts with probability at most s.

- Let Arthur's measurement operator which corresponds to "reject" be M.

- Then the maximum probability with which the Merlins can convince him to (incorrectly) accept is $h_{\text{SEP}}(M) = s$.

- So, if $h_{\text{SEP}}(M^{\otimes n}) = h_{\text{SEP}}(M)^n$, Arthur can simply repeat the protocol n times in parallel to achieve soundness error at most s^n.

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\operatorname{tr}\rho)I - \rho^T\right)$

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\mathrm{tr}\,\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\operatorname{tr}\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary
23/7/07	Hayden	$1 < p < 2$	Random subspace

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\mathrm{tr}\,\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary
23/7/07	Hayden	$1 < p < 2$	Random subspace
Dec 07	Cubitt et al	$p \lesssim 0.11$	Random/explicit

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\operatorname{tr}\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary
23/7/07	Hayden	$1 < p < 2$	Random subspace
Dec 07	Cubitt et al	$p \lesssim 0.11$	Random/explicit
2008	Hayden & Winter	$p > 1$	Random subspace

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\operatorname{tr}\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary
23/7/07	Hayden	$1 < p < 2$	Random subspace
Dec 07	Cubitt et al	$p \lesssim 0.11$	Random/explicit
2008	Hayden & Winter	$p > 1$	Random subspace
2008	Hastings	$H^{\min}$	Random subspace

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture is false for all $p > 1$!

When	Who	What	How
2002	Werner & Holevo	$p > 4.79$	$\rho \mapsto \frac{1}{d-1}\left((\operatorname{tr}\rho)I - \rho^T\right)$
3/7/07	Winter	$p > 2$	Random unitary
23/7/07	Hayden	$1 < p < 2$	Random subspace
Dec 07	Cubitt et al	$p \lesssim 0.11$	Random/explicit
2008	Hayden & Winter	$p > 1$	Random subspace
2008	Hastings	$H^{\min}$	Random subspace
2009	Grudka et al	$p > 2$	Antisym. subspace

Further, for $p = \infty$ it's really, really false: If P_{anti} is the projector onto the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$,

$$h_{\text{SEP}}(P_{\text{anti}}) = \frac{1}{2}, \text{ but } h_{\text{SEP}}(P_{\text{anti}}^{\otimes 2}) \geqslant \frac{1}{2}\left(1 - \frac{1}{d}\right).$$

What about more copies?

So we have an example of a channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes 2}\|_{1\to\infty} \approx \|\mathcal{N}\|_{1\to\infty}.$$

What about $\|\mathcal{N}^{\otimes n}\|_{1\to\infty}$ for large n?

What about more copies?

So we have an example of a channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes 2}\|_{1\to\infty} \approx \|\mathcal{N}\|_{1\to\infty}.$$

What about $\|\mathcal{N}^{\otimes n}\|_{1\to\infty}$ for large n?

- The following two extreme possibilities could be true:

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \overset{?}{\leqslant} \|\mathcal{N}\|_{1\to\infty}^{n/2}$$

for all $\mathcal{N}$; or there might exist a family of channels $\mathcal{N}$ such that there is no constant $\alpha > 0$ such that

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \leqslant \|\mathcal{N}\|_{1\to\infty}^{\alpha n}$$

What about more copies?

So we have an example of a channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes 2}\|_{1\to\infty} \approx \|\mathcal{N}\|_{1\to\infty}.$$

What about $\|\mathcal{N}^{\otimes n}\|_{1\to\infty}$ for large n?

- The following two extreme possibilities could be true:

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \overset{?}{\leqslant} \|\mathcal{N}\|_{1\to\infty}^{n/2}$$

  for all $\mathcal{N}$; or there might exist a family of channels $\mathcal{N}$ such that there is no constant $\alpha > 0$ such that

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \leqslant \|\mathcal{N}\|_{1\to\infty}^{\alpha n}$$

- If the first case is true, the largest possible violation of multiplicativity is quite mild, and a form of parallel repetition holds for quantum Merlin-Arthur games.

What about more copies?

So we have an example of a channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes 2}\|_{1\to\infty} \approx \|\mathcal{N}\|_{1\to\infty}.$$

What about $\|\mathcal{N}^{\otimes n}\|_{1\to\infty}$ for large n?

- The following two extreme possibilities could be true:

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \overset{?}{\leqslant} \|\mathcal{N}\|_{1\to\infty}^{n/2}$$

  for all $\mathcal{N}$; or there might exist a family of channels $\mathcal{N}$ such that there is no constant $\alpha > 0$ such that

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \leqslant \|\mathcal{N}\|_{1\to\infty}^{\alpha n}$$

- If the first case is true, the largest possible violation of multiplicativity is quite mild, and a form of parallel repetition holds for quantum Merlin-Arthur games.
- If the second case is true, severe violations are possible and parallel repetition fails.

Weak multiplicativity

Definition

A quantum channel $\mathcal{N}$ obeys weak p-norm multiplicativity with exponent α if, for all $n \geqslant 1$,

$$\|\mathcal{N}^{\otimes n}\|_{1\to p} \leqslant \|\mathcal{N}\|_{1\to p}^{\alpha n}.$$

Today's message

Random quantum channels obey weak ∞-norm multiplicativity!

Today's message

Random quantum channels obey weak ∞-norm multiplicativity!

Main result (informal)

Let $\mathcal{N}$ be a quantum channel whose corresponding subspace is a random dimension r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then the probability that $\mathcal{N}$ does not obey weak ∞-norm multiplicativity with exponent $1/2 - o(1)$ is exponentially small in $\min\{r, d_A, d_B\}$.

Today's message

Random quantum channels obey weak ∞-norm multiplicativity!

Main result (informal)

Let $\mathcal{N}$ be a quantum channel whose corresponding subspace is a random dimension r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then the probability that $\mathcal{N}$ does not obey weak ∞-norm multiplicativity with exponent $1/2 - o(1)$ is exponentially small in $\min\{r, d_A, d_B\}$.

Note: The above result holds with the following (fairly weak) restrictions on r, d_A, d_B:

- $r = o(d_A d_B)$.
- $\min\{r, d_A, d_B\} \geqslant 2(\log_2 \max\{d_A, d_B\})^{3/2}$.

Other p and the von Neumann entropy

This ∞-norm result also implies similar results for other p-norms and the von Neumann entropy.

Other p and the von Neumann entropy

This ∞-norm result also implies similar results for other p-norms and the von Neumann entropy.

- By the (matrix) Hölder inequality, if $\mathcal{N}$ obeys weak ∞-norm multiplicativity with exponent α, $\mathcal{N}$ also obeys weak p-norm multiplicativity for any $p > 1$, with exponent $\alpha(1 - 1/p)$, via

$$\|X\|_\infty \leqslant \|X\|_p \leqslant \|X\|_1^{1/p} \|X\|_\infty^{1-1/p}.$$

Other p and the von Neumann entropy

This ∞-norm result also implies similar results for other p-norms and the von Neumann entropy.

- By the (matrix) Hölder inequality, if $\mathcal{N}$ obeys weak ∞-norm multiplicativity with exponent α, $\mathcal{N}$ also obeys weak p-norm multiplicativity for any $p > 1$, with exponent $\alpha(1 - 1/p)$, via

$$\|X\|_\infty \leqslant \|X\|_p \leqslant \|X\|_1^{1/p} \|X\|_\infty^{1-1/p}.$$

- Using monotonicity of Rényi entropies, we can also write down a result for the von Neumann entropy in certain regimes, e.g. $r = d_A = d_B$:

$$\frac{1}{n} H_{\min}(\mathcal{N}^{\otimes n}) \geqslant \frac{1}{2} H_{\min}(\mathcal{N}) - O(1).$$

Proof technique

Conceptually very simple:

1. Let M be the projector onto a random dimension r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$.
2. Relax $h_{\mathrm{SEP}}(M)$ to a quantity which is multiplicative.
3. Prove an upper bound on this quantity.
4. Prove a lower bound on $h_{\mathrm{SEP}}(M)$.

Proof technique

Conceptually very simple:

1. Let M be the projector onto a random dimension r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$.
2. Relax $h_{\text{SEP}}(M)$ to a quantity which is multiplicative.
3. Prove an upper bound on this quantity.
4. Prove a lower bound on $h_{\text{SEP}}(M)$.

The only technical part is (3), which uses techniques from random matrix theory.

- Similar techniques were used by [Collins and Nechita $\times$3, '09], [Aubrun '10], [Collins, Fukuda and Nechita '11], ...

Relaxing $h_{\text{SEP}}(M)$

We use the operator norm of the partial transpose M^{Γ}.

Relaxing $h_{\text{SEP}}(M)$

We use the operator norm of the partial transpose M^{Γ}.

- A bipartite quantum state ρ is said to be positive partial transpose (PPT) if $\rho^{\Gamma} \geqslant 0$.

Relaxing $h_{\mathrm{SEP}}(M)$

We use the operator norm of the partial transpose M^{Γ}.

- A bipartite quantum state ρ is said to be positive partial transpose (PPT) if $\rho^{\Gamma} \geqslant 0$.
- We have SEP $\subset$ PPT and hence

$$h_{\mathrm{PPT}}(M) := \max_{\rho \in \mathrm{PPT}} \operatorname{tr} M\rho \geqslant h_{\mathrm{SEP}}(M).$$

Relaxing $h_{\mathrm{SEP}}(M)$

We use the operator norm of the partial transpose M^Γ.

- A bipartite quantum state ρ is said to be positive partial transpose (PPT) if $\rho^\Gamma \geqslant 0$.
- We have SEP $\subset$ PPT and hence

$$h_{\mathrm{PPT}}(M) := \max_{\rho \in \mathrm{PPT}} \operatorname{tr} M\rho \geqslant h_{\mathrm{SEP}}(M).$$

Observation

$$h_{\mathrm{PPT}}(M) \leqslant \|M^\Gamma\|_\infty.$$

Relaxing $h_{\mathrm{SEP}}(M)$

We use the operator norm of the partial transpose M^Γ.

- A bipartite quantum state ρ is said to be positive partial transpose (PPT) if $\rho^\Gamma \geqslant 0$.
- We have SEP $\subset$ PPT and hence

$$h_{\mathrm{PPT}}(M) := \max_{\rho \in \mathrm{PPT}} \operatorname{tr} M\rho \geqslant h_{\mathrm{SEP}}(M).$$

Observation

$$h_{\mathrm{PPT}}(M) \leqslant \|M^\Gamma\|_\infty.$$

Observation

For any operators M, N,
$\|(M \otimes N)^\Gamma\|_\infty = \|M^\Gamma \otimes N^\Gamma\|_\infty = \|M^\Gamma\|_\infty \|N^\Gamma\|_\infty$.

Lower bounding $h_{\mathrm{SEP}}(M)$

Proposition

Let M be the projector onto an r-dimensional subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then

$$h_{\mathrm{SEP}}(M) \geqslant \max\left\{\frac{r}{d_A d_B}, \frac{1}{d_A}\right\}.$$

Lower bounding $h_{\mathrm{SEP}}(M)$

Proposition

Let M be the projector onto an r-dimensional subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then

$$h_{\mathrm{SEP}}(M) \geqslant \max\left\{\frac{r}{d_A d_B}, \frac{1}{d_A}\right\}.$$

(Proof: for the first part, pick a uniformly random product state; for the second part, note that by the correspondence with quantum channels, any state output from the channel which corresponds to M must have largest eigenvalue at least $1/d_A$.)

Lower bounding $h_{\mathrm{SEP}}(M)$

Proposition

Let M be the projector onto an r-dimensional subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then

$$h_{\mathrm{SEP}}(M) \geqslant \max\left\{\frac{r}{d_A d_B}, \frac{1}{d_A}\right\}.$$

(Proof: for the first part, pick a uniformly random product state; for the second part, note that by the correspondence with quantum channels, any state output from the channel which corresponds to M must have largest eigenvalue at least $1/d_A$.)

Thus, if we can show that $\|M^\Gamma\|_\infty = O\left(\max\left\{\frac{r}{d_A d_B}, \frac{1}{d_A}\right\}^{1/2}\right)$ with high probability, we'll be done.

Large deviation bounds

- Our main result will follow easily from putting good upper bounds on $\mathbb{E}\,\mathrm{tr}(M^\Gamma)^k$ for arbitrary k.

Large deviation bounds

- Our main result will follow easily from putting good upper bounds on $\mathbb{E}\,\mathrm{tr}(M^\Gamma)^k$ for arbitrary k.
- Let M_0 be the projector onto an arbitrary dim r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and set

$$M^{(k)} := \mathbb{E}_U[U^{\otimes k} M_0^{\otimes k} (U^\dagger)^{\otimes k}].$$

Large deviation bounds

- Our main result will follow easily from putting good upper bounds on $\mathbb{E}\,\mathrm{tr}(M^\Gamma)^k$ for arbitrary k.
- Let M_0 be the projector onto an arbitrary dim r subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and set

$$M^{(k)} := \mathbb{E}_U[U^{\otimes k} M_0^{\otimes k} (U^\dagger)^{\otimes k}].$$

- Then

$$\mathbb{E}\,\mathrm{tr}(M^\Gamma)^k = \mathrm{tr}[D(\kappa)^\Gamma M^{(k)}],$$

  where

$$D(\pi) := \sum_{i_1,\ldots,i_k=1}^{d_A d_B} |i_{\pi(1)}\rangle|i_{\pi(2)}\rangle \ldots |i_{\pi(k)}\rangle\langle i_1| \ldots \langle i_k|$$

  is the representation of the permutation $\pi \in S_k$ which acts by permuting the k systems, and κ is an arbitrary k-cycle.

Main technical result

Theorem

For any k satisfying $2k^{3/2} \leqslant \min\{d_A, d_B, r\}$,

$$\mathrm{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \begin{cases} \mathrm{poly}(k) 2^{6k} r^{k/2} d_A^{-k/2+1} d_B^{-k/2+1} & \text{if } r \geqslant d_B/d_A \\ \mathrm{poly}(k) 2^{6k} d_A^{-k+1} d_B & \text{otherwise.} \end{cases}$$

Main technical result

Theorem

For any k satisfying $2k^{3/2} \leqslant \min\{d_A, d_B, r\}$,

$$\mathrm{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \begin{cases} \mathrm{poly}(k) 2^{6k} r^{k/2} d_A^{-k/2+1} d_B^{-k/2+1} & \text{if } r \geqslant d_B/d_A \\ \mathrm{poly}(k) 2^{6k} d_A^{-k+1} d_B & \text{otherwise.} \end{cases}$$

The above implies (when $r \geqslant d_B/d_A$, for example):

Theorem

There exists a universal constant C such that, for any $\delta > 0$,

$$\Pr\left[\|M^\Gamma\|_\infty \geqslant \delta \frac{2^8 r^{1/2}}{d_A^{1/2} d_B^{1/2}} \right] \leqslant C m^{16/3} \delta^{-(m/2)^{2/3}},$$

where $m = \min\{r, d_A, d_B\} \geqslant 2(\log_2 \max\{r, d_A, d_B\})^{3/2}$.

Outline of proof

- Write
$$M^{(k)} = \sum_{\pi \in S_k} \alpha_\pi D(\pi)$$
for some α_π (follows from Schur-Weyl duality).

Outline of proof

- Write
$$M^{(k)} = \sum_{\pi \in S_k} \alpha_\pi D(\pi)$$
for some α_π (follows from Schur-Weyl duality).
- Use
$$\mathrm{tr}[D(\kappa)^\Gamma D(\pi)] = d_A^{c(\kappa\pi)} d_B^{c(\kappa^{-1}\pi)},$$
where $c(\pi)$ is the number of cycles in π

Outline of proof

- Write
$$M^{(k)} = \sum_{\pi \in S_k} \alpha_\pi D(\pi)$$
for some α_π (follows from Schur-Weyl duality).

- Use
$$\mathrm{tr}[D(\kappa)^\Gamma D(\pi)] = d_A^{c(\kappa\pi)} d_B^{c(\kappa^{-1}\pi)},$$
where $c(\pi)$ is the number of cycles in π (proof:
$$\begin{aligned}
\mathrm{tr}[D(\kappa)^\Gamma D(\pi)] &= \mathrm{tr}[(D_{d_A}(\kappa) \otimes D_{d_B}(\kappa)^T)(D_{d_A}(\pi) \otimes D_{d_B}(\pi))] \\
&= \mathrm{tr}[D_{d_A}(\kappa) D_{d_A}(\pi)]\, \mathrm{tr}[D_{d_B}(\kappa^{-1}) D_{d_B}(\pi)] \\
&= d_A^{c(\kappa\pi)} d_B^{c(\kappa^{-1}\pi)}).
\end{aligned}$$

Outline of proof

- Write

$$M^{(k)} = \sum_{\pi \in S_k} \alpha_\pi D(\pi)$$

for some α_π (follows from Schur-Weyl duality).

- Use

$$\mathrm{tr}[D(\kappa)^\Gamma D(\pi)] = d_A^{c(\kappa\pi)} d_B^{c(\kappa^{-1}\pi)},$$

where $c(\pi)$ is the number of cycles in π (proof:

$$\begin{aligned}
\mathrm{tr}[D(\kappa)^\Gamma D(\pi)] &= \mathrm{tr}[(D_{d_A}(\kappa) \otimes D_{d_B}(\kappa)^T)(D_{d_A}(\pi) \otimes D_{d_B}(\pi))] \\
&= \mathrm{tr}[D_{d_A}(\kappa) D_{d_A}(\pi)]\, \mathrm{tr}[D_{d_B}(\kappa^{-1}) D_{d_B}(\pi)] \\
&= d_A^{c(\kappa\pi)} d_B^{c(\kappa^{-1}\pi)}).
\end{aligned}$$

- Upper bound the α_π coefficients.

Bounding the α_π coefficients

- When k is small with respect to $d_A d_B$, the matrices $\{D(\pi)\}$ are almost orthonormal with respect to the normalised Hilbert-Schmidt inner product, i.e.

$$\frac{1}{(d_A d_B)^k} \operatorname{tr}[D(\pi)^\dagger D(\sigma)] \approx 0 \text{ if } \pi \neq \sigma.$$

Bounding the α_π coefficients

- When k is small with respect to $d_A d_B$, the matrices $\{D(\pi)\}$ are almost orthonormal with respect to the normalised Hilbert-Schmidt inner product, i.e.

$$\frac{1}{(d_A d_B)^k} \operatorname{tr}[D(\pi)^\dagger D(\sigma)] \approx 0 \text{ if } \pi \neq \sigma.$$

- We know $\operatorname{tr} D(\pi) M^{(k)} = r^{c(\pi)}$ for any π. Because of the near-orthonormality we ought to have

$$\alpha_\pi \approx \frac{\operatorname{tr}[M^{(k)} D(\pi^{-1})]}{\operatorname{tr}[D(\pi^{-1}) D(\pi)]} = \frac{r^{c(\pi)}}{(d_A d_B)^k}.$$

Bounding the α_π coefficients

- When k is small with respect to $d_A d_B$, the matrices $\{D(\pi)\}$ are almost orthonormal with respect to the normalised Hilbert-Schmidt inner product, i.e.

$$\frac{1}{(d_A d_B)^k} \operatorname{tr}[D(\pi)^\dagger D(\sigma)] \approx 0 \text{ if } \pi \neq \sigma.$$

- We know $\operatorname{tr} D(\pi) M^{(k)} = r^{c(\pi)}$ for any π. Because of the near-orthonormality we ought to have

$$\alpha_\pi \approx \frac{\operatorname{tr}[M^{(k)} D(\pi^{-1})]}{\operatorname{tr}[D(\pi^{-1}) D(\pi)]} = \frac{r^{c(\pi)}}{(d_A d_B)^k}.$$

- In fact, the α_π coefficients can be calculated explicitly in terms of the Weingarten function.
- Finding a bound on this function lets us upper bound α_π.

Completing the proof

Lemma

Assume $k \leqslant (r/2)^{2/3}$. Then

$$|\alpha_\pi| \leqslant \text{poly}(k) 2^{4k} \frac{r^{c(\pi)}}{(d_A d_B)^k}.$$

Completing the proof

Lemma

Assume $k \leqslant (r/2)^{2/3}$. Then

$$|\alpha_\pi| \leqslant \text{poly}(k) 2^{4k} \frac{r^{c(\pi)}}{(d_A d_B)^k}.$$

- Using this bound on the α_π coefficients, we're left with

$$\text{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \text{poly}(k) 2^{4k} \sum_{\pi \in S_k} d_A^{c(\kappa\pi)-k} d_B^{c(\kappa^{-1}\pi)-k} r^{c(\pi)}$$

Completing the proof

Lemma

Assume $k \leqslant (r/2)^{2/3}$. Then

$$|\alpha_\pi| \leqslant \mathrm{poly}(k) 2^{4k} \frac{r^{c(\pi)}}{(d_A d_B)^k}.$$

- Using this bound on the α_π coefficients, we're left with

$$\mathrm{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \mathrm{poly}(k) 2^{4k} \sum_{\pi \in S_k} d_A^{c(\kappa\pi)-k} d_B^{c(\kappa^{-1}\pi)-k} r^{c(\pi)}$$

- To finish off, show that there can't be "too many" permutations π such that $c(\pi)$, $c(\kappa\pi)$ and $c(\kappa^{-1}\pi)$ are all large simultaneously.

Conclusions

- We've proven weak multiplicativity for random quantum channels by relaxing to a multiplicative quantity which we can upper bound using ideas from random matrix theory.

Conclusions

- We've proven weak multiplicativity for random quantum channels by relaxing to a multiplicative quantity which we can upper bound using ideas from random matrix theory.

- The result obtained is probably the strongest one could expect given known violations of multiplicativity.

Conclusions

- We've proven weak multiplicativity for random quantum channels by relaxing to a multiplicative quantity which we can upper bound using ideas from random matrix theory.

- The result obtained is probably the strongest one could expect given known violations of multiplicativity.

- In particular, by the results of Hayden and Winter, in certain regimes

$$\|\mathcal{N} \otimes \overline{\mathcal{N}}\|_{1\to\infty} \approx \|\mathcal{N}\|_{1\to\infty}$$

  for random $\mathcal{N}$, so increasing the exponent from $1/2$ seems unlikely (?).

Open problems

Prove weak p-norm multiplicativity for all quantum channels!

Open problems

Prove weak p-norm multiplicativity for all quantum channels!

On a more concrete level:

- The technique used here fails completely for the antisymmetric subspace.
- However, [Christandl, Schuch and Winter '09] have shown using a different technique that the antisymmetric subspace also obeys weak p-norm multiplicativity.
- Can one proof technique be made to work for both channels?

Thanks!

arXiv:1112.5271