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

Engineering and Physical Sciences Research Council

Maximum output p-norms

Some definitions:

- A quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$ is a completely positive, trace-preserving map (i.e. a map which takes quantum states to quantum states).

Maximum output p-norms

Some definitions:

- A quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$ is a completely positive, trace-preserving map (i.e. a map which takes quantum states to quantum states).
- 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

Some definitions:

- A quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$ is a completely positive, trace-preserving map (i.e. a map which takes quantum states to quantum states).
- 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.
- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

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

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

Maximum output p-norms

Some definitions:

- A quantum channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$ is a completely positive, trace-preserving map (i.e. a map which takes quantum states to quantum states).
- 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.
- Studying $\|\mathcal{N}\|_{1\to p}$ is equivalent to studying

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

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

The case $p = \infty$

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

The case $p = \infty$

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

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

where $\mathrm{SEP} \subset \mathcal{B}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ 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 case $p = \infty$

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

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

where $\text{SEP} \subset \mathcal{B}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ 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

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

Other interpretations 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.

Other interpretations 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.

- The Merlins are all-powerful but Arthur cannot trust them.

Other interpretations 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.
- The Merlins are all-powerful but Arthur cannot trust them.
- If Arthur's measurement operator which corresponds to a "yes" outcome is M, the maximum probability with which the Merlins can convince him to accept is $h_{\mathrm{SEP}}(M)$.

Multiplicativity of maximum output p-norms

The following is a reasonable conjecture:

Multiplicativity Conjecture **[Amosov, Holevo and Werner '00]**

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

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

Multiplicativity of maximum output p-norms

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.

Multiplicativity of maximum output p-norms

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.
- This conjecture is equivalent to additivity of minimum output Rényi p-entropies.

Why care about multiplicativity?

- In the limit $p \to 1$, multiplicativity (i.e. additivity of von Neumann entropy) is equivalent to other additivity conjectures in quantum information theory [Shor '03], 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 $(\min_{p_i,|v_i\rangle} \sum_i p_i H(\mathrm{tr}_B\, v_i))$

Why care about multiplicativity?

- In the limit $p \to 1$, multiplicativity (i.e. additivity of von Neumann entropy) is equivalent to other additivity conjectures in quantum information theory [Shor '03], 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 ($\min_{p_i,|v_i\rangle} \sum_i p_i H(\operatorname{tr}_B v_i)$)

- In the case $p = \infty$, multiplicativity is equivalent to parallel repetition for QMA(2) protocols.

- In other words, if $h_{\text{SEP}}(M^{\otimes n}) = h_{\text{SEP}}(M)^n$, Arthur can simply repeat the protocol n times in parallel to achieve failure probability exponentially small in n.

Failure of multiplicativity

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

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture (MC) 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 (MC) 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

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture (MC) 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

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture (MC) 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

Failure of multiplicativity

Unfortunately (?), the Multiplicativity Conjecture (MC) 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 (MC) 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 (MC) 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 $p = \infty$ MC is really, really false: If P_{anti} is the projector onto the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$,

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

Random quantum channels

The counterexamples of Hayden and Hayden-Winter are random constructions.

Random quantum channels

The counterexamples of Hayden and Hayden-Winter are random constructions.

- Let $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$'s corresponding subspace S in the Stinespring form be a random r-dimensional subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.

Random quantum channels

The counterexamples of Hayden and Hayden-Winter are random constructions.

- Let $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$'s corresponding subspace S in the Stinespring form be a random r-dimensional subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.
- In other words, form the projector $P = VV^\dagger$ onto S by taking the projector onto an arbitrary fixed subspace $S_0 \subseteq \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$ and conjugating it by a Haar-random unitary.

Random quantum channels

The counterexamples of Hayden and Hayden-Winter are random constructions.

- Let $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$'s corresponding subspace S in the Stinespring form be a random r-dimensional subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.
- In other words, form the projector $P = VV^\dagger$ onto S by taking the projector onto an arbitrary fixed subspace $S_0 \subseteq \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$ and conjugating it by a Haar-random unitary.
- Hayden and Winter show that, for any $p > 1$, and $r \approx d^{1+1/p}$, the pair of channels $(\mathcal{N}, \bar{\mathcal{N}})$ violates multiplicativity with high probability.

Random quantum channels

The counterexamples of Hayden and Hayden-Winter are random constructions.

- Let $\mathcal{N} : \mathcal{B}(\mathbb{C}^{d_A}) \to \mathcal{B}(\mathbb{C}^{d_B})$'s corresponding subspace S in the Stinespring form be a random r-dimensional subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$.
- In other words, form the projector $P = VV^\dagger$ onto S by taking the projector onto an arbitrary fixed subspace $S_0 \subseteq \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$ and conjugating it by a Haar-random unitary.
- Hayden and Winter show that, for any $p > 1$, and $r \approx d^{1+1/p}$, the pair of channels $(\mathcal{N}, \bar{\mathcal{N}})$ violates multiplicativity with high probability.
- Again, for $p = \infty$, the violation is almost maximal:

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

What about more copies?

- We have examples of channels $\mathcal{N}$ 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?

- We have examples of channels $\mathcal{N}$ 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 channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \overset{?}{\approx} \|\mathcal{N}\|_{1\to\infty}.$$

What about more copies?

- We have examples of channels $\mathcal{N}$ 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 channel $\mathcal{N}$ such that

$$\|\mathcal{N}^{\otimes n}\|_{1\to\infty} \overset{?}{\approx} \|\mathcal{N}\|_{1\to\infty}.$$

- 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 completely fails.

Weak multiplicativity

Definition

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

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

Weak multiplicativity

Definition

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

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

- 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

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

- We therefore concentrate on $p = \infty$ in what follows.

Today's message

Random quantum channels obey weak p-norm multiplicativity!

Today's message

Random quantum channels obey weak p-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 p-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:

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

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], [Collins, Fukuda and Nechita '11], ...

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

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

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

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

- Recall that the partial transpose $^\Gamma$ is the superoperator defined by
$$(|ij\rangle\langle kl|)^\Gamma = |il\rangle\langle kj|$$
and extending by linearity.

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

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

- Recall that the partial transpose $^\Gamma$ is the superoperator defined by
$$(|ij\rangle\langle kl|)^\Gamma = |il\rangle\langle kj|$$
and extending by linearity.

- 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 of M.

- Recall that the partial transpose $^\Gamma$ is the superoperator defined by
$$(|ij\rangle\langle kl|)^\Gamma = |il\rangle\langle kj|$$
and extending by linearity.

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

Two claims

Proposition

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

Two claims

Proposition

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

(Proof:

$$h_{\mathrm{PPT}}(M) = \max_{\rho,\, \rho \geqslant 0,\, \rho^\Gamma \geqslant 0, \operatorname{tr} \rho = 1} \operatorname{tr} M\rho = \max_{\sigma,\, \sigma \geqslant 0,\, \sigma^\Gamma \geqslant 0, \operatorname{tr} \sigma^\Gamma = 1} \operatorname{tr} M\sigma^\Gamma,$$

and for any density matrix σ, $\operatorname{tr} M\sigma^\Gamma = \operatorname{tr} M^\Gamma \sigma \leqslant \|M^\Gamma\|_\infty$.)

Two claims

Proposition

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

(Proof:

$$h_{\mathrm{PPT}}(M) = \max_{\rho,\rho\geqslant 0,\rho^\Gamma\geqslant 0,\mathrm{tr}\,\rho=1} \mathrm{tr}\, M\rho = \max_{\sigma,\sigma\geqslant 0,\sigma^\Gamma\geqslant 0,\mathrm{tr}\,\sigma^\Gamma=1} \mathrm{tr}\, M\sigma^\Gamma,$$

and for any density matrix σ, $\mathrm{tr}\, M\sigma^\Gamma = \mathrm{tr}\, M^\Gamma\sigma \leqslant \|M^\Gamma\|_\infty$.)

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

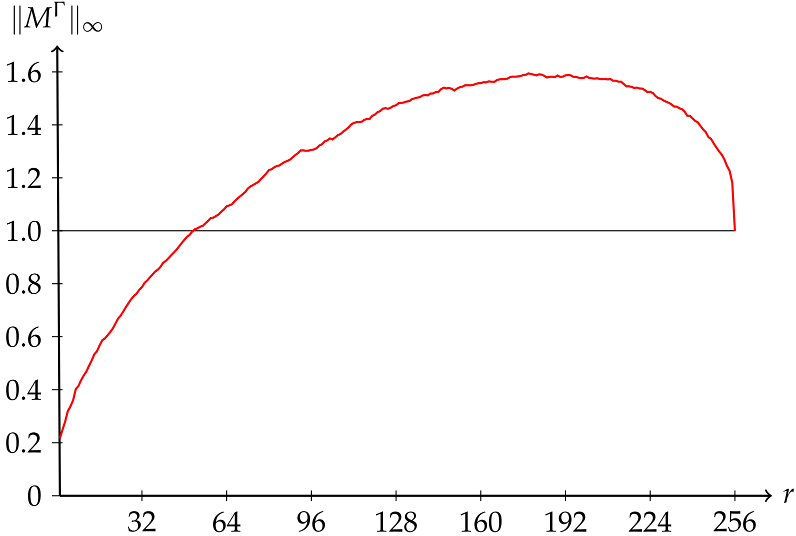
Let M be the projector onto an r-dimensional subspace of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then

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

(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.

Numerical intuition: random rank r subspaces of $\mathbb{C}^{16} \otimes \mathbb{C}^{16}$



Analytic intuition

- Important intuition that $\|M^\Gamma\|_\infty$ should be small comes from previous work by [Aubrun '11] and [Banica and Nechita '11] on the partial transpose of random quantum states.

Analytic intuition

- Important intuition that $\|M^\Gamma\|_\infty$ should be small comes from previous work by [Aubrun '11] and [Banica and Nechita '11] on the partial transpose of random quantum states.
- For constant $0 < \alpha < 1$ and growing d, set $r = \alpha d^2$. Let G be a $d^2 \times r$ matrix whose entries are picked from the complex normal distribution $N(0,1)$, and set $W = GG^\dagger/d^2$.

Analytic intuition

- Important intuition that $\|M^\Gamma\|_\infty$ should be small comes from previous work by [Aubrun '11] and [Banica and Nechita '11] on the partial transpose of random quantum states.
- For constant $0 < \alpha < 1$ and growing d, set $r = \alpha d^2$. Let G be a $d^2 \times r$ matrix whose entries are picked from the complex normal distribution $N(0,1)$, and set $W = GG^\dagger/d^2$.
- Aubrun showed that with high probability $\|W^\Gamma\|_\infty = O(\sqrt{r}/d)$.

Analytic intuition

- Important intuition that $\|M^\Gamma\|_\infty$ should be small comes from previous work by [Aubrun '11] and [Banica and Nechita '11] on the partial transpose of random quantum states.

- For constant $0 < \alpha < 1$ and growing d, set $r = \alpha d^2$. Let G be a $d^2 \times r$ matrix whose entries are picked from the complex normal distribution $N(0,1)$, and set $W = GG^\dagger / d^2$.

- Aubrun showed that with high probability $\|W^\Gamma\|_\infty = O(\sqrt{r}/d)$.

- As the columns of G are approximately orthogonal for large d, one might expect the operator norm of the partial transpose of the projector onto a random r-dimensional subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$ to behave similarly.

- We show that this is indeed the case.

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.

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

- Because of this 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.

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

- Because of this near-orthonormality we ought to have

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

Lemma

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

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

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.

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

- Because of this near-orthonormality we ought to have

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

Lemma

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

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

See Friday's talk by Aram Harrow for many more examples where this philosophy comes in useful.

Outline of proof

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

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

  or in other words

$$\operatorname{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \frac{\operatorname{poly}(k) 2^{4k}}{d_A^k d_B^k} \sum_{a,b,c \in \{1,\ldots,k\}} N(a,b,c) d_A^a d_B^b r^c$$

  where

$$N(a,b,c) := |\{\pi \in S_k : c(\kappa\pi) = a, c(\kappa^{-1}\pi) = b, c(\pi) = c\}|.$$

Basic combinatorial lemma

Lemma

$N(a, b, c) = 0$ unless

$$a + b \leqslant k + 2, \; a + c \leqslant k + 1, \; \text{and } b + c \leqslant k + 1.$$

Further, if all of these validity inequalities are satisfied,

$$N(a, b, c) \leqslant 4^{k-1} k^{(3/2)(k+2-\max\{a+b, a+c, b+c\})+1}.$$

- Intuition: there aren't "too many" permutations which are close to saturating the validity inequalities.

Basic combinatorial lemma

Lemma

$N(a,b,c) = 0$ unless

$$a+b \leqslant k+2,\ a+c \leqslant k+1,\ \text{and } b+c \leqslant k+1.$$

Further, if all of these validity inequalities are satisfied,

$$N(a,b,c) \leqslant 4^{k-1} k^{(3/2)(k+2-\max\{a+b,a+c,b+c\})+1}.$$

- Intuition: there aren't "too many" permutations which are close to saturating the validity inequalities.
- Proof: some combinatorics of the symmetric group...
- Based on a relationship between permutations saturating the validity inequalities and non-crossing partitions [Biane '97] and a recurrence for permutations close to saturating them [Adrianov '97]. See e.g. [Aubrun '11] for related results.

Finishing the proof

- Using this lemma, relax to

$$\mathrm{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \frac{\mathrm{poly}(k)2^{4k}}{d_A^k d_B^k} \max_{(a,b,c)\ \mathrm{valid}} \left\{ 4^k k^{(3/2)(k-\max\{a+b,a+c,b+c\})} d_A^a d_B^b r^c \right\},$$

  and then again to

$$\mathrm{tr}[D(\kappa)^\Gamma M^{(k)}] \leqslant \frac{\mathrm{poly}(k)2^{6k}}{d_A^k d_B^k} \max_{(a,b,c)\ \mathrm{valid}} \left\{ d_A^a d_B^b r^c \right\}.$$

Finishing the proof

- Using this lemma, relax to

$$\mathrm{tr}[D(\kappa)^{\Gamma} M^{(k)}] \leqslant \frac{\mathrm{poly}(k) 2^{4k}}{d_A^k d_B^k} \max_{(a,b,c) \text{ valid}} \left\{ 4^k k^{(3/2)(k - \max\{a+b, a+c, b+c\})} d_A^a d_B^b r^c \right\},$$

and then again to

$$\mathrm{tr}[D(\kappa)^{\Gamma} M^{(k)}] \leqslant \frac{\mathrm{poly}(k) 2^{6k}}{d_A^k d_B^k} \max_{(a,b,c) \text{ valid}} \left\{ d_A^a d_B^b r^c \right\}.$$

- Relax this maximisation to a simple linear program based on the validity constraints.

- Use duality to put upper bounds on this linear program.

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.

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?

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?

What about the limit $p \to 1$?

Thanks!

arXiv:1112.5271

Bounding the α_π coefficients

- Let A be the symmetric matrix defined by $A_{\pi\sigma} = d^{c(\pi^{-1}\sigma)-k}$, for $\pi, \sigma \in S_k$.
- Given some matrix M such that $M = \sum_{\pi \in S_k} \alpha_\pi D_d(\pi)$, A determines the coefficients α_π as follows:

$$\operatorname{tr} M D_d(\sigma) = \sum_{\pi \in S_k} \alpha_\pi d^{c(\pi\sigma)} = d^k \sum_{\pi \in S_k} A_{\sigma^{-1}\pi} \alpha_\pi.$$

- So, if we can invert A, we can determine the α_π coefficients corresponding to $M^{(k)}$ by

$$\alpha_\pi = \frac{1}{(d_A d_B)^k} \sum_{\sigma \in S_k} A^{-1}_{\pi\sigma} r^{c(\sigma)}.$$

- Note that A is approximately equal to the identity when d is large with respect to k, as its off-diagonal entries rapidly decay.

Bounding the α_π coefficients

- In order to evaluate the entries of A^{-1}, we define the Weingarten function [Collins and Śniady '06]

$$\mathrm{Wg}(\pi) := \frac{1}{(k!)^2} \sum_{\lambda \vdash k} \frac{(f^\lambda)^2}{s_\lambda(1^{\times d})} \chi^\lambda(\pi).$$

Facts [Collins and Śniady '06]

$$A^{-1}_{\pi\sigma} = d^k \, \mathrm{Wg}(\pi^{-1}\sigma).$$

Further,

$$|A^{-1}_{\pi\sigma}| \leqslant (C_{k-1} + O(d^{-2})) d^{c(\pi^{-1}\sigma)-k},$$

where C_n is the n'th Catalan number.

Now we just need to carefully upper bound the resulting sum.