Weak multiplicativity for random quantum channels

Ashley Montanaro[1]

Technical version: arXiv:1112.5271.

Introduction. For many years, some of the most vexatious open problems of quantum information theory have concerned maximum output p-norms of quantum channels. If $\mathcal{N}$ is a quantum channel (i.e. completely positive, trace-preserving map), the maximum output p-norm of $\mathcal{N}$ is defined as

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

where $\|X\|_p := (\operatorname{tr}|X|^p)^{1/p}$ is the Schatten p-norm. It was a long-standing conjecture in quantum information theory [1] that, for any two quantum channels $\mathcal{N}_1$, $\mathcal{N}_2$,

$$\|\mathcal{N}_1 \otimes \mathcal{N}_2\|_{1\to p} \stackrel{?}{=} \|\mathcal{N}_1\|_{1\to p}\|\mathcal{N}_2\|_{1\to p},$$

at least for p fairly close to 1. This is equivalent to the question of additivity of *minimum* output Rényi p-entropies, which are defined in terms of maximum output p-norms as

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

The minimum output Rényi ∞-entropy of $\mathcal{N}$ is defined as $H_\infty^{\min}(\mathcal{N}) = -\log\|\mathcal{N}\|_{1\to\infty}$, while the minimum output (von Neumann) entropy $H^{\min}(\mathcal{N})$ is obtained by taking the limit $p \to 1$ [1]. This case of the additivity question was of particular interest due to its connections with many other additivity problems in quantum information theory [10]. All of these multiplicativity/additivity conjectures are now known to be false [11, 12, 7, 8, 6].

As well as the limit $p \to 1$, another important special case of the multiplicativity question is $p = \infty$, which turns out to be closely related to a number of other quantities studied in quantum information theory, as we now discuss. By the Stinespring dilation, any quantum channel performing a map from a d_A-dimensional quantum system A to a d_B-dimensional quantum system B can be written as $\mathcal{N}(\rho) = \operatorname{tr}_E V\rho V^\dagger$ for some isometry $V : \mathbb{C}^{d_A} \to \mathbb{C}^{d_B}\otimes\mathbb{C}^{d_E}$. Let $\mathrm{SEP} \subset \mathcal{B}(\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_E})$ be the set of $d_B \times d_E$-dimensional separable quantum states. For any operator $M \in \mathcal{B}(\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_E})$ such that $0 \leq M \leq I$, the quantity

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

is known as the support function of the separable states, evaluated at M. This quantity has the following connection to maximum output p-norms of quantum channels, which can easily be proven using the Schmidt decomposition:

Fact 1. *Let $\mathcal{N}$ be a quantum channel with corresponding isometry V, and set $M = VV^\dagger$. Then $h_{\mathrm{SEP}}(M) = \|\mathcal{N}\|_{1\to\infty}$.*

The quantity h_{SEP} is crucially important in the study of multiple-prover quantum Merlin-Arthur games [9, 5]. Indeed, projectors M such that $h_{\mathrm{SEP}}(M^{\otimes n}) = h_{\mathrm{SEP}}(M)^n$ correspond to measurement operators occurring in two-prover quantum Merlin-Arthur games (called QMA(2) protocols) which obey *perfect parallel repetition*, i.e. where Arthur can simply repeat the protocol n times in parallel

[1]Centre for Quantum Information and Quantum Foundations, Department of Applied Mathematics and Theoretical Physics, University of Cambridge, UK; am994@cam.ac.uk.

to reduce a soundness error (failure probability) of s to a soundness error of s^n. The failure of multiplicativity of $\|\mathcal{N}\|_{1\to\infty}$ implies that such a precise form of parallel repetition cannot hold in general; however, it could still be the case that a weaker form of parallel repetition holds, where $h_{\mathrm{SEP}}(M^{\otimes n})$ necessarily decreases exponentially with n.

Counterexamples to multiplicativity. The construction used by [8] to falsify p-norm multiplicativity for all $p > 1$ is to choose the first channel $\mathcal{N}$'s corresponding subspace $S \subset \mathbb{C}^d \otimes \mathbb{C}^d$ at random from the set of all subspaces of dimension $r = O(d^{1+1/p})$ (i.e. according to Haar measure on the unitary group), and to take $\overline{\mathcal{N}}$ as the second channel.

In the case $p = \infty$, the violation of multiplicativity displayed by this construction is near-maximal. That is,

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

However, this example leaves open the question of the general behaviour of $\|\mathcal{N}^{\otimes n}\|_{1\to p}$ for larger n. To the author's knowledge, two extreme situations are still possibilities: on the one hand, it might hold that

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

for all $\mathcal{N}$; alternatively, there might be no universal constant α such that, for all channels $\mathcal{N}$,

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

The former possibility would imply that the largest possible violation of multiplicativity is quite mild, and in the case $p = \infty$ that a form of parallel repetition holds for QMA(2) protocols; the latter would mean that severe violations are possible and parallel repetition fails.

Main result. The main result of this work is that, even though in certain regimes almost all quantum channels do not obey multiplicativity, the violations of multiplicativity displayed by random channels are in some sense actually very weak. The result can be summarised informally as follows. For random channels $\mathcal{N}$ satisfying some mild dimensionality constraints, and for any $n \geq 1$, with high probability

$$\|\mathcal{N}^{\otimes n}\|_{1\to p} \leq \|\mathcal{N}\|_{1\to p}^{(1/2-o(1))(1-1/p)n}.$$

We stress that this result holds for all n, and the $o(1)$ term goes to 0 with the dimension of the space on which $\mathcal{N}$ acts, rather than with n. In the case $p = \infty$, this implies that almost all QMA(2) protocols obey a form of parallel repetition.

In certain regimes, by monotonicity of Rényi entropies our results imply a weak *additivity* result for the minimum output von Neumann entropy. Let the dimension of the output subspace of $\mathcal{N}$ in the Stinespring picture be r. Then if $r = \Theta(d_B) = \Theta(d_E)$ (roughly speaking, this is the setting of the random counterexamples to additivity given in [8, 6]), we obtain that

$$\frac{1}{n} H^{\min}(\mathcal{N}^{\otimes n}) \geq \frac{1}{2} H^{\min}(\mathcal{N}) - O(1)$$

with high probability. This is perhaps the strongest additivity result one could expect for random channels, given the counterexamples of [8, 6] (although, strictly speaking, in this prior work the pair $(\mathcal{N}, \overline{\mathcal{N}})$ is considered rather than multiple copies of $\mathcal{N}$).

Proof techniques. The proof of the main result is based on a general upper bound strategy for $h_{\mathrm{SEP}}(M)$. Maximising over the set of separable states is a daunting task, and a useful relaxation is to maximise over the larger set of PPT states (bipartite quantum states ρ such that $\rho^\Gamma \geq 0$, where $^\Gamma$ denotes the partial transpose operation, i.e. the transpose operation performed only on the second subsystem) and consider

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

We observe the following upper bound on this quantity.

Proposition 2. $h_{\mathrm{PPT}}(M) \leq \|M^\Gamma\|_\infty$.

A key property of $\|M^\Gamma\|_\infty$ which we use is that it is multiplicative: for any operators M, N, $\|(M \otimes N)^\Gamma\|_\infty = \|M^\Gamma \otimes N^\Gamma\|_\infty = \|M^\Gamma\|_\infty \|N^\Gamma\|_\infty$. Thus, if we can show that $\|M^\Gamma\|_\infty \leq \delta$ for some δ, we immediately have that $h_{\mathrm{SEP}}(M^{\otimes n}) \leq \delta^n$. If δ is small enough with respect to $h_{\mathrm{SEP}}(M)$, this can be used to prove that the channel corresponding to M obeys a weak version of ∞-norm multiplicativity. By Hölder's inequality, this implies weak multiplicativity results for all other maximum output p-norms.

It is easy to find a suitable general lower bound on $h_{\mathrm{SEP}}(M)$; the main technical contribution of this paper is to show a strong upper bound on $\|M^\Gamma\|_\infty$ which holds with high probability. In order to do this, we prove tail bounds on $\|M^\Gamma\|_\infty$ using the method of moments from random matrix theory. In other words, we develop bounds on the quantity $\mathbb{E} \operatorname{tr}[(M^\Gamma)^k]$ for arbitrary even k, where M is the projector onto a Haar-random subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$. This is equivalent to bounding the quantity $\operatorname{tr}[D(\kappa)^\Gamma M^{(k)}]$, where $\kappa \in S_k$ is a cyclic permutation, $D(\kappa)$ is the corresponding permutation of k $(d_B d_E)$-dimensional systems, and

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

with M_0 being the projector onto an arbitrary fixed dimension r subspace of $\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}$. By Schur-Weyl duality, the operator $M^{(k)}$ can be expanded in terms of permutations $D(\pi)$ of k $(d_B d_E)$-dimensional systems, where $\pi \in S_k$, i.e.

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

for some coefficients α_π. This implies that

$$\operatorname{tr}[D(\kappa)^\Gamma M^{(k)}] = \sum_{\pi \in S_k} d_B^{c(\kappa\pi)} d_E^{c(\kappa^{-1}\pi)} \alpha_\pi, \tag{1}$$

where $c(\pi)$ is the number of cycles of $\pi \in S_k$. The coefficients $\alpha_\pi \approx r^{c(\pi)}/(d_B d_E)^k$ can be explicitly calculated in terms of the so-called Weingarten function [4]. In order to find a strong enough bound on these coefficients, we give a new upper bound on the Weingarten function, which we hope will find uses elsewhere. And to finally complete the upper bound on eqn. (1), we prove bounds on the combinatorics of permutations.

Conclusions. We have shown that random channels obey a weak variant of multiplicativity with high probability. When combined with the results of Christandl, Schuch and Winter [2, 3] on the antisymmetric subspace, this implies that two of the constructions of channels which display the strongest known two-copy multiplicativity violations are in fact weakly multiplicative when the number of copies increases. This naturally leads one to conjecture that in fact *all* channels satisfy some form of weak multiplicativity (see [6] for a similar conjecture). This is an intriguing open problem.

References

[1] G. Amosov, A. Holevo, and R. Werner. On some additivity problems in quantum information theory, 2000. `math-ph/0003002`.

[2] M. Christandl, N. Schuch, and A. Winter. Entanglement of the antisymmetric state, 2009. `arXiv:0910.4151`.

[3] M. Christandl, N. Schuch, and A. Winter. Highly entangled states with almost no secrecy. *Phys. Rev. Lett.*, 104:240405, 2010. `arXiv:1101.4522`.

[4] B. Collins and P. Śniady. Integration with respect to the Haar measure on unitary, orthogonal and symplectic group. *Comm. Math. Phys.*, 264:773–795, 2006. `math-ph/0402073`.

[5] A. Harrow and A. Montanaro. An efficient test for product states, with applications to quantum Merlin-Arthur games. In *Proc. 51st Annual Symp. Foundations of Computer Science*, pages 633–642, 2010. `arXiv:1001.0017`.

[6] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5:255, 2009. `arXiv:0809.3972`.

[7] P. Hayden. The maximal p-norm multiplicativity conjecture is false, 2007. `arXiv:0707.3291`.

[8] P. Hayden and A. Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all p $>$ 1. *Comm. Math. Phys.*, 284(1):263–280, 2008.

[9] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: are multiple Merlins more helpful to Arthur? In *Proc. ISAAC '03*, pages 189–198, 2003. `quant-ph/0306051`.

[10] P. W. Shor. Equivalence of additivity questions in quantum information theory. *Comm. Math. Phys.*, 246(3):453–472, 2004. `quant-ph/0305035`.

[11] R. Werner and A. Holevo. Counterexample to an additivity conjecture for output purity of quantum channels, 2002. `quant-ph/0203003`.

[12] A. Winter. The maximum output p-norm of quantum channels is not multiplicative for any p$>$2, 2007. `arXiv:0707.0402`.