

Counterexamples to additivity of minimum output p -Rényi entropy for p close to 0

Toby Cubitt,¹ Aram W. Harrow,² Debbie Leung,³ Ashley Montanaro,² and Andreas Winter^{1,4}

¹Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.

²Department of Computer Science, University of Bristol, Bristol BS8 1UB, U.K.

³Institute for Quantum Computing, University of Waterloo, Waterloo N2L 3G1, Ontario, Canada

⁴Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542*

(Dated: 22nd January 2008)

Complementing recent progress on the additivity conjecture of quantum information theory, showing that the minimum output p -Rényi entropies of channels are not generally additive for $p > 1$, we demonstrate here by a careful random selection argument that also at $p = 0$, and consequently for sufficiently small p , there exist counterexamples.

An explicit construction of two channels from 4 to 3 dimensions is given, which have non-multiplicative minimum output rank; for this pair of channels, numerics strongly suggest that the p -Rényi entropy is non-additive for all $p \lesssim 0.11$. We conjecture however that violations of additivity exist for all $p < 1$.

I. INTRODUCTION AND DEFINITIONS

For a quantum channel (i.e. a completely positive and trace preserving linear map) \mathcal{N} between finite quantum systems, and $p \geq 0$, define

$$S_p^{\min}(\mathcal{N}) := \min_{\rho} \frac{1}{1-p} \log \text{Tr}(\mathcal{N}(\rho))^p,$$

where the minimisation is over all states (normalised density operators) on the input space of \mathcal{N} . The quantity $S_p(\sigma) = \frac{1}{1-p} \log \text{Tr} \sigma^p$ is known as p -Rényi entropy of the state σ ($0 < p < \infty$ and $p \neq 1$), with the definition extended to $p = 0, 1, \infty$ by taking limits; $S_1(\sigma) = S(\sigma) = -\text{Tr} \sigma \log \sigma$ is the von Neumann entropy. $S_\infty(\sigma) = -\log \|\sigma\|_\infty$ is the min-entropy, and $S_0(\sigma) = \log \text{rank} \sigma$. Due to the concavity of the Rényi entropies in ρ , the minimum in the above definition is attained at a pure input state $\rho = |\psi\rangle\langle\psi|$.

The additivity problem is the question whether for all channels \mathcal{N}_1 and \mathcal{N}_2 , it holds that

$$S_p^{\min}(\mathcal{N}_1 \otimes \mathcal{N}_2) \stackrel{?}{=} S_p^{\min}(\mathcal{N}_1) + S_p^{\min}(\mathcal{N}_2). \quad (1)$$

Note that the direction “ \leq ” here is trivial, so proofs and counterexamples have to concentrate on the direction “ \geq ”. This was indeed proved for special channels and some p ; for example, it is known for $p \geq 1$ if one of the channels is entanglement-breaking [1, 2], unital on a qubit space [3], or depolarising of any dimension [4]; in addition for a number of other cases. King [5] has furthermore shown that it holds for $p < 1$ if one of the channels is entanglement-breaking. Holevo and Werner [6] exhibited the first counterexamples to eq. (1), for $p > 4.79$. It was demonstrated recently [7, 8] that for every $p > 1$ there exist channels violating eq. (1).

Here we show that eq. (1) is also false at $p = 0$, and by continuity of S_p in p , it is thus violated for all $p \leq p_0$ with some small but positive p_0 . Since $S_0(\sigma)$ is the logarithm of the rank of the density matrix σ , so $S_0^{\min}(\mathcal{N})$ is the logarithm of the minimum output rank of the channel, i.e. of the smallest rank of an output state. In the next Section we prove our main existence result of counterexamples, in Section III we exhibit an explicit example, and in Section IV we explore up to which $p < 1$ we can violate additivity of S_p^{\min} .

II. MAIN RESULT

Theorem 1 *If $d_A > 2$, $d_B > 2$ and $d_A d_B$ is even then there exist quantum channels $\mathcal{N}_1, \mathcal{N}_2$ with d_A -dimensional input spaces and d_B -dimensional output spaces, such that*

$$S_0^{\min}(\mathcal{N}_1) = S_0^{\min}(\mathcal{N}_2) = \log d_B,$$

*Electronic address: a.j.winter@bris.ac.uk

but

$$S_0^{\min}(\mathcal{N}_1 \otimes \mathcal{N}_2) \leq \log(d_B^2 - 1) < 2 \log d_B.$$

Proof. Our approach is the following: let $\rho_{AB} = (\text{id} \otimes \mathcal{N})\Psi$ be a Choi-Jamiołkowski state of the channel \mathcal{N} , with a particular choice of reference state $|\Psi\rangle \in A \otimes B = \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Note that while usually people use a fixed maximally entangled state, for the isomorphism it is sufficient that it is of maximal Schmidt rank. In [7, 8], additivity counterexamples were found for $p > 1$ by choosing \mathcal{N} randomly subject to a certain constraint. Our approach will be instead to choose the Choi-Jamiołkowski state randomly, again subject to a certain constraint that helps guarantee the additivity counterexample.

First note that $\mathcal{N}(\varphi)$ has maximal rank d_B for every input state φ iff the orthogonal complement of ρ doesn't contain any product vectors, i.e. for all pure states $|\varphi\rangle \in A$, $|\psi\rangle \in B$,

$$\text{Tr}(\rho_{AB}(\varphi \otimes \psi)) \neq 0. \quad (2)$$

The easy justification of this is as follows: in Appendix A we show that the action of the channel \mathcal{N} can be written

$$\mathcal{N}(\varphi) = \text{Tr}_A \left[\rho_{AB} \left(\rho_A^{-1/2} U^\dagger \bar{\varphi} U \rho_A^{-1/2} \otimes \mathbf{1} \right) \right], \quad (3)$$

where $\bar{\cdot}$ denotes the complex conjugate with respect to a fixed computational basis and U is a unitary depending on Ψ (see Appendix A for details). Full rank of the output means that for all pure states φ, ψ ,

$$\begin{aligned} 0 &\neq \text{Tr}(\mathcal{N}(\varphi)\psi) \\ &= \text{Tr} \left[\rho_{AB} \left(\rho_A^{-1/2} U^\dagger \bar{\varphi} U \rho_A^{-1/2} \otimes \psi \right) \right] \\ &\propto \text{Tr}[\rho_{AB}(\varphi' \otimes \psi)], \end{aligned}$$

where we used the above identity and the fact that $\rho_A^{-1/2} U^\dagger \bar{\varphi}$ is, up to normalisation, another pure state $|\varphi'\rangle$. Note that *any* unitary U on A will serve to create a channel, so we shall fix it to be the identity from now on – this is only a matter of redefining Ψ_{AB} , which we can do if only given ρ_{AB} .

So, our task is to find two states ρ_{AB} and $\sigma_{A'B'}$ on $A \otimes B$ with this property, such that $\omega_{AA'BB'} = \rho_{AB} \otimes \sigma_{A'B'}$ does *have* a product state in its orthogonal complement; we'll choose it to be the maximally entangled state $\Phi_{AA'} \otimes \Phi_{BB'}$. Then the condition we seek to enforce is

$$0 = \text{Tr}((\rho_{AB} \otimes \sigma_{A'B'}) (\Phi_{AA'} \otimes \Phi_{BB'})) = \frac{1}{d_A d_B} \text{Tr}(\rho \sigma^\top),$$

where \top signifies the matrix transpose. Note that the channel input will not be $\Phi_{AA'}$, but rather the normalised version of $(\sqrt{\rho_A} \otimes \sqrt{\sigma_{A'}}) |\Phi\rangle_{AA'}$.

What we will do is simply pick ρ to be the (normalised) projection onto a $d_A d_B / 2$ -dimensional random subspace, drawn according to the unitary invariant measure on AB , and σ^\top the (normalised) projection onto the orthogonal complement of ρ :

$$\rho = \frac{2}{d_A d_B} \Pi, \quad \sigma = \frac{2}{d_A d_B} (\mathbf{1} - \Pi^\top).$$

This enforces the condition $\text{Tr}(\rho \sigma^\top) = 0$ deterministically, while both the supporting subspaces of ρ and σ are individually uniformly random. Thus we are done once we prove Lemma 2, stated below, since it implies for large enough d_A and d_B , that with probability 1 neither the orthogonal complement of ρ nor that of σ (which are themselves uniformly random subspaces) contains a product vector. \square

Lemma 2 *Let Π be a uniformly random projector in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ of rank d_E such that $d_A d_B > d_A + d_B + d_E - 2$. Then,*

$$\Pr_{\Pi} \{ \exists \varphi_A \in \mathbb{C}^{d_A}, \varphi_B \in \mathbb{C}^{d_B} \text{Tr}((\varphi_A \otimes \varphi_B) \Pi) = 1 \} = 0. \quad (4)$$

In words: the probability that a random subspace of “small” dimension contains a product state, is zero.

Proof. Note that if $d_A d_B$ is even then $d_E = d_A d_B / 2$ is an integer, and so the inequality $(d_A - 2)(d_B - 2) > 0$ can be rearranged to obtain $d_A d_B > d_A + d_B + d_E - 2$, thus justifying the application to Theorem 1.

Geometrically, we want to show that the probability for a random subspace of dimension d_E to contain a product state, is zero. Using the isomorphism between bipartite vectors and $d_A \times d_B$ -matrices (which identifies Schmidt rank with matrix rank) [9], we can reformulate the task as describing the d_E -dimensional subspaces of $d_A \times d_B$ -matrices not containing any nonzero elements of rank 1. In other words, subspaces intersecting the *determinantal variety* of vanishing 2×2 -minors only in the zero matrix. The dimension of this variety – known as the Segre embedding – is easily seen to be $d_A + d_B - 1$, so a generic subspace of dimension $d_E \leq d_A d_B - (d_A + d_B - 1) = (d_A - 1)(d_B - 1)$ will not intersect it except trivially, by standard algebraic-geometric arguments [10, 11]; a more explicit argument for this fact was given recently by Walgate and Scott [12]. \square

III. AN EXPLICIT CONSTRUCTION IN SMALL DIMENSION

Since our additivity violation takes the form of only a single zero eigenvalue in the two-copy output, it is strongest when the channel dimensions are smallest. Indeed, violations for large dimension can be constructed from channels from small dimension by tensoring the channel with a trivial channel, such as a completely depolarising channel. Thus, we are most interested in finding counterexamples with small dimension.

One such counterexample, with $d_A = 4$ and $d_B = 3$ is described here. Based on the constructions in [9], and indeed a slight variation of it, we show now – using the same methodology as above – how to construct two channels $\mathcal{N}_i : \mathcal{B}(\mathbb{C}^4) \rightarrow \mathcal{B}(\mathbb{C}^3)$ ($i = 1, 2$) such that

$$S_0^{\min}(\mathcal{N}_1) = S_0^{\min}(\mathcal{N}_2) = \log 3, \quad \text{but } S_0^{\min}(\mathcal{N}_1 \otimes \mathcal{N}_2) \leq \log 8 < 2 \log 3.$$

These happen to be the smallest dimensions that satisfy Lemma 2.

As we have discussed above, we describe them via their Jamiołkowski states ρ_{AB} and σ_{AB} (with A and B being a 4- and 3-dimensional system, respectively) such that $\text{Tr } \rho \sigma^\top = 0$ and neither ρ nor σ contains a product state in the respective orthogonal complement of their supports.

Resorting to the supporting subspaces of ρ and σ^\top , denoted $R, S < A \otimes B$, respectively, we have nothing to do but choose them to be orthogonal and of dimension 6, such that neither contains a product state.

Using the customary notation of vectors in $\mathbb{C}^4 \times \mathbb{C}^3$ as 3×4 matrices [9], and with $\omega = e^{2\pi i/3}$, we let R be spanned by

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & \omega & & \\ & & \omega^2 & 0 \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & & \\ & & \omega^2 & \\ & & & \omega \\ & & & & \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & \\ & & & -1 \\ & & & & \end{bmatrix}, \text{ and } \begin{bmatrix} & 0 & 0 & 1 \\ & 0 & & \\ & & & \\ -1 & & & \end{bmatrix};$$

whereas S is spanned by

$$\begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & 0 \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & \omega^2 & & \\ & & \omega & 0 \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & & \\ & & 1 & \\ & & & 1 \\ & & & & \end{bmatrix}, \begin{bmatrix} 0 & 1 & & \\ & & \omega & \\ & & & \omega^2 \\ & & & & \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & \\ & & & 1 \\ & & & & \end{bmatrix}, \text{ and } \begin{bmatrix} & 0 & 0 & 1 \\ & 0 & & \\ & & & \\ 1 & & & \end{bmatrix}.$$

Since these twelve vectors are clearly orthogonal, the subspaces R and S are each of dimension 6, and orthogonal to each other; the proof that they don't contain a product state is as follows: the first five vectors of R and S span respective 5-dimensional subspaces R_0 and S_0 . Notice that they are entirely symmetric to each other, and that they don't contain product states by the arguments of [9]. Also, the sixth vector is clearly not product in either case. Hence, to obtain a product vector in R , say (the argument for S is very similar), we need to form the sum of the sixth vector with an element from R_0 :

$$\begin{aligned} M &= \alpha \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ & & & 0 \end{bmatrix} + \beta \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ & & & 0 \end{bmatrix} + \gamma \begin{bmatrix} 1 & & & \\ & \omega & & \\ & & \omega^2 & 0 \\ & & & 0 \end{bmatrix} + \delta \begin{bmatrix} 0 & 1 & & \\ & & \omega^2 & \\ & & & \omega \\ & & & & \end{bmatrix} + \varepsilon \begin{bmatrix} 0 & 0 & 1 & \\ & & & -1 \\ & & & & \end{bmatrix} \\ &\quad + \begin{bmatrix} & 0 & 0 & 1 \\ & 0 & & \\ & & & \\ -1 & & & \end{bmatrix} \\ &= \begin{bmatrix} \beta + \gamma & & \delta & \varepsilon & 1 \\ \alpha & \beta + \omega\gamma & & \omega^2\delta & -\varepsilon \\ -1 & & \alpha & \beta + \omega^2\gamma & \omega\delta \end{bmatrix} \end{aligned}$$

For this to be a product vector, all its 2×2 -minors have to vanish, but we need to look at only a few to obtain a contradiction: the minors $\{1, 2\} \times \{3, 4\}$, $\{1, 3\} \times \{2, 4\}$ and $\{2, 3\} \times \{1, 4\}$ imply $0 = -\varepsilon^2 - \omega^2\delta = \omega\delta^2 - \alpha = \omega\alpha\delta - \varepsilon$, which in turn allow us to express all other variables in terms of ε :

$$\delta = -\omega\varepsilon^2, \quad \alpha = \omega\delta^2 = \varepsilon^4, \quad \varepsilon = \omega\alpha\delta = -\omega^2\varepsilon^6,$$

leaving for ε only the possibilities of being 0 or a fifth root of $-\omega^2$. If $\varepsilon = 0$, so are α and δ , and in this case the $\{1, 3\} \times \{1, 3\}$ -minor is non-vanishing. Hence we continue with $\varepsilon^5 = -\omega^2$, and look at the minors $\{1, 3\} \times \{1, 4\}$, $\{1, 2\} \times \{2, 4\}$ and $\{1, 3\} \times \{3, 4\}$: these yield the constraints

$$0 = (\beta + \gamma)\omega\delta + 1 = -\delta\varepsilon - (\beta + \omega\gamma) = \omega\delta\varepsilon - (\beta + \omega^2\gamma),$$

in other words

$$\beta + \gamma = -\omega^2/\delta = \omega/\varepsilon^2 = -\omega^2\varepsilon^3, \quad \beta + \omega\gamma = -\delta\varepsilon = \omega\varepsilon^3, \quad \beta + \omega^2\gamma = \omega\delta\varepsilon = -\omega^2\varepsilon^3,$$

which implies $\gamma = 0$ and $\beta = -\omega^2\varepsilon^3$ from the 1st and 3rd equation, but then the 2nd contradicts by demanding $\beta = \omega\varepsilon^3$.

Hence, in conclusion, R cannot contain a product state, and the argument for S is similar in nature. \square

IV. LARGER RÉNYI PARAMETER

Now we can use the explicit pair of channels constructed in the previous section to look for larger values of p for which additivity of S_p^{\min} is violated. The simplest thing is to take the Choi-Jamiołkowski states to be the normalised projections onto the subspaces R and S , respectively. However, we may clearly take *any* state of rank 6 supported on the respective subspace to obtain a bona fide generalised Choi-Jamiołkowski state. We performed some numerics in both cases: for the first (Jamiołkowski states proportional to the subspace projections), using $S((\mathcal{N} \otimes \mathcal{N}')\Phi_3)$ as an upper bound of $S_p^{\min}(\mathcal{N} \otimes \mathcal{N}')$ and numerical calculations of $S_p^{\min}(\mathcal{N})$ and $S_p^{\min}(\mathcal{N}')$, we see violations of additivity for values of p up to ≈ 0.096 .

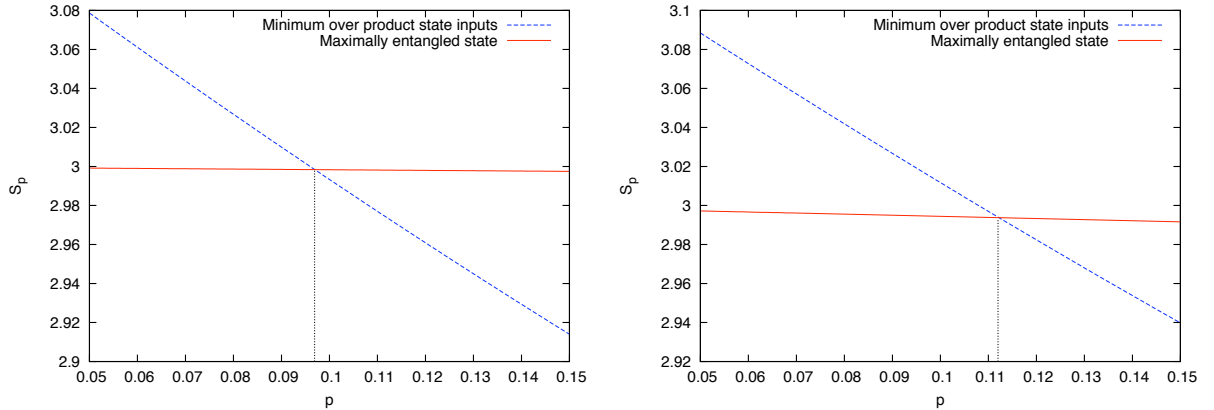


FIG. 1: Plots of the output entropy of the tensor product channel with the input state corresponding to the maximally entangled state (red line, shallow slope), versus the numerically obtained minimum when restricted to tensor product input states (blue line, steep slope). On the left the Choi-Jamiołkowski states are simply the normalised projections of the subspaces R and S ; on the right, one chooses appropriately weighted density operators with support R and S , respectively.

For the second, it turns out that a very good choice is to have ρ_{AB} and $\sigma_{A'B'}$ to be diagonal in the above bases of R and S , respectively, with specific probability weights obtained by another numerical search. The weights of the basis vectors of R and S , in the above order, are

$$0.172776, 0.118738, 0.199229, 0.136705, 0.306899, 0.0656529, \text{ and} \\ 0.344911, 0.124908, 0.120721, 0.156968, 0.162754, 0.089738,$$

respectively. This results in a numerical violation of additivity for p up to ≈ 0.112 . We see no reason to believe that this value should be the limit of additivity violations.

To obtain a rigorous interval $[0; p_0]$ of violations of additivity, we turn to the ideas of measure concentration explored in [13] in the context of quantum information theory. We will not make everything explicit, but the idea is as follows: we need to put rather tight lower bounds on S_p^{\min} of the two individual channels; in fact, each of the two channels $\mathcal{N}, \mathcal{N}'$ is individually random from the class of channels with Stinespring dilations $A \hookrightarrow B \otimes \mathbb{C}^{d_A d_B/2}$ (random meaning: according to the unitary invariant measure on $B \otimes \mathbb{C}^{d_A d_B/2}$). For the output properties of each the channels, only the embedded d_A -dimensional subspace $S, S' < B \otimes \mathbb{C}^{d_A d_B/2}$ is relevant, which is a random subspace in the same sense [13].

Now in [13], Lemmas III.4 and III.6, it is shown that the spectrum of all states in a random subspace $S < B \otimes \mathbb{C}^{d_A d_B/2}$ is tightly concentrated around the value $1/d_B$, for large enough dimensions d_A and d_B such that $d_A \gg d_B \geq \Omega(\log d_A)$. I.e., with high probability the minimum Schmidt coefficient of any state in S, S' is, say, $\geq \frac{1}{2} \frac{1}{d_B}$. In other words, the output states of the channels have spectrum bounded away from 0 by this amount. Then for $0 \leq p < 1$, clearly,

$$\begin{aligned} S_p^{\min}(\mathcal{N}), S_p^{\min}(\mathcal{N}') &> \frac{1}{1-p} \log \left(d_B \left(\frac{1}{2d_B} \right)^p \right) \\ &= \log d_B + \frac{p}{1-p} \log \frac{1}{2} = \log d_B - \frac{p}{1-p}. \end{aligned}$$

However,

$$S_p^{\min}(\mathcal{N} \otimes \mathcal{N}') \leq S_0^{\min}(\mathcal{N} \otimes \mathcal{N}') \leq \log(d_B^2 - 1) = 2 \log d_B + \log \left(1 - \frac{1}{d_B^2} \right).$$

In conclusion, a violation is obtained as soon as

$$\frac{2p}{1-p} \leq -\log \left(1 - \frac{1}{d_B^2} \right),$$

which follows if $p \leq \frac{1}{1+2 \ln 2 d_B^2}$. We omit here any estimate of the d_B required in the above concentration of reduced state spectrum, which depends on the exact constants one uses in the probability bounds, but it is possible by this approach to get p_0 in the range of 10^{-3} to 10^{-2} .

There is yet another way to get rigorous estimates of p_0 for every example, like for the explicit construction in the previous section. Namely, get a lower bound on the minimum minimal eigenvalue of an output state of the single copy channel \mathcal{N} , which can be relaxed to a convex optimisation problem, and then use the argument above.

In detail, consider the usual Choi-Jamiołkowski operator of the channel, $\Omega_{AB} = (\text{id} \otimes \mathcal{N})\Gamma$, with $|\Gamma\rangle = \sum_{i=1}^{d_A} |i\rangle|i\rangle$. Then, $\mathcal{N}(\varphi) = \text{Tr}_A[\Omega_{AB}(\varphi \otimes \mathbb{1})]$ (see Appendix A), and

$$\begin{aligned} \min_{\varphi} \lambda_{\min}(\mathcal{N}(\varphi)) &= \min_{\varphi, \psi} \text{Tr}[\Omega_{AB}(\varphi \otimes \psi)] = \min_{\rho \text{ separable}} \text{Tr}[\Omega_{AB}\rho] \\ &\geq \min_{\rho \text{ PPT}} \text{Tr}[\Omega_{AB}\rho]. \end{aligned}$$

The latter is a semidefinite program, so duality theory will yield rigorous lower bounds on the minimum minimal eigenvalue of an output state. Doing that for our example in Section III, yields again a rather poor bound for p_0 of the order 10^{-2} .

V. DISCUSSION

After the disproof of the additivity conjecture for S_p^{\min} at $p > 1$, and the close shave by which the original and main conjecture at $p = 1$ has escaped, some hope was raised that one could prove additivity for $p < 1$, and hence by taking the limit for $p = 1$. This suggestion didn't seem so unreasonable after King [5] showed additivity if one of the channels is entanglement-breaking. Also, it can be seen quite easily that arbitrary numbers of copies of the Holevo-Werner channel [6] obey additivity for $p \leq 1$, via the result of [14]. In this respect the log of the minimum output rank, S_0^{\min} , took prominence as an important test case, and the finding of a counterexample here is putting into doubt possible programmes to prove the "standard additivity conjectures" by approaching $p = 1$ from below.

We feel that, with the minimum output rank not multiplicative, it is rather unlikely that any of the S_p^{\min} for $p < 1$ should be additive. It is to be noted however, that the present technique doesn't really yield massive violations of

additivity, even at $p = 0$, and presumably less so at other $0 < p < 1$. This is in contrast to what one observes at $p > 1$ [7, 8], but it can be understood pretty well in terms of control by the random selection to engineer a certain conspiracy between the two channels: while for $p > 1$ we only need to fix one large eigenvalue of the two-copy output corresponding to the maximally entangled input state, at $p < 1$ (and most extremely so at $p = 0$) *all* non-zero eigenvalues are relevant, and even to make d of them zero exhausts the possibilities of the random selection performing well on the single-copy level. It is amusing to note, however, that we still exploit the peculiar symmetries, and indeed the multiplicativity, of the maximally entangled state to construct a violation.

It is our hope that the present work will spark the search for further counterexamples, potentially finding a unified principle behind the constructions for $p > 1$ and $p < 1$ – and eventually helping to decide the original additivity conjecture(s) at $p = 1$. Note that the construction presented here and in [7, 8] share already a couple of important traits. First, the candidate channels are individually random from the unitary invariant ensemble of Stinespring dilations with fixed input, output and environment dimensions – to get strong lower bounds on the minimum output entropy. Second, the pair of channels is chosen to be in some fixed relation to each other, so as to make the output state corresponding to the maximally entangled input (or, in our case, something very close to it) special; for $p > 1$ we want it to have an unusually large eigenvalue (which is why we choose the channels to be complex conjugate to each other), here we want an eigenvalue to vanish (which is why we impose orthogonality on the Choi-Jamiołkowski states). The possible extension or unification of the constructions thus is not so much how they are individually selected, but has to address the way the two channels are related to each other.

Note added. After this work was presented at the AQIS'07 workshop in Kyoto (September 2007), Duan and Shi [15] used the methodology of our explicit construction in their surprising results on quantum zero-error capacity; they also exhibit a single channel from 4 to 4 dimensions violating additivity of S_0^{\min} – as opposed to our using the tensor product of two different channels – in the sense that $S_0^{\min}(\mathcal{N}^{\otimes 2}) < 2S_0^{\min}(\mathcal{N})$.

Acknowledgments

The authors thank Patrick Hayden, Richard Low, Koenraad Audenaert, Runyao Duan and Yaoyun Shi for their interest in the present work, and encouraging as well as interesting discussions.

AWH and AW acknowledge support by the European Commission under a Marie Curie Fellowship (ASTQIT, FP-022194). TC, AWH, AM and AW acknowledge support through the integrated EC project “QAP” (contract no. IST-2005-15848), as well as by the U.K. EPSRC, project “QIP IRC”. AH was furthermore supported by the Army Research Office under grant W9111NF-05-1-0294. DL thanks NSERC, CRC, CFI, ORF, MITACS, ARO, and CIFAR for support. AW furthermore acknowledges support through an Advanced Research Fellowship of the U.K. EPSRC and a Royal Society Wolfson Research Merit Award.

APPENDIX A: CHOI-JAMIOLKOWSKI STATES

Here we give a detailed explanation of eq. (3) by describing how the channel can be recovered from our non-standard Choi-Jamiołkowski operator.

Recall how to reconstruct the channel from the “standard” Choi-Jamiołkowski operator $\Omega_{AB} = (\text{id} \otimes \mathcal{N})\Gamma$, where $|\Gamma\rangle = \sum_{i=1}^d |i\rangle|i\rangle$. The key is the identity

$$\mathcal{N}(\varphi) = \text{Tr}_A[\Omega_{AB}(\bar{\varphi} \otimes \mathbf{1})],$$

with the complex conjugation with respect to the basis $\{|i\rangle\}_{i=1}^d$ denoted by $\bar{\cdot}$.

Now, if we have any entangled state $|\Psi\rangle$ of maximal Schmidt rank, it has a Schmidt form

$$|\Psi\rangle = \sum_{i=1}^d \sqrt{\lambda_i} |e_i\rangle_A |f_i\rangle_B,$$

with local bases $\{|e_i\rangle_A\}_{i=1}^d$ and $\{|f_i\rangle_B\}_{i=1}^d$, and strictly positive Schmidt coefficients $\lambda_i > 0$. This means that $\Psi_A = \text{Tr}_B \Psi_{AB} = \sum_i \lambda_i |e_i\rangle\langle e_i|$ has full rank (in particular it is invertible), so its inverse is well-defined, and

$$\left(\Psi_A^{-1/2} \otimes \mathbf{1}\right) |\Psi\rangle_{AB} = \sum_i |e_i\rangle |f_i\rangle.$$

Thus, introducing the unitary basis change $U : |e_i\rangle \mapsto |\bar{f}_i\rangle$, we finally get

$$\left(U \Psi_A^{-1/2} \otimes \mathbb{1} \right) |\Psi\rangle_{AB} = \sum_i |\bar{f}_i\rangle |f_i\rangle = \sum_i |i\rangle |i\rangle = |\Gamma\rangle,$$

due to the $U \otimes \bar{U}$ -invariance of $|\Gamma\rangle$.

So, since the mapping from Ψ to Γ only acts on A while the Choi-Jamiołkowski mapping acts only on B , and using the fact that $\rho_A = \Psi_A$ for the generalised Choi-Jamiołkowski state $\rho_{AB} = (\text{id} \otimes \mathcal{N})\Psi_{AB}$, we finally find that we can recover the “standard” operator Ω_{AB} as

$$\Omega_{AB} = \left(U \Psi_A^{-1/2} \otimes \mathbb{1} \right) \rho_{AB} \left(\Psi_A^{-1/2} U^\dagger \otimes \mathbb{1} \right).$$

In other words, using the above identities, the channel can be written

$$\begin{aligned} \mathcal{N}(\varphi) &= \text{Tr}_A [\Omega_{AB} (\bar{\varphi} \otimes \mathbb{1})] \\ &= \text{Tr}_A \left[\left(U \Psi_A^{-1/2} \otimes \mathbb{1} \right) \rho_{AB} \left(\Psi_A^{-1/2} U^\dagger \otimes \mathbb{1} \right) (\bar{\varphi} \otimes \mathbb{1}) \right] \\ &= \text{Tr}_A \left[\rho_{AB} \left(\rho_A^{-1/2} U^\dagger \bar{\varphi} U \rho_A^{-1/2} \otimes \mathbb{1} \right) \right], \end{aligned} \tag{A1}$$

which is eq. (3) needed in the proof of Theorem 1. \square

Different U correspond to choosing different initial reference states Ψ with the same Schmidt spectrum, with respect to which to formulate the Choi-Jamiołkowski isomorphism. Since in our random selection argument we don't mention Ψ to begin with, we are free to put the unitary to $U = \mathbb{1}$.

-
- [1] P. W. Shor, “Additivity of the classical capacity of entanglement-breaking quantum channels”, *J. Math. Phys.* **43**:4334-4340 (2002); arXiv:quant-ph/0201149.
- [2] C. King, “Maximization of capacity and p-norms for some product channels”, arXiv:quant-ph/0103086 (2001).
- [3] C. King, “Additivity for unital qubit channels”, *J. Math. Phys.* **43**:4641-4653 (2002); arXiv:quant-ph/0103156.
- [4] C. King, “The capacity of the quantum depolarizing channel”, *IEEE Trans. Inf. Theory* **49**:221-229 (2003); arXiv:quant-ph/0204172.
- [5] C. King, announced at the 1st joint AMS-PTM meeting, Warsaw 31 July – 3 Aug 2007.
- [6] A. S. Holevo, R. F. Werner, “Counterexample to an additivity conjecture for output purity of quantum channels”, *J. Math. Phys.* **43**:4353-4357 (2002); arXiv:quant-ph/0203003.
- [7] A. Winter, “The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$ ”, arXiv:0707.0402[quant-ph] (2007).
- [8] P. Hayden, “The maximal p-norm multiplicativity conjecture is false”, arXiv:0707.3291[quant-ph] (2007).
- [9] T. Cubitt, A. Montanaro, A. Winter, “On the dimension of subspaces with bounded Schmidt rank”, to appear in *J. Math. Phys.*; arXiv:0706.0705[quant-ph] (2007).
- [10] D. Eisenbud “Linear Sections of Determinantal Varieties”, *Amer. J. Math.* **110**(3):541-575 (1988).
- [11] B. Ilic, J. M. Landsberg, “On symmetric degeneracy loci, spaces of symmetric matrices of constant rank and dual varieties”, *Math. Ann.* **314**:1591-174 (1999).
- [12] J. Walgate, A. J. Scott, “Generic local distinguishability and completely entangled subspaces”, arXiv:0709.4238[quant-ph] (2007).
- [13] P. Hayden, D. Leung, A. Winter, “Aspects of generic entanglement”, *Comm. Math. Phys.* **265**:95-117 (2006); arXiv:quant-ph/0407049.
- [14] R. Alicki, M. Fannes, “Note on Multiple Additivity of Minimal Rényi Entropy Output of the Werner-Holevo Channels”, *Open Systems Inf. Dyn.* **11**(4):339-342 (2004); arXiv:quant-ph/0407033.
- [15] R. Y. Duan, Y. Shi, “Entanglement between Two Uses of a Noisy Multipartite Quantum Channel Enables Perfect Transmission of Classical Information”, arXiv:0712.3700[quant-ph] (2007).