Constructive counterexamples to the additivity of minimum output Rényi entropy of quantum channels for all $p > 1$

Harm Derksen*† and Benjamin Lovitz*‡

†Northeastern University, Boston, USA
‡Concordia University, Montreal, Canada

October 10, 2025

Abstract

We present explicit quantum channels with strictly sub-additive minimum output Rényi entropy for all $p > 1$, improving upon prior constructions which handled $p > 2$. Our example is provided by explicit constructions of linear subspaces with high geometric measure of entanglement. This construction applies in both the bipartite and multipartite settings. As further applications, we use our construction to find entanglement witnesses with many highly negative eigenvalues, and to construct entangled mixed states that remain entangled after perturbation.

1 Introduction

Often, it is easier to prove that a randomly chosen object satisfies a given property than to exhibit a single, explicit object that satisfies that property. This is often referred to as the *hay-in-a-haystack problem*, and has appeared in fields as diverse as number theory [Khi97], algebraic geometry [LM19], circuit complexity [FGHK16], and coding theory [TS17]. In this paper, we address a hay-in-a-haystack problem for a question regarding additivity of quantum channel capacities.

As observed by Hayden and Winter for $p > 1$ [HW08], and by Hastings for $p = 1$ [Has09] there exist randomized constructions of quantum channels Φ and Ψ for which the minimum output Rényi p-entropy is strictly sub-additive, i.e.

$$H_{\min,p}(\Phi \otimes \Psi) < H_{\min,p}(\Phi) + H_{\min,p}(\Psi).$$

Derandomizing Hastings' construction is a major open problem, in part due to its equivalence to several other channel capacity problems such as superadditivity of the Holevo capacity [Sho04]. Despite considerable efforts across more than 15 years since these randomized constructions came to light, all of the known explicit constructions only handle $p > 2$ [GHP10, BC18, SS24] or p close to (or equal to) zero [CHL+08]. In this work, we give explicit constructions of quantum channels

*emails: ha.derksen@northeastern.edu, benjamin.lovitz@concordia.ca

with strictly subadditive minimum output Rényi entropy for all $p > 1$. Moreover, our construction takes $\Phi = \Psi$.

By associating a quantum channel $\Phi : \mathrm{End}(\mathcal{H}_{\mathrm{in}}) \to \mathrm{End}(\mathcal{H}_A)$ with the image $\mathcal{U}$ of the isometry $U : \mathcal{H}_{\mathrm{in}} \to \mathcal{H}_A \otimes \mathcal{H}_B$ appearing in its Stinespring representation, it is equivalent to exhibit linear subspaces $\mathcal{U} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{V} \subseteq \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ for which

$$H_{\min,p}(\mathcal{U} \otimes \mathcal{V}) < H_{\min,p}(\mathcal{U}) + H_{\min,p}(\mathcal{V}).$$

See e.g. [Hay07, GHP10]. Here, $H_{\min,p}(\mathcal{U})$ denotes the minimum Rényi p-entropy of the squared Schmidt coefficients of any unit vector in $\mathcal{U}$, and we view $\mathcal{U} \otimes \mathcal{V}$ as a subspace of the bipartite space $(\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'})$. We let $H_{\min}(\mathcal{U}) := H_{\min,1}(\mathcal{U})$. Our main result is the following:

Theorem 1.1. *For any $p > 1$, there is an explicit subspace $\mathcal{U} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ for which $H_{\min,p}(\mathcal{U} \otimes \mathcal{U}) < 2H_{\min,p}(\mathcal{U})$, where n can be taken as $n = 2^{\Theta((p-1)^{-2})}$ as $p \to 1^+$, and (for example) $n = 3 \cdot 10^9$ for $p \geq 2$.*

We give an explicit choice of n in Theorem 3.3. For example, when $p = 2$ we show that $n = 71$ suffices. In this case, $\dim(\mathcal{U}) = 3676$. Translating to quantum channels, this construction yields an explicit quantum channel $\Phi : \mathrm{End}(\mathbb{C}^{3676}) \to \mathrm{End}(\mathbb{C}^{71})$ such that $H_{\min,2}(\Phi^{\otimes 2}) < 2H_{\min,2}(\Phi)$.

To prove this result, we employ a commonly used reduction to the problem of exhibiting subspaces with high geometric measure of entanglement [Hay07, GHP10, BC18]. For a subspace $\mathcal{U} \subseteq \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_m}$, we let

$$E(\mathcal{U}) := \min_{|\phi_i\rangle \in \mathbb{C}^{n_i}} 1 - \langle \phi_1 \otimes \cdots \otimes \phi_m | \Pi_{\mathcal{U}} | \phi_1 \otimes \cdots \otimes \phi_m \rangle$$

be the *geometric measure of entanglement* of $\mathcal{U}$. Here and throughout, $\Pi_{\mathcal{U}}$ denotes the (orthogonal) projection to $\mathcal{U}$, $|\psi\rangle$ denotes a unit vector, and ψ denotes a (not necessarily normalized) vector. We construct subspaces of high geometric measure of entanglement in both the bipartite and multipartite settings (although the bipartite setting is all that is needed for the subadditivity problem). We say a subspace $\mathcal{U}$ is *entangled* if it contains no product states, i.e. $E(\mathcal{U}) > 0$.

Several *randomized* constructions of subspaces with high min-entropy [HLW06, Has09, BH10, FK10, ASW11, BCN12, ASY14] or high geometric measure of entanglement [Har13b, BESV24] have appeared in the literature. However, these random techniques provide little information on how to find explicit constructions. To quote [BC18]: "...there is a need for a systematic development of non-random examples of highly entangled subspaces."

Focusing for simplicity on the case $n := n_1 = \cdots = n_m$, we obtain the following. It is well-known that the maximum dimension of an entangled subspace is $n^m - m(n-1) - 1$ [Par04, Har13a].

Theorem 1.2. *Let $\mathcal{H} = (\mathbb{C}^n)^{\otimes m}$.*

1. *There is an explicit entangled subspace $\mathcal{U} \subseteq \mathcal{H}$ of maximal dimension $n^m - m(n-1) - 1$ for which $E(\mathcal{U}) \geq m^{-(n-1)m}$.*

2. *For any $0 < \varepsilon < 1$, there is an explicit subspace $\mathcal{U} \subseteq \mathcal{H}$ for which $\dim(\mathcal{U}) = (1 - o(1))(1 - \varepsilon)n^m$ and $E(\mathcal{U}) \geq \varepsilon m^{-m}$. In the special case when $\varepsilon = \binom{md}{d,\ldots,d}^{-1}$ for some positive integer d, this bound can be strengthened to $E(\mathcal{U}) \geq \varepsilon$.*

Here and throughout, $o(1)$ denotes a function that approaches zero in the limit $n \to \infty$ when all other parameters are fixed. Part 1 of this theorem addresses Question 1 in [HLW06]. Part 2 of this theorem implies Theorem 1.1, using the well-known bounds $H_{\min,p}(\mathcal{U}) \geq \frac{1}{1-p} \log(E(\mathcal{U})^p +$

$(1-E(\mathcal{U}))^p)$ and $H_{\min,p}(\mathcal{U}\otimes\overline{\mathcal{U}}) \le \frac{p}{1-p}\log\left[\frac{\dim(\mathcal{U})}{n^2}\right]$, along with a careful analysis of the $o(1)$ term appearing in the dimension of $\mathcal{U}$ (for our construction, $\mathcal{U}=\overline{\mathcal{U}}$). See Section 3.

Entangled subspaces are also useful for certifying entanglement of mixed quantum states via the range criterion [Hor97, BDM⁺99] and constructing entanglement witnesses [ATL11, CS14]. In Section 4 we illustrate these applications of our construction. In particular, we construct entangled mixed states that remain entangled after perturbation, and we construct entanglement witnesses with many, highly negative eigenvalues.

1.1 Construction overview

We now give a high-level overview of our construction. For simplicity, we focus on the bipartite setting $m=2$ with $n_1=n_2=n$. For a collection of non-zero scalars $C=(C_{i,j})_{i,j=1}^n$, let

$$\mathcal{U}_C := \{\psi\in\mathbb{C}^n\otimes\mathbb{C}^n : \sum_{i+j=k} C_{i,j}\psi_{i,j}=0 \quad \text{for all} \quad k=2,3,\ldots,2n\}.$$

First observe that $\mathcal{U}_C$ is an entangled subspace: Suppose toward contradiction that $|\phi\rangle := |\phi_1\rangle\otimes|\phi_2\rangle$ is a product unit vector in $\mathcal{U}_C$. Let $\alpha_1,\alpha_2\in[n]$ be the smallest indices for which $\phi_{1,\alpha_1}\neq 0$ and $\phi_{2,\alpha_2}\neq 0$, respectively, and let $k=\alpha_1+\alpha_2$. Then $\sum_{i+j=k} C_{i,j}\phi_{i,j} = C_{\alpha_1,\alpha_2}\phi_{1,\alpha_1}\phi_{2,\alpha_2}\neq 0$, a contradiction.

Note also that $\dim(\mathcal{U}_C)=(n-1)^2$, which is the maximum dimension of an entangled subspace [Par04] (see also [Har13a, Definition 11.2]). One can verify that the antisymmetric subspace used in [GHP10] as well as the constructions of entangled subspaces used in [CMW08] are examples of subspaces of the form $\mathcal{U}_C$.

One of the main insights in the present work is to exhibit a particular choice of C for which $E(\mathcal{U}_C)$ is bounded away from zero. For example, we prove that the subspace

$$\mathcal{U} := \left\{\psi : \sum_{\substack{i,j\in[n]\\ i+j=k}} \binom{n-1}{i-1}^{1/2}\binom{n-1}{j-1}^{1/2}\psi_{i,j}=0 \quad \text{for all} \quad k=2,\ldots,2n\right\} \subseteq (\mathbb{C}^n)^{\otimes 2} \tag{1}$$

satisfies $E(\mathcal{U})\ge 2^{-2n+2}$. Surprisingly, this outperforms a randomized construction of [Har13b], which achieves $E(\mathcal{U}) > n^{-2n-2}$.

Our choice of coefficients is tailored so that we can invoke a result of [BBEM90] on symmetric projections. The *symmetric subspace* $S^d(\mathbb{C}^a)\subseteq(\mathbb{C}^a)^{\otimes d}$ is the subspace of tensors invariant under all permutations of the d subsystems. It is a standard fact that the projection onto $S^d(\mathbb{C}^a)$ is given by $\Pi_{a,d} := \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d} U_\sigma$, where U_σ is the unitary that permutes subsystems according to the permutation σ, i.e. $U_\sigma|i_1\cdots i_d\rangle = |i_{\sigma^{-1}(1)}\cdots i_{\sigma^{-1}(d)}\rangle$.

Theorem 1.3 ([BBEM90]). *For any unit vectors $|\psi\rangle\in S^d(\mathbb{C}^a)$, $|\phi\rangle\in S^d(\mathbb{C}^a)$, it holds that*

$$\|\Pi_{a,2d}(|\psi\rangle\otimes|\phi\rangle)\| \ge \binom{2d}{d}^{-1/2}. \tag{2}$$

We let $a=2$ and $d=n-1$ so that $\mathcal{H}_n := S^{n-1}(\mathbb{C}^2)$ is n-dimensional. As an immediate consequence of this theorem, $\mathcal{U} := \ker(\Pi_{a,2d})$ is an entangled subspace of the bipartite space $\mathcal{H}_n\otimes\mathcal{H}_n$, and $E(\mathcal{U}) \ge \binom{2n-2}{n-1}^{-1} \ge 2^{-2n+2}$. It turns out that $\mathcal{U}$ is precisely the subspace defined in (1) when the standard basis of $\mathbb{C}^n$ is identified with a standard (monomial) orthonormal basis of $\mathcal{H}_n$.

We generalize this construction in several directions. First, we generalize to the case of potentially unequal subsystem dimensions as well as to the multipartite setting. We also generalize this construction to produce entangled subspaces for which $E(\mathcal{U})$ is higher, at the expense of $\dim(\mathcal{U})$ being smaller. To do this, we choose d smaller (and a larger) so that $S^d(\mathbb{C}^a)$ is still (at least) n-dimensional. This makes the lower bound in (2) higher, at the expense of $\mathcal{U} = \ker(\Pi_{a,2d})$ having lower dimension. In coordinates, the resulting subspaces are no longer of the form $\mathcal{U}_C$, but they can still be described explicitly (see Section 2).

1.2 Related work

In this section we compare our work to previous constructions of highly entangled subspaces. We consider explicit and randomized constructions separately.

1.2.1 Explicit constructions

Many constructions of highly entangled subspaces have been presented in the literature. An entangled subspace of maximum dimension was presented by Bhat [Bha06]. Later, maximum-dimensional subspaces avoiding the set of states of low Schmidt rank were presented in [CMW08]. The antisymmetric subspace is an entangled subspace, which was used in [GHP10] to construct quantum channels exhibiting subadditivity for $p > 2$. Further examples were recently presented in [SS24].

Explicit constructions of highly entangled subspaces were also presented in [BC18] in the bipartite setting using the representation theory of free orthogonal quantum groups. Various properties of an associated class of quantum channels are analyzed in [BCLY20], along with a more general class of channels they call *Temperley-Lieb* channels. In more details, the subspace they construct is an irreducible subrepresentation of the tensor product of two representations of free orthogonal quantum groups. A similar idea is also used to construct entangled subspaces in [AN13, AN14] using representations of SU(2), although they only prove bounds on the entropy in very special cases, such as when one of the spaces has dimension 2 (see [AN13, Section 2.4] and [BC18, Remark 6]).

We now compare in detail our construction to the one presented in [BC18]. For simplicity, we focus on the case $n_1 = n_2 = n$. In effect, the authors of [BC18] endeavour to construct a subspace $\mathcal{U}$ of dimension ℓ for which the quantity

$$\mu(\mathcal{U}) := \frac{H_{\min}(\mathcal{U})}{\log(n^2/\ell)}$$

is as large as possible (see [BC18, Equation 1]). The authors construct a subspace for which $E(\mathcal{U}) \geq 1 - (\frac{\ell}{n^2})^{1/2} - o(1)$. From here, it follows that

$$\begin{aligned} H_{\min}(\mathcal{U}) &\geq -\log(1 - E(\mathcal{U})) \\ &\geq \frac{1}{2}\log(\frac{n^2}{\ell}) - o(1), \end{aligned}$$

which implies the bound $\mu(\mathcal{U}) \geq \frac{1}{2} - o(1)$. By comparison, our construction applies to both the bipartite and multipartite settings, and in the bipartite setting we produce subspaces with $\mu(\mathcal{U})$ arbitrarily close to 1. Indeed, when $\varepsilon = \binom{2d}{d}^{-1}$ our construction achieves $H_{\min}(\mathcal{U}) \geq -\log(1-\varepsilon)$ with $\ell/n^2 = (1 - o(1))(1 - \varepsilon)$, so by increasing d, $\mu(\mathcal{U})$ can be brought arbitrarily close to 1.

1.2.2 Randomized constructions

Randomized constructions of subspaces of high geometric measure of entanglement are given in [Har13b]. As before, for simplicity we focus on the case $m = 2$, $n_1 = n_2 = n$. The more general setting can be analyzed similarly. In particular, the following randomized construction is given in [Har13b]:

Proposition 1.4 (Proposition 11 in [Har13b])**.** *Let $\mathcal{U} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ be a Haar-random subspace of dimension $\ell = n^2 - 2(n-1) - x$ for some positive integer x. Then*

$$\Pr(E(\mathcal{U}) \leq n^{-2n/x-2}) \leq n^{-n}.$$

We now compare the bound on $E(\mathcal{U})$ obtained by this randomized construction to the one obtained by our explicit construction. We consider two examples $\ell = (n-1)^2$ (the largest possible) and $\ell = (1-o(1))(1-\varepsilon)n^2$. We find that our explicit construction outperforms the randomized construction in both cases:

- When $\ell = (n-1)^2$, the randomized construction obtains $E(\mathcal{U}) > n^{-2n-2}$. By comparison, our explicit construction obtains the better bound $E(\mathcal{U}) \geq 2^{-2n+2}$.
- When $\ell = (1-o(1))(1-\varepsilon)n^2$, the randomized construction obtains $E(\mathcal{U}) > n^{\frac{-2n}{\varepsilon n^2 - 2n + 2 + o(1)(1-\varepsilon)n^2} - 2}$. Note that this bound is less than n^{-2} for $n \gg 0$. By comparison, our explicit construction obtains a constant bound $E(\mathcal{U}) \geq \varepsilon/4$ (or $E(\mathcal{U}) \geq \varepsilon$ when $\varepsilon = \binom{2d}{d}^{-1}$ for some d). We note that the construction of [BC18] also achieves a constant bound of $E(\mathcal{U}) \geq 1 - \sqrt{1-\varepsilon}$.

Randomized constructions of highly entangled subspaces are also presented in [BESV24] over the real numbers. In particular, they construct a subspace of dimension $\dim(\mathcal{U}) = cn^2$ for a fixed constant c, with $E(\mathcal{U})$ depending inverse-polynomially in n. See [BESV24, Theorem 7.1] for a more general statement, which holds for other types of entanglement as well as in the smoothed analysis setting.

Relatedly, there have been several randomized constructions of subspaces with high min-entropy $H_{\min}(\mathcal{U})$ [HLW06, Has09, BH10, FK10, ASW11, BCN12, ASY14]. Notably, such a random construction was used by Hastings to show that the minimum output entropy of quantum channels can be strictly subadditive under the tensor product [Has09].

It is a major open problem to derandomize Hasting's counterexample. See [NS22] for partial progress using unitary designs. Using the bound $H_{\min}(\mathcal{U}) \geq -\log(1 - E(\mathcal{U}))$, it would suffice to find a subspace $\mathcal{U} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of dimension ℓ for which

$$2\left(1 - \ell/n^2\right)\log(n) + h\left(\ell/n^2\right) < -2\log(1 - E(\mathcal{U})),$$

where $h(x) := -x\log x - (1-x)\log(1-x)$ is the binary entropy [GHP10]. It is an interesting question for future work whether some variant of our construction can achieve this.

2 The construction

In this section we explicitly construct subspaces of $\mathcal{H} = \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_m}$ with high geometric measure of entanglement. Let $S = [n_1] \times \cdots \times [n_m]$. For a tuple of coefficients $C = (C_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in S}$, let

$$\mathcal{U}_C := \left\{ \psi \in \mathcal{H} : \sum_{\substack{\boldsymbol{\alpha} \in S \\ |\boldsymbol{\alpha}| = k}} C_{\boldsymbol{\alpha}}\, \psi_{\boldsymbol{\alpha}} = 0 \quad \text{for all} \quad k \right\},$$

where $|\boldsymbol{\alpha}| := \alpha_1 + \cdots + \alpha_m$, and k ranges over $\{m, m+1, \ldots, n_1 + \cdots + n_m\}$.

Proposition 2.1. *If $C_{\boldsymbol{\alpha}} \neq 0$ for all $\boldsymbol{\alpha} \in S$, then $\mathcal{U}_C$ is a completely entangled subspace (i.e. it contains no product states) of maximum dimension.*

Proof. Let $|\phi\rangle = |\phi_1 \otimes \cdots \otimes \phi_m\rangle$ be a product state. For each $i \in [m]$ let α_i be the smallest index for which $\phi_{i,\alpha_i} \neq 0$, and let $k = \sum_i \alpha_i$. Then

$$\sum_{\substack{\boldsymbol{\alpha} \in S \\ |\boldsymbol{\alpha}|=k}} C_{\boldsymbol{\alpha}}\, \phi_{\boldsymbol{\alpha}} = C_{\boldsymbol{\alpha}} \phi_{1,\alpha_1} \cdots \phi_{m,\alpha_m} \neq 0,$$

so $\phi \notin \mathcal{U}_C$. This shows that $\mathcal{U}_C$ is completely entangled. Furthermore, $\dim(\mathcal{U}_C) = n_1 \cdots n_m - \sum_{i=1}^m (n_i) + m - 1$, which is the maximum dimension of a completely entangled subspace by [Par04] (see also [Har13a, Definition 11.2]). □

More generally, let $P = (P_1, \ldots, P_\ell)$ be any ordered partition of S that respects the ordering of each $[n_i]$ in the sense that if $\boldsymbol{\alpha} \in P_q$ and $\gamma_i < \alpha_i$ then $(\alpha_1, \ldots, \alpha_{i-1}, \gamma_i, \alpha_{i+1}, \ldots, \alpha_m) \in P_r$ for some $r < q$. Let $\mathcal{U}_{C,P}$ be the set of ψ for which $\sum_{\boldsymbol{\alpha} \in P_i} C_{\boldsymbol{\alpha}} \psi_{\boldsymbol{\alpha}} = 0$ for all i. Then $\mathcal{U}_{C,P}$ is completely entangled (but may not be of maximum dimension).

Our main result is to exhibit choices of C and P for which $E(\mathcal{U}_{C,P})$ is high. For convenience, we summarize our main results in the case $n_1 = \cdots = n_m = n$:

Theorem 2.2. *Let $\mathcal{H} = (\mathbb{C}^n)^{\otimes m}$.*

1. *There is an explicit choice of $C \in \mathbb{C}^S$ for which $E(\mathcal{U}_C) \geq m^{-(n-1)m}$ (and by construction, $\dim(\mathcal{U}_C)$ is maximal among all completely entangled subspaces).*
2. *For any $0 < \varepsilon < 1$, there is an explicit choice of C and P for which $\dim(\mathcal{U}_{C,P}) = (1 - o(1))(1 - \varepsilon)n^m$ and $E(\mathcal{U}_{C,P}) \geq \varepsilon m^{-m}$. In the special case when $\varepsilon = \binom{md}{d,\ldots,d}^{-1}$ for some positive integer d, this bound can be strengthened to $E(\mathcal{U}_{C,P}) \geq \varepsilon$.*

2.1 Choosing C and P for the construction

We now explain how we choose C and P so that $U_{C,P}$ has high geometric measure of entanglement. We first choose positive integers a, d_i with $n_i \leq \binom{a+d_i-1}{d_i}$, and view $\mathbb{C}^{n_i}$ as a subspace of $S^{d_i}(\mathbb{C}^a)$ by sending the standard basis of $\mathbb{C}^{n_i}$ to the the first n_i elements of the orthonormal basis

$$\left\{ |\boldsymbol{\alpha}_i\rangle := \binom{d_i}{\boldsymbol{\alpha}_i}^{1/2} \Pi_{S^{d_i}(\mathbb{C}^a)}(|1\rangle^{\otimes \alpha_{i,1}} \otimes \cdots \otimes |a\rangle^{\otimes \alpha_{i,a}}) : \boldsymbol{\alpha}_i \in \{0, 1, \ldots, d_i\}^a, |\boldsymbol{\alpha}_i| = d_i \right\}$$

for $S^{d_i}(\mathbb{C}^a)$, where $\Pi_{S^{d_i}(\mathbb{C}^a)}$ is the orthogonal projection onto $S^{d_i}(\mathbb{C}^a)$. (Alternatively, any isometric embedding $\mathbb{C}^{n_i} \hookrightarrow S^{d_i}(\mathbb{C}^a)$ will do.) Let $\mathbf{d} := (d_1, \ldots, d_m)$, and let $\mathcal{J}_{a,\mathbf{d}} := S^{d_1}(\mathbb{C}^a) \otimes \cdots \otimes S^{d_m}(\mathbb{C}^a)$.

After making the choice, we let $\Pi_{a,\mathbf{d}}$ be the orthogonal projection onto the symmetric subspace $S^{d_1+\cdots+d_m}(\mathbb{C}^a) \subseteq \mathcal{J}_{a,\mathbf{d}}$, and define

$$\mathcal{U}_{a,\mathbf{d}} := \ker(\Pi_{a,\mathbf{d}}) \subseteq \mathcal{J}_{a,\mathbf{d}}.$$

Then $\mathcal{U}_{a,\mathbf{d}}$ is a completely entangled subspace of $\mathcal{H}$ (after intersecting with $\mathcal{H}$ if the inequality $n_i \leq \binom{a+d_i-1}{d_i}$ is strict for some i). This can be verified from the following remark, or from Corollary 2.7 below.

Remark 2.3 (Writing $\mathcal{U}_{a,\mathbf{d}}$ in coordinates)**.** In coordinates, we can write $\mathcal{U}_{a,\mathbf{d}}$ as a subspace of the form $\mathcal{U}_{C,P}$ as follows. For each $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m) \in \mathbb{Z}_{\geq 0}^{a \times m}$ with $(1, \dots, 1)\boldsymbol{\alpha} = \mathbf{d}$ we let

$$C_{\boldsymbol{\alpha}} := \binom{d_1}{\boldsymbol{\alpha}_1}^{1/2} \cdots \binom{d_m}{\boldsymbol{\alpha}_m}^{1/2}.$$

Then

$$\mathcal{U}_{a,\mathbf{d}} = \left\{ \psi : \sum_{\substack{\boldsymbol{\alpha} \in \mathbb{Z}_{\geq 0}^{a \times m} \\ (1,\dots,1)\boldsymbol{\alpha} = \mathbf{d} \\ (1,\dots,1)\boldsymbol{\alpha}^{\mathsf{T}} = \boldsymbol{\beta}}} C_{\boldsymbol{\alpha}} \psi_{\boldsymbol{\alpha}} = 0 \quad \text{for all} \quad \boldsymbol{\beta} \right\} \subseteq \mathcal{J}_{a,\mathbf{d}}, \tag{3}$$

where $\boldsymbol{\beta} = (\beta_1, \dots, \beta_a)$ ranges over $\{\boldsymbol{\beta} \in \mathbb{Z}_{\geq 0}^a : |\boldsymbol{\beta}| = |\mathbf{d}|\}$. One can verify that the expressions (3) and $\mathcal{U}_{a,\mathbf{d}} = \ker(\Pi_{a,\mathbf{d}})$ are equivalent by noting that $|\psi\rangle \in \ker(\Pi_{a,\mathbf{d}})$ if and only if

$$(\langle 1|^{\otimes \beta_1} \otimes \cdots \otimes \langle a|^{\otimes \beta_a})\Pi_{a,\mathbf{d}}|\psi\rangle = 0$$

for all $\boldsymbol{\beta}$, and

$$(\langle 1|^{\otimes \beta_1} \otimes \cdots \otimes \langle a|^{\otimes \beta_a})\Pi_{a,\mathbf{d}} = \binom{|\mathbf{d}|}{\boldsymbol{\beta}}^{-1} \sum_{\substack{\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m) \in \mathbb{Z}_{\geq 0}^{a \times m} \\ (1,\dots,1)\boldsymbol{\alpha} = \mathbf{d} \\ (1,\dots,1)\boldsymbol{\alpha}^{\mathsf{T}} = \boldsymbol{\beta}}} C_{\boldsymbol{\alpha}} (\langle \boldsymbol{\alpha}_1| \otimes \cdots \otimes \langle \boldsymbol{\alpha}_m|),$$

which is a tedious but elementary computation.

If $d_1 = \cdots = d_m =: d$ we let $\mathcal{J}_{a,d} = \mathcal{J}_{a,\mathbf{d}}$ and $\mathcal{U}_{a,d} = \mathcal{U}_{a,\mathbf{d}}$. Let us now restate Theorem 2.2 in more details.

Theorem 2.4. *Let $\mathcal{H} = (\mathbb{C}^n)^{\otimes m}$, and for a, d with $n \leq \binom{a+d-1}{d}$ let $\mathcal{U}_{a,d} \subseteq \mathcal{J}_{a,d}$ be defined as above.*

1. *If $a = 2, d = n - 1$, then $\mathcal{U}_{a,d} \subseteq \mathcal{H}$ is completely entangled of maximum dimension, and $E(\mathcal{U}) \geq m^{-(n-1)m}$.*
2. *For any $0 < \varepsilon < 1$, there is a choice of $d = d(\varepsilon)$ (given by (4)) for which letting $a = \lceil \sqrt[d]{d! \cdot n} \rceil$ gives $\dim(\mathcal{U}_{a,d}) = (1 - o(1))(1 - \varepsilon)n^m$ and $E(\mathcal{U}_{a,d}) \geq \varepsilon m^{-m}$. In the special case when $\varepsilon = \binom{md'}{d', \dots, d'}^{-1}$ for some positive integer d', one can choose $d = d'$ and this bound can be strengthened to $E(\mathcal{U}_{a,d}) \geq \varepsilon$.*

Example 2.5 (Bipartite setting)**.** In the bipartite setting,

$$\mathcal{U}_{2,n-1} = \left\{ \psi : \sum_{\substack{i,j \in [n] \\ i+j=k}} \binom{n-1}{i-1}^{1/2} \binom{n-1}{j-1}^{1/2} \psi_{i,j} = 0 \quad \text{for all} \quad k = 2, \dots, 2n \right\} \subseteq (\mathbb{C}^n)^{\otimes 2}.$$

By Theorem 2.4, $\mathcal{U}_{2,n-1}$ is completely entangled of maximum dimension, and $E(\mathcal{U}) \geq 2^{-2n+2}$.

2.2 Analyzing the geometric measure of entanglement for the construction

In this section we prove Theorem 2.4, along with more general statements that handle the case of potentially unequal subsystem dimensions. We carry over the definitions from the previous section, including $\mathcal{H} = \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_m}$.

The starting point in our analysis is the following result of [BBEM90].

Theorem 2.6. *If $\psi \in S^{d_1}(\mathbb{C}^a)$, $\phi \in S^{d_2}(\mathbb{C}^a)$ and $\mathbf{d} = (d_1, d_2)$, then*

$$\|\Pi_{a,\mathbf{d}}(\psi \otimes \phi)\| \geq \binom{d_1 + d_2}{d_1}^{-1/2} \|\psi\| \|\phi\|.$$

A one-page proof of this result can be found in [Zei94]. In these references, the result is stated as a bound on the Bombieri norm of the product of homogeneous polynomials. One can translate this to the above statement by identifying $|\boldsymbol{\alpha}_i\rangle$ with the polynomial $\binom{d}{\boldsymbol{\alpha}}^{1/2} x_1^{\alpha_1} \cdots x_a^{\alpha_a}$ and verifying that this map is a linear isometry for which $\Pi_{a,\mathbf{d}}(\psi \otimes \phi)$ corresponds to the product of ψ and ϕ as polynomials.

Corollary 2.7. *If $\psi_i \in S^{d_i}(\mathbb{C}^a)$ for $i = 1, 2, \ldots, m$, and $\mathbf{d} = (d_1, \ldots, d_m)$, then*

$$\|\Pi_{a,\mathbf{d}}(\psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_m)\| \geq \binom{d_1 + d_2 + \cdots + d_m}{d_1, d_2, \ldots, d_m}^{-1/2} \|\psi_1\| \|\psi_2\| \cdots \|\psi_m\|.$$

Proof. We have

$$\begin{aligned}
\|\Pi_{a,\mathbf{d}}(\psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_m)\| &= \|\Pi_{a,\mathbf{d}}(\psi_1 \otimes \Pi_{a,(d_2,\ldots,d_m)}(\psi_2 \otimes \cdots \otimes \psi_m))\| \\
&\geq \binom{d_1 + \cdots + d_m}{d_1}^{-1/2} \|\psi_1\| \ \ \|\Pi_{a,(d_2,\ldots,d_m)}(\psi_2 \otimes \cdots \otimes \psi_m)\| \\
&\geq \cdots \geq \binom{d_1 + d_2 + \cdots + d_m}{d_1, d_2, \ldots, d_m}^{-1/2} \|\psi_1\| \ \ \|\psi_2\| \cdots \|\psi_m\|,
\end{aligned}$$

completing the proof. □

Theorem 2.8. *Let $a, d_1, \ldots, d_m, \ell$ be positive integers. If $n_i \leq \binom{a+d_i-1}{a-1}$ and*

$$\ell \leq n_1 \cdots n_m - \dim(S^{d_1+\cdots+d_m}(\mathbb{C}^a))$$

then there exists a subspace $\mathcal{U} \subseteq \mathcal{H}$ of dimension ℓ with $E(\mathcal{U}) \geq \binom{d_1+d_2+\cdots+d_m}{d_1,d_2,\ldots,d_m}^{-1}$.

Proof. Let $\mathcal{U} = \ker(\Pi_{a,\mathbf{d}}) \cap \mathcal{H} \subseteq \mathcal{H}$ (recall that we view $\mathbb{C}^{n_i}$ as a subspace of $S^{d_i}(\mathbb{C}^a)$), which has dimension at least $n_1 \cdots n_m - \dim(S^{d_1+\cdots+d_m}(\mathbb{C}^a))$. It remains to prove that $E(\mathcal{U}) \geq \binom{d_1+d_2+\cdots+d_m}{d_1,d_2,\ldots,d_m}^{-1}$. Note that

$$\begin{aligned}
E(\mathcal{U}) &= \min_{\substack{|\psi\rangle \in \mathcal{U} \\ |\phi_i\rangle \in \mathbb{C}^{n_i}}} (1 - |\langle \psi | \phi_1 \otimes \cdots \otimes \phi_m \rangle|^2) \\
&\geq \min_{\substack{|\psi\rangle \in \ker(\Pi_{a,\mathbf{d}}) \\ |\phi_i\rangle \in S^{d_i}(\mathbb{C}^{a_i})}} (1 - |\langle \psi | \phi_1 \otimes \cdots \otimes \phi_m \rangle|^2) \\
&= \max_{|\phi_i\rangle \in S^{d_i}(\mathbb{C}^{a_i})} \|\Pi_{a,\mathbf{d}} |\phi_1 \otimes \cdots \otimes \phi_m\rangle\|^2 \\
&\geq \binom{d_1 + d_2 + \cdots + d_m}{d_1, d_2, \ldots, d_m}^{-1},
\end{aligned}$$

where the second line follows from $\mathcal{U} \subseteq \ker(\Pi_{a,\mathbf{d}})$ and $\mathbb{C}^{n_i} \subseteq S^{d_i}(\mathbb{C}^{a_i})$. This completes the proof. □

Corollary 2.9. *There exists a subspace $\mathcal{U} \subseteq \mathcal{H}$ of dimension*

$$\ell = n_1 \cdots n_m - \sum_{i=1}^{m}(n_i) + m - 1$$

with $E(\mathcal{U}) \geq \binom{n_1+n_2+\cdots+n_m-m}{n_1-1,n_2-1,\ldots,n_m-1}^{-1}$.

Note that the subspace $\mathcal{U}$ constructed in this corollary is entangled of maximum dimension.

Proof. Take $a = 2$, $d_i = n_i - 1$ for $i = 1, 2, \ldots, m$, and

$$\ell = n_1 \cdots n_m - \binom{d_1 + d_2 + \cdots + d_m + a - 1}{a - 1} = n_1 \cdots n_m - \sum_{i=1}^{m}(n_i) + m - 1$$

in Theorem 2.8. □

Let us now look at the special case where $n_1 = n_2 = \cdots = n_m = n$.

Corollary 2.10. *There exists a subspace $\mathcal{U} \subseteq (\mathbb{C}^n)^{\otimes m}$ of dimension $n^m - mn + m - 1$ with $E(\mathcal{U}) \geq m^{-(n-1)m}$.*

Proof. We take $n_1 = n_2 = \cdots = n_m = n$ in Corollary 2.9. Then $\mathcal{U}$ is a subspace of the specified dimension, and $E(\mathcal{U}) \geq \binom{m(n-1)}{n-1,n-1,\ldots,n-1}^{-1} \geq m^{-(n-1)m}$. □

We constructed entangled subspaces $\mathcal{U}$ of $(\mathbb{C}^n)^{\otimes m}$ of maximal dimension for which $E(\mathcal{U})$ has a lower bound that is exponentially small in n. For subspaces of smaller dimension we can get better bounds. For example, we can construct $\mathcal{U}$ of dimension $(1 - o(1))(1 - \varepsilon)n^m$ for which $E(\mathcal{U})$ is lower bounded by a constant independent of n.

Proposition 2.11. *For any $d \in \mathbb{N}$ there exists a subspace $\mathcal{U} \subseteq (\mathbb{C}^n)^{\otimes m}$ of dimension*

$$\ell \geq n^m - n^m \binom{md}{d, d, \ldots, d}^{-1} \left(1 + \frac{me}{\sqrt[d]{n}}\right)^{md}$$

for which $E(\mathcal{U}) \geq \binom{md}{d,d,\ldots,d}^{-1}$.

In the statement of the proposition, e is Euler's constant.

Proof. In Theorem 2.8 we will take $d_1 = d_2 = \cdots = d_m = d$ and $n_1 = n_2 = \cdots = n_m = n$. We take $a = \lceil \sqrt[d]{d! \cdot n} \rceil \leq \sqrt[d]{d! \cdot n} + 1$, so that

$$\binom{d + a - 1}{a - 1} = \binom{d + a - 1}{d} \geq \frac{a^d}{d!} \geq n.$$

Now we have

$$\binom{d_1 + d_2 + \cdots + d_m + a - 1}{a - 1} = \binom{md + a - 1}{md} \leq \frac{(md + a - 1)^{md}}{(md)!} \leq \frac{(md + \sqrt[d]{d! \cdot n})^{md}}{(md)!} =$$
$$= n^m \binom{md}{d, d, \ldots, d}^{-1} \left(1 + \frac{md}{\sqrt[d]{d! \cdot n}}\right)^{md} \leq n^m \binom{md}{d, d, \ldots, d}^{-1} \left(1 + \frac{me}{\sqrt[d]{n}}\right)^{md}.$$

This completes the proof. □

Theorem 2.12. *Let $0 < \varepsilon < 1$ be arbitrary but fixed. Then there exists a subspace $\mathcal{U} \subseteq (\mathbb{C}^n)^{\otimes m}$ of dimension $(1-o(1))(1-\varepsilon)n^m$ with $E(\mathcal{U}) \geq \varepsilon m^{-m}$. In the special case that $\varepsilon = \binom{md}{d,d,\ldots,d}^{-1}$ for some $d \in \mathbb{N}$, this bound can be strengthened to $E(\mathcal{U}) \geq \varepsilon$.*

Proof. Choose d such that

$$\binom{md}{d,d,\ldots,d}^{-1} \leq \varepsilon < \binom{m(d-1)}{(d-1),(d-1),\ldots,(d-1)}^{-1}. \tag{4}$$

Multiplying by $\binom{md}{d,d,\ldots,d}$ gives

$$1 \leq \binom{md}{d,d,\ldots,d}\varepsilon < \frac{(md)(md-1)\cdots(md-m+1)}{d^m} \leq m^m.$$

From Proposition 2.11 and (4) it follows that

$$E(\mathcal{U}) \geq \binom{md}{d,d,\ldots,d}^{-1} \geq \varepsilon m^{-m}.$$

In the special case $\binom{md}{d,d,\ldots,d}\varepsilon = 1$ this bound can be strengthened to $E(\mathcal{U}) \geq \varepsilon$, as claimed. The dimension of $\mathcal{U}$ is at least

$$\begin{aligned} n^m - n^m\binom{md}{d,d,\ldots,d}^{-1}\left(1+\frac{me}{\sqrt[d]{n}}\right)^{md} &> n^m - \varepsilon n^m\left(1+\frac{me}{\sqrt[d]{n}}\right)^{md} \\ &\geq (1-o(1))(1-\varepsilon)n^m. \end{aligned}$$

This completes the proof. ☐

The following theorem gives a general tradeoff between $\dim(\mathcal{U})$ and $E(\mathcal{U})$. Here, $\ln(\cdot)$ denotes the logarithm base e.

Theorem 2.13. *Let $0 < \alpha < m$ be arbitrary but fixed. There exists a sequence of subspaces $\mathcal{U}_n \subseteq (\mathbb{C}^n)^{\otimes m}$, $n \geq 1$ of dimension at least $n^m - n^{f_m(\alpha)}$ with $E(\mathcal{U}_n) \geq n^{-2\alpha}$, where*

$$f_m(\alpha) = m + \frac{2\alpha\ln(m^{-1}+em^{-m/2\alpha})}{\ln m}.$$

Proof. Note that

$$\lim_{d\to\infty}\frac{\ln\binom{md}{d,d,\ldots,d}}{d} = m\ln m.$$

Define $d = d(n) = \lceil \beta\ln(n)\rceil$, where $\beta = 2\alpha/(m\ln m)$. Then we have

$$\lim_{n\to\infty}\frac{\ln\binom{md(n)}{d(n),d(n),\ldots,d(n)}}{\ln n} = \lim_{n\to\infty}\frac{d(n)}{\ln n}\cdot\frac{\ln\binom{md(n)}{d(n),d(n),\ldots,d(n)}}{d(n)} \geq \beta m\ln m.$$

Let $\mathcal{U}_n$ be equal to $\mathcal{U}$ as in Proposition 2.11. Then we have

$$\liminf_{n\to\infty}\frac{\ln E(\mathcal{U}_n)}{\ln(n)} \geq \liminf_{n\to\infty}\frac{\ln\binom{md(n)}{d(n),d(n),\ldots,d(n)}^{-1}}{\ln n} = -\beta m\ln m = -2\alpha,$$

which proves that $E(\mathcal{U}_n) \geq n^{-2\alpha}$. Let $c(n) = n^m - \dim(\mathcal{U}_n)$ be the codimension of $\mathcal{U}_n$. From

$$c(n) \leq n^m \binom{md(n)}{d(n), d(n), \ldots, d(n)}^{-1} \left(1 + \frac{me}{\sqrt[d(n)]{n}}\right)^{md(n)}$$

it follows that

$$\limsup_{n\to\infty} \frac{\ln c(n)}{\ln(n)} \leq m - \beta m \ln m + \beta m \ln(1 + me^{1-1/\beta}) = m + \beta m \ln(m^{-1} + e^{1-1/\beta}) =$$

$$= m + \frac{2\alpha \ln(m^{-1} + e \cdot e^{-m\ln(m)/2\alpha})}{\ln m} = m + \frac{2\alpha \ln(m^{-1} + em^{-m/2\alpha})}{\ln m}.$$

This completes the proof. $\square$

3 Strict subadditivity of minimum output Rényi p-entropy for $p > 1$

For a unit vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and a constant $p > 1$, let

$$H_p(\psi) = \frac{1}{1-p} \log(\sum_i \lambda_i^p)$$

be the *Rényi p-entropy* of ψ, where the logarithm is taken base-2, and λ_i are the squared Schmidt coefficients of $|\psi\rangle$. For a subspace $\mathcal{U} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$, define the *min-$p$-entropy* $H_{p,\min}(\mathcal{U})$ to be the minimum Rényi p-entropy of any unit vector in $\mathcal{U}$. The following lemma is well-known, see e.g. [Hay07, Equation 26], [GHP10, Lemma 1], or [SS24, Lemmas 2 and 3].

Lemma 3.1. *If $\mathcal{U} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ is a subspace, then $\mathcal{U} \otimes \overline{\mathcal{U}} \subseteq (\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'})$ satisfies*

$$H_{\min,p}(\mathcal{U} \otimes \overline{\mathcal{U}}) \leq \frac{p}{1-p} \log\left[\frac{\dim(\mathcal{U})}{\dim(\mathcal{H}_A)\dim(\mathcal{H}_B)}\right].$$

In the statement of the lemma, we view $\mathcal{U} \otimes \overline{\mathcal{U}}$ as a subspace of bipartite space according to the bipartition $(\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'})$.

We also require the following lower bound on $H_{\min,p}(\mathcal{U})$. This bound can be proven easily using Schur-concavity of the Rényi p-entropy. See also [SS24, Lemma 4].

Lemma 3.2. *If $\mathcal{U} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ is a subspace, then*

$$H_{\min,p}(\mathcal{U}) \geq \frac{1}{1-p} \log(E(\mathcal{U})^p + (1 - E(\mathcal{U}))^p).$$

Our goal is to construct subspaces $\mathcal{U}, \mathcal{V} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ for which

$$H_{\min,p}(\mathcal{U} \otimes \mathcal{V}) < H_{\min,p}(\mathcal{U}) + H_{\min,p}(\mathcal{V}).$$

We now present such a construction for any $p > 1$ with $\mathcal{U} = \mathcal{V} = \overline{\mathcal{U}}$.

Theorem 3.3 (Theorem 1.1 in more details)**.** *Let $\mathcal{U} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ be the subspace constructed in Proposition 2.11 with $m = 2$,*

$$d = \begin{cases} \lceil \frac{4}{p-1} \rceil, & p \in (1, 2) \\ 3, & p \geq 2 \end{cases},$$

and

$$n = \begin{cases} \lceil (40\, d\, 4^d)^d \rceil, & p \in (1,2) \\ 3 \cdot 10^9, & p \geq 2 \end{cases}.$$

Then $H_{\min,p}(\mathcal{U} \otimes \mathcal{U}) < 2H_{\min,p}(\mathcal{U})$.

Note that $n = 2^{\Theta((p-1)^{-2})}$ as $p \to 1^+$.

Proof. Recall that Proposition 2.11 constructs, for any $d \in \mathbb{N}$, a subspace $\mathcal{U} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ for which $\mathcal{U} = \overline{\mathcal{U}}$ (because the projection matrix $\Pi_{a,\mathbf{d}}$ has real entries),

$$E(\mathcal{U}) \geq \varepsilon := \binom{2d}{d}^{-1},$$

and

$$\begin{aligned} \dim(\mathcal{U}) &= n^2 - \binom{2d + \left\lceil \sqrt[d]{d!n} \right\rceil - 1}{2d} \\ &\geq n^2 - \varepsilon n^2 \left(1 + \frac{2e}{\sqrt[d]{n}}\right)^{2d} \\ &\geq n^2(1 - \varepsilon e^x), \end{aligned} \tag{5}$$

where $x = \frac{4ed}{\sqrt[d]{n}}$. Note that $0 < \varepsilon \leq \frac{1}{2}$. It suffices to find n, d for which

$$H_{\min,p}(\mathcal{U} \otimes \mathcal{U}) < 2H_{\min,p}(\mathcal{U}), \tag{6}$$

or sufficiently by the lemmas above,

$$p \ln(1 - \varepsilon e^x) > 2 \ln(\varepsilon^p + (1-\varepsilon)^p). \tag{7}$$

Our choice of n and d will ensure that $e^x \leq 1 + \frac{\varepsilon}{2}$. This implies

$$\begin{aligned} p \ln(1 - \varepsilon e^x) &\geq p \ln\left((1-\varepsilon)(2 - e^x)\right) \geq p \ln\left((1-\varepsilon)(1 - \frac{\varepsilon}{2})\right) \\ &= 2p \ln(1-\varepsilon) + p \ln\left(1 + \frac{\varepsilon}{2(1-\varepsilon)}\right) > 2p\ln(1-\varepsilon) + \frac{\varepsilon p}{4(1-\varepsilon)}. \end{aligned}$$

For the first inequality, we used $(1 - \varepsilon y) \geq (1-\varepsilon)(2-y)$ for all $\varepsilon \leq 1/2$ and $y \geq 1$. For the second inequality we used $e^x \leq 1 + \frac{\varepsilon}{2}$. For the last inequality we used $\ln(1+u) > \frac{u}{2}$ for $0 < u < 1$. Note also that

$$2\ln(\varepsilon^p + (1-\varepsilon)^p) = 2[p\ln(1-\varepsilon) + \ln(1+t)] < 2p\ln(1-\varepsilon) + 2t,$$

where $t := \left(\frac{\varepsilon}{1-\varepsilon}\right)^p$. Here, we used the inequality $\ln(1+u) < u$ for $0 < u < 1$. Putting these bounds together, it suffices to prove that our choice of n and d satisfy

$$\frac{\varepsilon p}{4(1-\varepsilon)} > 2\left(\frac{\varepsilon}{1-\varepsilon}\right)^p.$$

Equivalently, $\varepsilon^{p-1} < \left(\frac{p}{8}\right)(1-\varepsilon)^{p-1}$. Since $1-\varepsilon \geq 1/2$, it suffices that

$$\varepsilon^{p-1} < \frac{p}{2^{p+2}}. \tag{8}$$

At this point, we have proven that (6) holds as long as (8) holds and $e^x \leq 1 + \frac{\varepsilon}{2}$.

We first verify that (8) holds under our choice of d. Note that

$$\varepsilon = \binom{2d}{d}^{-1} \leq \frac{2d+1}{4^d} < \frac{3d}{4^d}.$$

First consider the case $p \in (1,2)$. Then $4 \leq d(p-1) \leq 5$ and

$$\varepsilon^{p-1} < \frac{(3d)^{p-1}}{4^{d(p-1)}} \leq \frac{15}{4^4},$$

where for the second inequality we have used $(3d)^{p-1} \leq (15/(p-1))^{p-1} \leq 15$. On the other hand, $\min_{p\in(1,2]} \frac{p}{2^{p+2}} = \frac{1}{8} > \frac{15}{4^4}$. For $p \geq 2$, note that (8) is equivalent to $R := \frac{(2\varepsilon)^{p-1}}{p/8} < 1$. Since $\frac{\partial(\ln R)}{\partial p} = \ln(2\varepsilon) - \frac{1}{p}$ is negative for all $\varepsilon \leq 1/2$, R is decreasing on $[2,\infty)$, so it suffices to prove the inequality for the case $p = 2$. In this case, $R = \frac{2}{5} < 1$, which verifies (8) for our given choice of d.

Now we verify that our choice of n satisfies $e^x \leq 1 + \frac{\varepsilon}{2}$. First note that $e^x \leq 1 + (e-1)x$ as long as $x < 1$, so it suffices to verify $x \leq \frac{\varepsilon}{2(e-1)}$. Recalling the definition of x, we can take

$$\sqrt[d]{n} \geq \frac{8e(e-1)d}{\varepsilon}.$$

Using the lower bound $\varepsilon < 4^{-d}$, it suffices to set

$$n = \lceil (40\, d\, 4^d)^d \rceil.$$

Note that $n = 2^{\Theta((p-1)^{-2})}$ as $p \to 1^+$. When $p \geq 2$, one can easily verify that $e^x \leq 1 + \frac{\varepsilon}{2}$ under the choice $n = 3 \cdot 10^9$. This completes the proof. $\square$

Remark 3.4. The above bounds on d and n are not optimized. For example, when $p = 2$ one can directly analyze (7) and obtain that $d = 2$, $n = 1813$ suffices. This can be further optimized to $d = 2$, $n = 71$ by using the exact expression for $\dim(\mathcal{U})$ given in the first line of (5). We record a loosely optimized table of sufficient values for d and n, along with $\dim(\mathcal{U})$, for a few values of p:

p	n	d	$\dim(\mathcal{U})$
2	71	2	3676
1.5	200	2	31145
1.25	70289	3	$\approx 4.6 \cdot 10^9$
1.125	10^{12}	5	$\approx 9.96 \cdot 10^{24}$
1.0625	10^{28}	9	$\approx 9.99978785 \cdot 10^{55}$

4 Further applications

In this section we discuss further applications of our construction to produce entangled mixed states that remain entangled after perturbation, and entanglement witnesses with many, highly negative eigenvalues.

In the following, $\|\cdot\|_1$ denotes the trace norm and $\|\cdot\|_\infty$ denotes the spectral norm.

Theorem 4.1 (Robustly entangled mixed states)**.** *Let $\mathcal{H} = (\mathbb{C}^n)^{\otimes m}$.*

1. *There is an explicit mixed state ρ on $\mathcal{H}$ of rank $n^m - m(n-1) - 1$ such that for every Hermitian operator H with trace norm $\|H\|_1 \leq m^{-(n-1)m/2}$, the state $e^{iH}\rho e^{-iH}$ is entangled.*

2. *For any $0 < \varepsilon < 1$, there is an explicit mixed state ρ on $\mathcal{H}$ of rank $(1 - o(1))(1 - \varepsilon)n^m$ such that $e^{iH}\rho e^{-iH}$ is entangled for every Hermitian operator H with trace norm $\|H\|_1 \leq \sqrt{\varepsilon m^{-m}}$. In the particular case when $\varepsilon = \binom{md}{d,\ldots,d}^{-1}$ for some positive integer d, this condition can be weakened to $\|H\|_1 \leq \sqrt{\varepsilon}$.*

Proof. This follows from [ZZZ24, Theorem 2] by taking ρ to be a state supported on one of the subspaces specified by Theorem 1.2. □

Theorem 4.2 (Entanglement witnesses with many, highly negative eigenvalues)**.** *Let $\mathcal{H} = (\mathbb{C}^n)^{\otimes m}$.*

1. *There is an explicit entanglement witness H with $\|H\|_\infty = 1$ having $n^m - m(n-1) - 1$ negative eigenvalues, each of magnitude at least $m^{-(n-1)m}$.*

2. *For any $0 < \varepsilon < 1$ there is an explicit entanglement witness H with $\|H\|_\infty = 1$ having $(1 - o(1))(1 - \varepsilon)n^m$ negative eigenvalues, each of magnitude at least εm^{-m}. In the particular case when $\varepsilon = \binom{md}{d,\ldots,d}^{-1}$ for some positive integer d, this bound on the magnitude can be improved to ε.*

Proof. This follows from e.g. [DJL24, Proposition 5.4] by taking $H = \mathbb{1} - \mu\Pi_{\mathcal{U}}$, where $\Pi_{\mathcal{U}}$ is the projection onto one of the subspaces specified in Theorem 1.2 and $\mu = (1 - E(\mathcal{U}))^{-1}$. □

Acknowledgments

H.D. was supported by the National Science Foundation under Grant No. DMS-2147769. B.L. acknowledges that part of this work was funded by the National Science Foundation under Award No. DMS-2202782.

References

[AN13] Muneerah Al Nuwairan. Potential examples for non-additivity of the minimal output entropy. *arXiv preprint*, arXiv:1312.2200, 2013.

[AN14] Muneerah Al Nuwairan. The extreme points of SU(2)-irreducibly covariant channels. *International Journal of Mathematics*, 25(06):1450048, 2014.

[ASW11] Guillaume Aubrun, Stanisław Szarek, and Elisabeth Werner. Hastings's additivity counterexample via Dvoretzky's theorem. *Communications in Mathematical Physics*, 305:85–97, 2011.

[ASY14] Guillaume Aubrun, Stanisław Szarek, and Deping Ye. Entanglement thresholds for random induced states. *Communications on Pure and Applied Mathematics*, 67(1):129–171, 2014.

[ATL11] Remigiusz Augusiak, Jordi Tura, and Maciej Lewenstein. A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces. *Journal of Physics A: Mathematical and Theoretical*, 44:212001, 2011.

[BBEM90] Bernard Beauzamy, Enrico Bombieri, Per Enflo, and Hugh L Montgomery. Products of polynomials in many variables. *Journal of Number Theory*, 36(2):219–245, 1990.

[BC18] Michael Brannan and Benoît Collins. Highly entangled, non-random subspaces of tensor products from quantum groups. *Communications in Mathematical Physics*, 358:1007–1025, 2018.

[BCLY20] Michael Brannan, Benoît Collins, Hun Hee Lee, and Sang-Gyun Youn. Temperley–Lieb quantum channels. *Communications in Mathematical Physics*, 376(2):795–839, 2020.

[BCN12] Serban Belinschi, Benoît Collins, and Ion Nechita. Eigenvectors and eigenvalues in a random subspace of a tensor product. *Inventiones Mathematicae*, 190:647–697, 2012.

[BDM+99] Charles H. Bennett, David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82:5385–5388, 1999.

[BESV24] Aditya Bhaskara, Eric Evert, Vaidehi Srinivas, and Aravindan Vijayaraghavan. New tools for smoothed analysis: Least singular value bounds for random matrices with dependent entries. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 375–386, 2024.

[BH10] Fernando GSL Brandao and Michał Horodecki. On Hastings' counterexamples to the minimum output entropy additivity conjecture. *Open Systems & Information Dynamics*, 17(01):31–52, 2010.

[Bha06] B. V. Rajarama Bhat. A completely entangled subspace of maximal dimension. *International Journal of Quantum Information*, 4:325–330, 2006.

[CHL+08] Toby Cubitt, Aram W Harrow, Debbie Leung, Ashley Montanaro, and Andreas Winter. Counterexamples to additivity of minimum output p-Rényi entropy for p close to 0. *Communications in Mathematical Physics*, 284(1):281–290, 2008.

[CMW08] Toby Cubitt, Ashley Montanaro, and Andreas Winter. On the dimension of subspaces with bounded Schmidt rank. *Journal of Mathematical Physics*, 49:022107, 2008.

[CS14] Dariusz Chruściński and Gniewomir Sarbicki. Entanglement witnesses: construction, analysis and classification. *Journal of Physics A: Mathematical and Theoretical*, 47:483001, 2014.

[DJL24] Harm Derksen, Nathaniel Johnston, and Benjamin Lovitz. X-arability of mixed quantum states. *arXiv preprint*, arXiv:2409.18948, 2024.

[FGHK16] Magnus Gausdal Find, Alexander Golovnev, Edward A Hirsch, and Alexander S Kulikov. A better-than-3n lower bound for the circuit complexity of an explicit function. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 89–98. IEEE, 2016.

[FK10] Motohisa Fukuda and Christopher King. Entanglement of random subspaces via the hastings bound. *Journal of Mathematical Physics*, 51(4), 2010.

[GHP10] Andrzej Grudka, Michał Horodecki, and Łukasz Pankowski. Constructive counterexamples to the additivity of the minimum output Rényi entropy of quantum channels for all $p > 2$. *Journal of Physics A: Mathematical and Theoretical*, 43(42):425304, 2010.

[Har13a] Joe Harris. *Algebraic Geometry: A First Course*. Graduate Texts in Mathematics. Springer New York, 2013.

[Har13b] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint*, arXiv:1308.6595, 2013.

[Has09] Matthew B Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, 2009.

[Hay07] Patrick Hayden. The maximal p-norm multiplicativity conjecture is false. *arXiv preprint arXiv:0707.3291*, 2007.

[HLW06] Patrick Hayden, Debbie W Leung, and Andreas Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265:95–117, 2006.

[Hor97] Pawel Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232:333–339, 1997.

[HW08] Patrick Hayden and Andreas Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all p$>$ 1. *Communications in Mathematical Physics*, 284(1):263–280, 2008.

[Khi97] A Ya Khinchin. *Continued Fractions*. Dover Publications, 1997.

[LM19] JM Landsberg and Mateusz Michałek. Towards finding hay in a haystack: explicit tensors of border rank greater than $2.02m$ in $\mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$. *arXiv preprint*, arXiv:1912.11927, 2019.

[NS22] Aditya Nema and Pranab Sen. Approximate unitary designs give rise to quantum channels with super additive classical holevo capacity. *IEEE Transactions on Information Theory*, 68(9):5937–5954, 2022.

[Par04] K. R. Parthasarathy. On the maximal dimension of a completely entangled subspace for finite level quantum systems. *Proceedings Mathematical Sciences*, 114:365–374, 2004.

[Sho04] Peter W Shor. Equivalence of additivity questions in quantum information theory. *Communications in Mathematical Physics*, 246(3):453–472, 2004.

[SS24] Krzysztof Szczygielski and Michał Studziński. New constructive counterexamples to additivity of minimum output Rényi p-entropy of quantum channels. *IEEE Transactions on Information Theory*, 2024.

[TS17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 238–251, 2017.

[Zei94] Doron Zeilberger. Chu's 1303 identity implies Bombieri's 1990 norm-inequality (via an identity of Beauzamy and Dégot). *The American Mathematical Monthly*, 101(9):894–896, 1994.

[ZZZ24] Xuanran Zhu, Chao Zhang, and Bei Zeng. Quantifying subspace entanglement with geometric measures. *Physical Review A*, 110(1):012452, 2024.