

Super-Duper-Activation of Quantum Zero-Error Capacities

Toby S. Cubitt^{*1} and Graeme Smith^{†2}

¹*Department of Mathematics, University of Bristol
University Walk, Bristol BS8 1TW, United Kingdom*

²*IBM T.J. Watson Research Center
Yorktown Heights, NY 10598, USA*

January 8, 2010

Abstract

The zero-error capacity of a channel is the rate at which it can send information perfectly, with zero probability of error, and has long been studied in classical information theory. We show that the zero-error capacity of quantum channels exhibits an extreme form of non-additivity, one which is not possible for classical channels, or even for the usual capacities of quantum channels. By combining probabilistic arguments with algebraic geometry, we prove that there exist channels \mathcal{E}_1 and \mathcal{E}_2 with no zero-error *classical* capacity whatsoever, $C_0(\mathcal{E}_1) = C_0(\mathcal{E}_2) = 0$, but whose joint zero-error *quantum* capacity is positive, $Q_0(\mathcal{E}_1 \otimes \mathcal{E}_2) \geq 1$. We term this striking effect *super-duper-activation*, as it implies that both the classical and quantum zero-error capacities of these channels can be superactivated simultaneously, whilst being a strictly stronger property of capacities. Superactivation of the quantum zero-error capacity was not previously known.

^{*}toby.cubitt@bristol.ac.uk

[†]gsbsmith@gmail.com

1 Introduction

The zero-error capacity, introduced by Shannon in 1956, characterises the optimal achievable communication rate of a noisy channel when information must be transmitted with zero probability of error [1]. This is in contrast with the more traditional capacity, which only demands error probabilities vanishing in the limit of many channel uses. The question of zero-error capacity (and more generally zero-error information theory [2]) has a much more combinatorial flavor than the usual case, and has played an important role in the development of graph theory. Combinatorial optimisation problems are often intractable so, perhaps unsurprisingly, the zero-error capacity is unknown even for many very simple channels.

Quantum information theory seeks to extend information theory to include information sources and communication systems where quantum effects are important. Because all physical systems are fundamentally quantum, this can be seen as an attempt to more accurately model physical information processing systems. Furthermore, expanding our notion of information to include quantum messages leads to new insights and applications, such as quantum cryptography and quantum computing. Because quantum systems are notoriously delicate, error correction is extremely important, and the capacities of a noisy quantum channel for transmitting various types of information noiselessly play a central role in the theory. In the context of zero-error quantum information theory, first studied in Ref. [3], the central capacities are the zero-error classical and zero-error quantum capacities.

A rather surprising effect has recently been discovered in the theory of quantum communication. Classically, there is a simple criterion for deciding whether a channel has non-zero capacity—any channel with some correlation between input and output has some positive capacity—and this criterion carries over to the classical capacity of quantum channels. However, when sending quantum information, the situation is very different. There are some quantum channels that are sufficiently noisy to have zero capacity for quantum communications, yet can still create correlations. In Ref. [4] it was shown that there are pairs of channels with very different noise characteristics, but both with zero quantum capacity, that, when used together, have a large joint quantum capacity. This *superactivation* is completely different from what happens in the classical case, and depends crucially on choosing entangled signal states for the joint channel.

Superactivation of classical channel capacities is easily seen to be impossi-

ble, both for the usual capacity and the zero-error capacity. If two classical channels have no correlation between input and output, so that their usual classical capacity vanishes, this will also hold for the joint channel. Similarly, if two classical channels each have the property that all pairs of inputs can lead to ambiguous outputs, so that the zero-error capacity vanishes, then the joint channel necessarily has this property too. The argument for the usual classical capacity carries over directly to the case of quantum channels: superactivation of the classical capacity of a quantum channel remains impossible.

However, in Ref. [5] it was shown that the *zero-error* classical capacity of a quantum channel actually *can* be superactivated (see also Ref. [6], which found superactivation of the non-asymptotic one-shot zero-error classical capacity, and a weaker form of activation in the asymptotic setting). In this paper, we significantly strengthen the results and techniques of Ref. [5]. There, techniques from algebraic geometry were combined with probabilistic arguments to show that there are pairs of channels, each with vanishing zero-error classical capacity, that have positive joint zero-error classical capacity when used together. Here, we find that there exist pairs of channels which each have vanishing zero-error classical capacity, as before, but when the two channels are used together they can even transmit *quantum* information with zero-error (indeed, only a single use of the joint channel is required). This is the strongest possible form of superactivation (which we therefore call *super-duper-activation*). It implies simultaneous superactivation of both the classical (already known from Ref. [5]) and quantum (previously unknown) zero-error capacities of quantum channels, whilst being strictly stronger than either of these.

The rest of the paper is organised as follows. In the next section we review some basic facts about quantum mechanics and algebraic geometry. Section 3 establishes sufficient conditions for super-duper-activation, whilst Section 4 shows that there exist channels which satisfy these conditions. Finally, Section 5 discusses the implications of our findings.

2 Preliminaries

2.1 Quantum Mechanics

A minimum uncertainty state of a d -level quantum system is a pure state, represented by a d -dimensional complex unit vector $|\psi\rangle \in \mathbb{C}^d$. More generally, the state of a d -level system is given by a density matrix, $\rho \in \mathcal{B}(\mathbb{C}^d)$, where,

$\mathcal{B}(\mathbb{C}^d)$ denotes the set of bounded linear operators on \mathbb{C}^d . Such a density matrix is Hermitian ($\rho = \rho^\dagger$) and has unit trace: $\text{Tr } \rho = 1$. As a result, any such ρ admits a spectral decomposition $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with orthogonal $|\psi_i\rangle$, which can be interpreted as describing a system that is in state $|\psi_i\rangle$ with probability p_i . Whilst we will not need to consider measurement processes below, we will need to know when there is some measurement to distinguish two states. This is possible exactly when the states are orthogonal: for pure states $\langle\psi|\phi\rangle = 0$ or for mixed states $\text{Tr } \rho\sigma = 0$.

It is sometimes useful to consider (unnormalised) pure states $|\psi\rangle_{AB}$ in a bipartite space $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ as matrices $M = \mathbb{M}(|\psi\rangle_{AB})$ in the isomorphic space of $d_A \times d_B$ matrices \mathcal{M}_{d_A, d_B} . The isomorphism arises from fixing some product basis $|i\rangle_A |j\rangle_B$ for $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, and expanding $|\psi\rangle_{AB} = \sum_{i,j} M_{ij} |i\rangle_A |j\rangle_B$ in this basis. A bipartite subspace $S \subseteq \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ is isomorphic in this way to a matrix subspace which we denote $\mathbb{M}(S)$.

We define the ‘‘flip’’ operation on a bipartite state as the operation that swaps the two systems and takes the complex conjugate:

$$\mathbb{F}(|\psi\rangle_{AB}) = \text{SWAP}(|\bar{\psi}\rangle_{AB}). \quad (1)$$

In terms of the matrix representation $M = \mathbb{M}(|\psi\rangle_{AB})$, the flip operation is just Hermitian conjugation: $\mathbb{M}(\mathbb{F}|\psi\rangle_{AB}) = M^\dagger$. The flip operation can be extended to operators and subspaces in the obvious way.

The most general physical operation in quantum mechanics is a completely positive trace preserving (CPT) map from $\mathcal{B}(\mathbb{C}^{d_{\text{in}}})$ to $\mathcal{B}(\mathbb{C}^{d_{\text{out}}})$, where d_{in} and d_{out} are the input and output dimensions of the map. We will refer to such operations as *quantum channels* throughout, as they are directly analogous to channels in classical information theory. A quantum channel that maps a space A to B can always be thought of as an isometry followed by a partial trace. In other words, for any channel \mathcal{E} we have $\mathcal{E}(\rho) = \text{Tr}_E U \rho U^\dagger$, where $U : A \rightarrow BE$ is an isometry satisfying $U^\dagger U = I_A$. Equivalently, the action of a channel can be expressed in terms of Kraus operators: $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$, where $\sum_k A_k^\dagger A_k = I_A$. A third representation of quantum channels (indeed, it extends to any linear map), which plays an important role in Ref. [5], is the *Choi-Jamiołkowski matrix*, defined to be the result of applying the channel to one half of an unnormalised maximally entangled state. In other words, the Choi-Jamiołkowski matrix of a channel \mathcal{E} is given by $\sigma = (\mathcal{I} \otimes \mathcal{E})(\omega)$ where $\omega = \sum_{i=1}^{d_A} |i\rangle |i\rangle$. The action of the channel can be recovered from the Choi-Jamiołkowski matrix via $\mathcal{E}(\rho) = \text{Tr}_A [\sigma_{AB} \cdot \rho_A^T \otimes \mathbb{1}_B]$ (where ρ_A^T denotes the transpose of the density matrix ρ_A).

We will also need the $*$ -conjugate \mathcal{E}^* of a channel \mathcal{E} , which is simply the dual with respect to the Hilbert-Schmidt inner product, i.e. the unique map defined by:

$$\mathrm{Tr}[X^\dagger \mathcal{E}(Y)] = \mathrm{Tr}[\mathcal{E}^*(X)^\dagger Y]. \quad (2)$$

In terms of Kraus operators A_k , the $*$ -conjugate is the channel whose Kraus operators are the Hermitian conjugates A_k^\dagger .

2.2 Algebraic Geometry

In order to prove our results, we need some basic notions from algebraic geometry (see e.g. Ref. [7]). A key concept is that of a *Zariski-closed* set, and the resulting *Zariski topology*. We will only ever work over base fields \mathbb{C} or \mathbb{R} , so for our purposes Zariski-closed sets are sets defined by a collection of polynomial equations, i.e. they are the solution sets of simultaneous polynomial equations. We will use the terms *Zariski-closed set* and *algebraic set* interchangeably.

The Zariski topology is the topology whose *closed* sets are the Zariski-closed sets. It is the standard topology in algebraic geometry, but it serves more as a convenient terminology than providing any useful geometric information. The main use we will make of it is the fact that intersections of Zariski-closed sets are themselves Zariski-closed. Indeed, the only Zariski-closed set that has non-zero measure (in the usual sense on \mathbb{C}^d or \mathbb{R}^d) is the entire space. This “Zariski dichotomy”—that a Zariski-closed set is either zero-measure or the entire space—lies at the heart of our proofs.

We will also frequently refer to the *Grassmannian* $\mathrm{Gr}_d(V)$ of a vector space V : the set of all d -dimensional subspaces of V . There is a standard way of embedding the Grassmannian in projective space, called the *Plücker embedding* and conventionally denoted ι . If a d -dimensional subspace in the Grassmannian is spanned by some basis $\{|\psi_i\rangle\}$, then $\iota(S)$ is defined to be $\wedge_{i=1}^d |\psi_i\rangle$, with \wedge denoting the anti-symmetric product. This is uniquely defined, since picking some other basis replaces $|\psi_i\rangle$ by $\sum_{j=1}^d A_{i,j} |\psi_j\rangle$ for some invertible matrix A , which in turn replaces $\iota(S)$ by $\det(A)\iota(S)$. In projective space, rescaling by the scalar $\det(A)$ makes no difference.

Via the Plücker embedding, points in the Grassmannian are naturally parametrised by the coordinates of points in projective space, called the *Plücker coordinates*. (Note that not all points in the ambient projective space correspond to points in the Grassmannian; the Plücker coordinates of points within the Grassmannian must satisfy quadratic constraints called

the *Plücker relations*.) Thus the Plücker coordinates P_{α_d} of S are defined by $\sum_{\alpha_d} P_{\alpha_d} (\wedge_{j \in \alpha_d} |j\rangle) = \wedge_{i=1}^d |\psi_i\rangle$, where α_d are size d subsets of $\{1 \dots n\}$, with $|1\rangle, \dots, |n\rangle$ a basis of V .

3 Sufficient Conditions for Super-Duper-Activation

We start by reducing the problem of proving existence of super-duper-activation to a question about the existence of subspaces satisfying certain conditions. The arguments are very similar to those leading to Theorem 13 of Ref. [5], but the stronger requirement that the joint channel have positive *quantum zero-error capacity* adds an additional constrain on the subspaces. To derive this new constraint, we need the following lemma, which gives us a sufficient condition for a channel to have positive zero-error quantum capacity.

Lemma 1 *Let $\mathcal{E} : A \rightarrow B$ be a channel, $|0\rangle$ and $|1\rangle$ be states on A , and $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. Then, if*

$$\text{Tr} [\mathcal{E}(|0\rangle\langle 0|) \mathcal{E}(|1\rangle\langle 1|)] = 0 \quad (3)$$

and

$$\text{Tr} [\mathcal{E}(|+\rangle\langle +|) \mathcal{E}(|-\rangle\langle -|)] = 0, \quad (4)$$

we have $Q_0(\mathcal{E}) \geq 1$.

Proof To see this, suppose A_k are the Kraus operators of \mathcal{E} and $\varphi = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$, and let

$$\mathcal{R}_\varphi(\rho) = \sum_k \sqrt{\varphi} A_k^\dagger \mathcal{E}(\varphi)^{-1/2} \rho \mathcal{E}(\varphi)^{-1/2} A_k \sqrt{\varphi} \quad (5)$$

be the reversal operation of Ref. [8]. This is completely positive and trace preserving by design, and $\mathcal{M} := \mathcal{R}_\varphi \circ \mathcal{E}$ is the identity on $\text{span}(|0\rangle, |1\rangle)$. To see this, first note that, by assumption,

$$0 = \text{Tr} [\mathcal{E}(|0\rangle\langle 0|) \mathcal{E}(|1\rangle\langle 1|)] \quad (6a)$$

$$= \sum_{j,k} \text{Tr} \left[A_j |0\rangle\langle 0| A_j^\dagger A_k |1\rangle\langle 1| A_k^\dagger \right] \quad (6b)$$

$$= \sum_{j,k} \left| \langle 0| A_j^\dagger A_k |1\rangle \right|^2, \quad (6c)$$

so that $\langle 0|A_j^\dagger A_k|1\rangle = 0$ for all j, k , and similarly for $\langle +|A_j^\dagger A_k|-\rangle$. Now consider

$$\text{Tr} \left[\sqrt{\varphi} A_k^\dagger \mathcal{E}(\varphi)^{-1/2} \mathcal{E}(|0\rangle\langle 0|) \mathcal{E}(\varphi)^{-1/2} A_k \sqrt{\varphi} |1\rangle\langle 1| \right] \quad (7a)$$

$$= \frac{1}{2} \text{Tr} \left[A_k^\dagger \mathcal{E}(\varphi)^{-1/2} \mathcal{E}(|0\rangle\langle 0|) \mathcal{E}(\varphi)^{-1/2} A_k |1\rangle\langle 1| \right] \quad (7b)$$

$$= \frac{1}{2} \text{Tr} \left[\mathcal{E}(\varphi)^{-1/2} \mathcal{E}(|0\rangle\langle 0|) \mathcal{E}(\varphi)^{-1/2} \mathcal{E}(|1\rangle\langle 1|) \right]. \quad (7c)$$

Since $\mathcal{E}(|0\rangle\langle 0|)$ and $\mathcal{E}(|1\rangle\langle 1|)$ are orthogonal, we have

$$\mathcal{E}(\varphi)^{-1/2} = \sqrt{2} \mathcal{E}(|0\rangle\langle 0|)^{-1/2} + \sqrt{2} \mathcal{E}(|1\rangle\langle 1|)^{-1/2}, \quad (8)$$

which immediately implies with the above that

$$\mathcal{M}(|0\rangle\langle 0|) = |0\rangle\langle 0| \quad (9a)$$

$$\mathcal{M}(|1\rangle\langle 1|) = |1\rangle\langle 1|. \quad (9b)$$

Similarly, we also have

$$\mathcal{M}(|+\rangle\langle +|) = |+\rangle\langle +| \quad (10a)$$

$$\mathcal{M}(|-\rangle\langle -|) = |-\rangle\langle -|. \quad (10b)$$

Now all we have to do is show that any CPT map \mathcal{M} satisfying the above four equations must be the identity. We can easily use these four equations to show that

$$\mathcal{M}(\mathbb{1}) = \mathbb{1} \quad (11a)$$

$$\mathcal{M}(X) = X \quad (11b)$$

$$\mathcal{M}(Z) = Z, \quad (11c)$$

which also implies that $\mathcal{M}(Y) = \lambda Y$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. All we have to do now is show that for any such map to be CP we need $\lambda = 1$. This is easily confirmed by considering the action of \mathcal{M} on $|\phi_d\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. \square

We are now in a position to reduce the super-duper-activation problem to a question about subspaces. The following theorem is a lot like Theorem 13 in Ref. [5].

Theorem 2 *Suppose there is a subspace S such that*

$$\forall k, \nexists |\psi\rangle, |\varphi\rangle \in \mathcal{H}_A^{\otimes k} : |\psi\rangle \otimes |\varphi\rangle \in (S^{\otimes k})^\perp, \quad (12a)$$

$$\forall k, \nexists |\psi\rangle, |\varphi\rangle \in \mathcal{H}_A^{\otimes k} : |\psi\rangle \otimes |\varphi\rangle \in ((S^\perp)^{\otimes k})^\perp, \quad (12b)$$

$$\mathbb{F}(S) = S, \quad (12c)$$

$$\mathbb{F}(\mathbb{1} \otimes X \cdot S) = \mathbb{1} \otimes X \cdot S, \quad (12d)$$

$$\exists \{M_i \geq 0\} : \mathbb{M}(S) = \text{span}\{M_i\}, \quad (12e)$$

$$\exists \{M_j \geq 0\} : \mathbb{M}(\mathbb{1} \otimes X \cdot S^\perp) = \text{span}\{M_j\}, \quad (12f)$$

$$S \perp (\mathbb{1} + X) \otimes (\mathbb{1} - X)S^\perp. \quad (12g)$$

Then there exist channels $\mathcal{E}_{1,2}$ with $C_0(\mathcal{E}_1) = C_0(\mathcal{E}_2) = 0$ but $Q_0(\mathcal{E}_1 \otimes \mathcal{E}_2) \geq 1$.

Proof Equations (12a)–(12f) are identical to the conditions in Theorem 13 of Ref. [5], and are derived in exactly the same way. Only Eq. (12g) is new, so we will focus on that. Recall from Ref. [5] that S will be the support of $\sigma_1 = (\mathcal{I} \otimes \mathcal{E}_1^* \circ \mathcal{E}_1)(|\omega\rangle\langle\omega|)$ with $|\omega\rangle = \sum_i |i\rangle|i\rangle$ and $S_2 = (\mathbb{1} \otimes X)S^\perp$ the support of σ_2^T defined similarly. The two signal states for $\mathcal{E}_1 \otimes \mathcal{E}_2$ are $|\varphi_0\rangle = |\phi_d\rangle$ and $|\varphi_1\rangle = (\mathbb{1} \otimes X)|\phi_d\rangle$. What we have to do now is show that, letting $|\varphi_\pm\rangle = (|\varphi_0\rangle \pm |\varphi_1\rangle)/\sqrt{2}$, we have

$$\text{Tr}[(\mathcal{E}_1 \otimes \mathcal{E}_2)(|\varphi_+\rangle\langle\varphi_+|)(\mathcal{E}_1 \otimes \mathcal{E}_2)(|\varphi_-\rangle\langle\varphi_-|)] = 0. \quad (13)$$

Now,

$$\text{Tr}[(\mathcal{E}_1 \otimes \mathcal{E}_2)(|\varphi_+\rangle\langle\varphi_+|)(\mathcal{E}_1 \otimes \mathcal{E}_2)(|\varphi_-\rangle\langle\varphi_-|)] \quad (14a)$$

$$= \text{Tr}[(\mathcal{E}_1^* \circ \mathcal{E}_1 \otimes \mathcal{E}_2^* \circ \mathcal{E}_2)(|\varphi_+\rangle\langle\varphi_+|)|\varphi_-\rangle\langle\varphi_-|] \quad (14b)$$

$$= \text{Tr}\left[\sigma_1^{A'_1 A_1} \otimes \sigma_2^{A'_2 A_2} |\varphi_+\rangle\langle\varphi_+|_{A'_1 A'_2}^T \otimes |\varphi_-\rangle\langle\varphi_-|_{A_1 A_2}\right] \quad (14c)$$

$$= \text{Tr}\left[\sigma_1^{A'_1 A_1} \otimes \sigma_2^{A'_2 A_2} \left(P_+ \otimes \mathbb{1} |\omega\rangle\langle\omega|_{A'_1 A'_2} P_+ \otimes \mathbb{1}\right) \otimes \left(P_- \otimes \mathbb{1} |\omega\rangle\langle\omega|_{A_1 A_2} P_- \otimes \mathbb{1}\right)\right] \quad (14d)$$

$$= \text{Tr}\left[\left(P_+ \otimes P_-\right)\sigma_1^{A'_1 A_1} \left(P_+ \otimes P_-\right) \otimes \sigma_2^{A'_2 A_2} |\omega\rangle\langle\omega|_{A'_1 A'_2} \otimes |\omega\rangle\langle\omega|_{A_1 A_2}\right] \quad (14e)$$

$$= \text{Tr}\left[\left[\left(P_+ \otimes P_-\right)\sigma_2 \left(P_+ \otimes P_-\right)\right]^T \sigma_1\right] \quad (14f)$$

where $P_{\pm} = (\mathbb{1} \pm X)/2$ are projectors and we have used the fact that $\text{Tr}[\langle \omega | M \otimes N \rangle] = \text{Tr}[N^T M]$. As a result, the requirement Eq. (13) is met by choosing $S \perp (P_+ \otimes P_-)S_2$. This is equivalent to $S \perp (\mathbb{1} + X) \otimes (\mathbb{1} - X)S^\perp$, since $P_-X = -P_-$ and we chose $S_2 = (\mathbb{1} \otimes X)S^\perp$. \square

4 Existence of Super-Duper-Activation

Given Theorem 2, all we need to do in order to show the super-duper-activation phenomenon is to prove that there do exist subspaces satisfying the conditions of the theorem. We use a combination of algebraic-geometry and probabilistic arguments to establish this result.

In what follows, we will need to consider a number of sets of subspaces. Recall the definition of extendibility from Refs. [5, 9]:

Definition 3 *A subspace $S \in \mathcal{H}_A \otimes \mathcal{H}_B$ is k -unextendible if $(S^{\otimes k})^\perp$ contains no product state in $\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}$. A subspace is strongly unextendible if it is k -unextendible for all $k \geq 1$. Conversely, a subspace is k -extendible if it is not k -unextendible, and extendible if it is not strongly unextendible.*

Following Ref. [5], we denote the sets of d -dimensional k -extendible, extendible, and unextendible subspaces, respectively, by

$$E_d^k(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \text{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) | S \text{ is } k\text{-extendible}\}, \quad (15)$$

$$E_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \text{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) | S \text{ is extendible}\}, \quad (16)$$

$$U_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \text{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) | S \text{ is unextendible}\}, \quad (17)$$

Lemma 15 of Ref. [5] proves that E_d^k is Zariski-closed in $\text{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) = \text{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$.

We will also refer to the set

$$F_d(\mathbb{R}, d_A) = \{S \in \text{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}) | \\ S = iS, \mathbb{F}(S) = S, \mathbb{F}(\mathbb{1} \otimes X \cdot S) = \mathbb{1} \otimes X \cdot S\} \quad (18)$$

of subspaces satisfying the symmetry constraints of Eqs. (12c) and (12d). Note that we are considering F_d as a subset of the *real* Grassmannian, in which context $i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Lemma 17 of Ref. [5] proves that F_d is Zariski-closed in $\text{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A})$.

In order to extend the arguments of Ref. [5] to our case, we will need to consider an additional set: the set of subspaces satisfying the orthogonality

constraint of Eq. (12g):

$$C_d(\mathbb{C}, d_A) = \{S \in \text{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}) | S \perp (\mathbb{1} + X) \otimes (\mathbb{1} - X) S^\perp\}, \quad (19)$$

and also the isomorphic set of real vector spaces:

$$C_d(\mathbb{R}, d_A) = \{S \in \text{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}) | S = iS, S \perp (\mathbb{1} + X) \otimes (\mathbb{1} - X) S^\perp\}. \quad (20)$$

The first step is to show that this set is algebraic (cf. Lemma 17 of Ref. [5]).

Lemma 4 $C_d(\mathbb{C}, d_A)$ is Zariski-closed in $\text{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A})$.

Proof First, we let $W = \wedge_{i=1}^d |\psi_i\rangle$ for some basis $\{|\psi_i\rangle\}$ of S . We have $|\psi\rangle \in S$ exactly when $|\psi\rangle \wedge W = 0$ and we want to use this to construct a basis for S^\perp . If P_{α_d} are the Plücker coordinates of S , and supposing $|\psi\rangle = \sum_{i=1}^n v_i |i\rangle$, then $|\psi\rangle$ is in S exactly when

$$|\psi\rangle \wedge W = \sum_{\alpha_d} \sum_i v_i P_{\alpha_d} |i\rangle \wedge (\wedge_{j \in \alpha_d} |j\rangle) \quad (21a)$$

$$= \sum_{i, \beta_{d+1}} v_i N_{i, \beta_{d+1}} \wedge_{k \in \beta_{d+1}} |k\rangle = 0, \quad (21b)$$

so that we have an N such that $|\psi\rangle \in S$ iff $\langle \psi | N = 0$. Now, the support of NN^\dagger is S^\perp and its eigenvalues are positive. Most importantly, we can think of NN^\dagger as a matrix with entries that are quadratic polynomials in P_{α_d} . Thus, we are interested in ensuring that

$$N \cdot P_+ \otimes P_- |\psi\rangle = 0 \quad (22)$$

for all $|\psi\rangle \in S$, which is equivalent to showing that

$$N^{\otimes n} (P_+ \otimes P_-)^{\otimes n} \iota(S) = 0. \quad (23)$$

This is a linear constraint on $\iota(S)$, so $\{\iota(S) : N^{\otimes n} (P_+ \otimes P_-)^{\otimes n} \iota(S) = 0\}$ is Zariski-closed. Since ι is a proper morphism (cf. Lemma 17 of Ref. [5]), $C_d = \{S : \forall |\psi\rangle \in S, N \cdot P_+ \otimes P_- |\psi\rangle = 0\}$ must also be Zariski-closed. \square

Any Zariski-closed set in a complex vector space is also Zariski-closed in the isomorphic real vector space. Furthermore, the intersection of two Zariski-closed sets is again Zariski-closed. This immediately gives:

Corollary 5 $E_d^k(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ is Zariski-closed in $F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$.

We can now use the ‘‘Zariski dichotomy’’ to prove that the set of strongly unextendible subspaces is full measure in $F_d \cap C_d$.

Lemma 6 For $d \geq 12(d_A + d_B - 1)$, the set of strongly unextendible subspaces $U_d(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$ is full measure in $F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$.

Proof Since $E_d^k(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ is Zariski-closed by Corollary 5, $\bigcup_k E_d^k(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ is a countable union of Zariski-closed sets, so it is either zero measure (in the usual Haar measure) in $F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$, or it is the full space. Conversely, its complement $U_d(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ is either full measure or empty.

To rule out the possibility that it is empty, we prove that there exists a subspace in $U_d \cap F_d \cap C_d$ by constructing one using unextendible product bases (UPBs). Lemma 22 of Ref. [5] proves that the span of a UPB is a strongly unextendible subspace, and Ref. [10] showed that UPBs of dimension m exist in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ for any $m \geq d_A + d_B - 1$. Let S be a subspace spanned by such a minimal UPB, and let the set of matrices $\{M_i\}$ be a basis for $\mathbb{M}(S)$. Consider the symmetrised subspace $\mathbb{M}(S')$ spanned by

$$\begin{aligned} & \left\{ M, XMX, M^\dagger, XM^\dagger X, \right. \\ & \quad P_+MP_-, P_+XMXP_-, P_+M^\dagger P_-, P_+XM^\dagger XP_-, \\ & \quad \left. P_-MP_+, P_-XMXP_+, P_-M^\dagger P_+, P_-XM^\dagger XP_+ \right\}. \end{aligned} \quad (24)$$

The resulting subspace S' has dimension at most $12(d_A + d_B - 1)$, and satisfies both the symmetry and orthogonality constraints of Eqs. (12c), (12d) and (12g) from Theorem 2. Thus $S' \in F_d \cap C_d$. As $S \subseteq S'$, S' is clearly strongly unextendible, which completes the proof. \square

Corollary 7 For $d_A \geq 48$, and for a subspace $S \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}$ of dimension $12(2d_A - 1) \leq d \leq d_A^2 - 12(2d_A - 1)$ chosen uniformly at random subject to the constraints $\mathbb{F}(S) = S$, $\mathbb{F}(\mathbb{1} \otimes X \cdot S) = \mathbb{1} \otimes X \cdot S$ and $S \perp (\mathbb{1} + X) \otimes (\mathbb{1} - X) S^\perp$, both S and S^\perp will almost-surely be strongly unextendible.

Proof Lemma 6 implies that S chosen in this way will almost-surely be strongly unextendible. But S^\perp is then a random subspace subject to the same

constraints, with dimension $12(2d_A - 1) \leq d^\perp = d_A^2 - d \leq d_A^2 - 12(2d_A - 1)$. Thus Lemma 6 implies that S^\perp will also be almost-surely strongly unextendible. For there to exist a suitable d , we require $12(2d_A - 1) \leq d_A^2 - 12(2d_A - 1)$, or $d_A \geq 48$. \square

Corollary 5 tells us that, although Eqs. (12a) and (12b) of Theorem 2 would appear to impose severe constraints on the subspace S , they are in fact benign. Even if we restrict to subspaces satisfying Eqs. (12c), (12d) and (12g), a randomly chosen subspace will satisfy Eqs. (12a) and (12b) with probability 1.

It remains to show that such a subspace can also satisfy Eqs. (12e) and (12f). For this, we require more information about the structure of the set $F_d \cap C_d$ of subspaces that simultaneously satisfy Eqs. (12c), (12d) and (12g).

Lemma 8 *If d_A is even, then*

$$\begin{aligned}
& F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A) \\
& \cong \bigoplus_{r=\max[0, d-\frac{d_A^2}{2}]}^{\min[d, \frac{d_A^2}{2}]} \bigoplus_{k_1=0}^r \bigoplus_{k_2=0}^{d-r} \left(\text{Gr}_{k_1}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{r-k_1}(\mathbb{R}^{d_A^2/2}) \times \right. \\
& \qquad \qquad \qquad \left. \text{Gr}_{k_2}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d-r-k_2}(\mathbb{R}^{d_A^2/2}) \right). \tag{25}
\end{aligned}$$

In other words, an element of $F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ can be uniquely identified by specifying non-negative integers r , k_1 and k_2 satisfying $d - d_A^2/2 \leq r \leq d$, $k_1 \leq r$ and $k_2 \leq d - r$, along with elements of $\text{Gr}_{k_1}(\mathbb{R}^{d_A^2/2})$, $\text{Gr}_{r-k_1}(\mathbb{R}^{d_A^2/2})$, $\text{Gr}_{k_2}(\mathbb{R}^{d_A^2/2})$ and $\text{Gr}_{d-r-k_2}(\mathbb{R}^{d_A^2/2})$.

Proof Elements of $F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$ are $2d$ -dimensional real subspaces of $\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}$. As such, they can be expressed as rank- $2d$ projectors. In terms of these projectors Π , the constraints in Eq. (18) defining $F_d(\mathbb{R}, d_A)$ become $i \Pi i^T = \Pi$, $\mathbb{F} \Pi \mathbb{F}^T = \Pi$ and $(X \otimes X) \Pi (X \otimes X) = \Pi$ (cf. Lemma 28 of Ref. [5]).

The additional constraint $S \perp (P_+ \otimes P_-)S^\perp$ in Eq. (20) defining $C_d(\mathbb{R}, d_A)$ can also be expressed as a symmetry of Π . Note that this constraint is symmetric: if S satisfies it, then so does S^\perp . (To see this, express the constraint as

$$\forall |\psi\rangle \in S^\perp, |\varphi\rangle \in S : \langle \varphi | P_+ \otimes P_- |\psi\rangle = 0 \tag{26}$$

and take the complex conjugate.) If Π is the projector corresponding to a subspace S , the constraint is equivalent to

$$\Pi(P_+ \otimes P_-)\Pi = (P_+ \otimes P_-)\Pi. \quad (27)$$

and we know the same holds for S^\perp :

$$(\mathbb{1} - \Pi)P(\mathbb{1} - \Pi) = P(\mathbb{1} - \Pi), \quad (28)$$

or, equivalently,

$$\Pi(P_+ \otimes P_-)\Pi = \Pi(P_+ \otimes P_-). \quad (29)$$

Together, Eqs. (27) and (29) imply that if Eq. (27) is satisfied then Π and $P_+ \otimes P_-$ commute. Conversely, it is easy to see that Eq. (27) is satisfied if Π commutes with $P_+ \otimes P_-$. Thus the subspace S is in $C_d(\mathbb{R}, d_A)$ iff Π commutes with $(P_+ \otimes P_-) = (\mathbb{1} + X) \otimes (\mathbb{1} - X)$ and $i\Pi i^T = \Pi$.

We will first consider the $P_+ \otimes P_-$ and \mathbb{F} symmetries. Since Π commutes with $P_+ \otimes P_-$, it must be of the form $\Pi = \Pi_{P_{+-}} + \Pi_{P_{+-}}^\perp$ where $\Pi_{P_{+-}}$ is a projector onto a subspace in the support of $P_+ \otimes P_-$, and $\Pi_{P_{+-}}^\perp$ is a projector onto a subspace in the orthogonal complement thereof. Note that, as we are working in the real vector space, $P_+ \otimes P_-$ is rank $d_A^2/2$. Now, \mathbb{F} exchanges $P_+ \otimes P_-$ with $P_- \otimes P_+$, so $\mathbb{F}\Pi\mathbb{F}^T = \Pi_{P_{-+}} + \Pi_{P_{-+}}^\perp$, where $\Pi_{P_{-+}}$ ($\Pi_{P_{-+}}^\perp$) is a projector onto a subspace in the (orthogonal complement of the) support of $P_- \otimes P_+$. But $\mathbb{F}\Pi\mathbb{F}^T = \Pi$, so $\Pi_{P_{-+}}$ must commute with $\Pi_{P_{+-}}^\perp$ and, furthermore, $\Pi_{P_{-+}} = \mathbb{F}\Pi_{P_{+-}}\mathbb{F}^T$. Thus

$$\Pi = (\Pi_{P_{+-}} + \mathbb{F}\Pi_{P_{+-}}\mathbb{F}^T) + \Pi^\perp, \quad (30)$$

where Π^\perp is a projector onto a subspace in the support of $\mathbb{1} - (P_+ \otimes P_- + P_- \otimes P_+)$ that satisfies $\mathbb{F}\Pi^\perp\mathbb{F}^T = \Pi^\perp$. Let $r \leq d$ denote the rank of $\Pi_{P_{+-}}$. Since $P_+ \otimes P_-$ has $d_A^2/2$ dimensional support, r cannot be larger than this. Also, as Π has rank $2d$, Π^\perp has rank $2(d - r)$. But Π^\perp must live in the support of $\mathbb{1} - (P_+ \otimes P_- + P_- \otimes P_+)$ which has dimension d_A^2 , so we require $2(d - r) \leq d_A^2$. Thus r is constrained to take values in the range

$$\max [0, d - d_A^2/2] \leq r \leq \min [d, d_A^2/2]. \quad (31)$$

Now consider the i and \mathbb{F} symmetries. Since $P_+ \otimes P_- + P_- \otimes P_+$ is invariant under both these operations, $\Pi_{P_{+-}} + \mathbb{F}\Pi_{P_{+-}}\mathbb{F}^T$ and Π^\perp must satisfy these symmetries independently. We first focus on Π^\perp . Let \mathbb{F}_\pm denote the

± 1 eigenspaces of \mathbb{F} . Since Π^\perp commutes with \mathbb{F} , it must be the sum of a projector onto a subspace of \mathbb{F}_+ and a projector onto a subspace of \mathbb{F}_- . In other words, $\Pi^\perp = \Pi_+^\perp + \Pi_-^\perp$ where $\Pi_\pm \mathbb{F} = \mathbb{F} \Pi_\pm = \pm \Pi_\pm$. Since i and \mathbb{F} anti-commute, i must map \mathbb{F}_\pm to \mathbb{F}_\mp . Thus $i \Pi_\pm^\perp i^T$ is a projector onto \mathbb{F}_\mp . Combined with the fact that $i \Pi^\perp i^T = \Pi^\perp$ we obtain $i \Pi_\pm^\perp i^T = \Pi_\mp^\perp$. We can thus assume that

$$\Pi^\perp = \Pi_+^\perp + i \Pi_+^\perp i^T \quad (32)$$

where Π_+^\perp is a projector onto \mathbb{F}_+ within the support of $\mathbb{1} - (P_+ \otimes P_- + P_- \otimes P_+)$. Since Π^\perp has rank $2(d-r)$, Π_+^\perp must have rank $d-r$.

Turning now to $\Pi_{P_{+-}} + \mathbb{F} \Pi_{P_{+-}} \mathbb{F}^T$, this already commutes with \mathbb{F} , so we must be able to rewrite it as $\Pi_{P_{+-}} + \mathbb{F} \Pi_{P_{+-}} \mathbb{F}^T = \Pi_+ + \Pi_-$ where Π_\pm are projectors onto \mathbb{F}_\pm within the support of $P_+ \otimes P_- + P_- \otimes P_+$. By the same argument as before, the i symmetry imposes $\Pi_- = i \Pi_+ i^T$, so

$$\Pi_{P_{+-}} + \mathbb{F} \Pi_{P_{+-}} \mathbb{F}^T = \Pi_+ + i \Pi_+ i^T. \quad (33)$$

Since $\Pi_{P_{+-}} + \mathbb{F} \Pi_{P_{+-}} \mathbb{F}^T$ has rank $2r$, Π_+ must have rank r .

Finally, consider the $X \otimes X$ symmetry. Since $X \otimes X$ commutes with \mathbb{F} and $P_{+-} \otimes P_{-+}$, we have that Π_+ and Π_+^\perp must also commute with $X \otimes X$. This means we can write Π_+ as $\Pi_{++} + \Pi_{+-}$ and Π_+^\perp as $\Pi_{++}^\perp + \Pi_{+-}^\perp$, where $\Pi_{+\pm}, \Pi_{+\pm}^\perp$ are projectors onto subspaces of the ± 1 eigenspace of $X \otimes X$. Since Π_+ has rank r , the ranks of Π_{++} and Π_{+-} must sum to r . Similarly, Π_+^\perp has rank $d-r$, so the ranks of Π_{++}^\perp and Π_{+-}^\perp must sum to $d-r$. Thus we have finally that

$$\Pi = \Pi_{++} + \Pi_{+-} + \Pi_{++}^\perp + \Pi_{+-}^\perp + i(\Pi_{++} + \Pi_{+-} + \Pi_{++}^\perp + \Pi_{+-}^\perp) i^T. \quad (34)$$

Conversely, if $\Pi_{++}, \Pi_{+-}, \Pi_{++}^\perp$ and Π_{+-}^\perp are arbitrary projectors with the appropriate supports and with ranks summing to r and $d-r$, respectively, then a Π of the above form projects onto a subspace in $F_d(\mathbb{R}, d_A) \cap C_d(\mathbb{R}, d_A)$. For each value of r satisfying Eq. (31), if Π_{++} and Π_{++}^\perp have ranks k_1 and k_2 , then our choice of Π is equivalent to choosing an element of $\text{Gr}_{k_1}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{r-k_1}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{k_2}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d-r-k_2}(\mathbb{R}^{d_A^2/2})$. \square

This structure lemma allows us to deal with the remaining conditions of Theorem 2, namely Eqs. (12e) and (12f), using probabilistic arguments.

Theorem 9 *If d_A is even, and $\lfloor d/2 \rfloor \leq d_A^2/2 - 2$, then the set*

$$P_d(d_A) = \{S \in F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A) \mid \exists M \in \mathbb{M}(S), M' \in \mathbb{M}(\mathbb{1} \otimes X \cdot S^\perp) : M, M' \geq 0\} \quad (35)$$

has non-zero measure in $F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$.

Proof Since $\dim \text{Gr}_k(\mathbb{R}^{d_A^2/2}) = (d_A^2/2 - k)k$, we have

$$\begin{aligned} & \dim \left(\text{Gr}_{k_1}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{r-k_1}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{k_2}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d-r-k_2}(\mathbb{R}^{d_A^2/2}) \right) \\ &= \left(\frac{d_A^2}{2} - k_1 \right) k_1 \left(\frac{d_A^2}{2} - r + k_1 \right) (r - k_1) \cdot \\ & \quad \left(\frac{d_A^2}{2} - k_2 \right) k_2 \left(\frac{d_A^2}{2} - d + r + k_1 \right) (d - r - k_2). \end{aligned} \quad (36)$$

which takes its maximum value at $r = d/2$, $k_1 = k_2 = d/4$ for d a multiple of 4, or the closest integers to this otherwise. This means that all but a measure-zero subset of $F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$ is contained in the component associated with these values of r , k_1 and k_2 . Indeed, if d is a multiple of 4 then the component of $F_d(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$ corresponding to $\text{Gr}_{d/4}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d/4}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d/4}(\mathbb{R}^{d_A^2/2}) \times \text{Gr}_{d/4}(\mathbb{R}^{d_A^2/2})$ has measure 1 in $F_d(\mathbb{C}, d_A)$. Otherwise, the components corresponding to the closest integers to $r = d/2$, $k_1 = k_2 = d/4$ together have total measure 1, with the measure split equally between them. For the remainder of the proof we will take $r = d/2$, $k_1 = k_2 = d/4$ (d divisible by 4) or any set of closest integers to these. Let $K_d(\mathbb{C}, d_A)$ denote the corresponding part of $F(\mathbb{C}, d_A) \cap C_d(\mathbb{C}, d_A)$.

It suffices to show that $P_d(d_A) \cap K_d(\mathbb{C}, d_A)$ has positive measure in $K_d(\mathbb{C}, d_A)$. To do so, we first construct a subspace $S \in K_d(\mathbb{C}, d_A)$ that contains a positive-definite element (i.e. $M > 0$ for some $M \in \mathbb{M}(S)$), such that $(\mathbb{1} \otimes X) \cdot S^\perp$ also contains a positive-definite element. This will guarantee that every $S' \in K_d(\mathbb{C}, d_A)$ that is sufficiently close to S will belong to $P_d(d_A) \cap K_d(\mathbb{C}, d_A)$, implying that this set has non-zero measure and proving the theorem.

To construct the desired S , note that for S to be positive definite it is sufficient for $\mathbb{M}(S)$ to contain a single positive-definite element. In particular, we will choose S to contain $|\omega\rangle = \sum_{i=1}^{d_A} |i, i\rangle$. We will also require that S be orthogonal to $(\mathbb{1} \otimes X)|\omega\rangle$ so that $(\mathbb{1} \otimes X)S^\perp$ also contains $|\omega\rangle$ and is

positive definite. (Note that this only works if d_A is even, otherwise $|\omega\rangle$ and $(\mathbb{1} \otimes X)|\omega\rangle$ are not orthogonal.)

$P_{\pm} \otimes P_{\mp} |\omega\rangle = P_{\pm} \otimes P_{\mp} (\mathbb{1} \otimes X) |\omega\rangle = 0$, so both $|\omega\rangle$ and $(\mathbb{1} \otimes X) |\omega\rangle$ are contained in the support of $\mathbb{1} - (P_+ \otimes P_- + P_- \otimes P_+)$. They also both belong to the +1 eigenspace of $X \otimes X$. Thus to choose S we need only choose an additional $k_2 - 1$ dimensions for Π_{++}^{\perp} (from a space of dimension $d^2/4 - 1$) as well as an arbitrary rank- $(d - r - k_2)$ projector Π_{+-}^{\perp} whose support is contained within the portion of the -1 eigenspace of $X \otimes X$ orthogonal to $\Pi_{\pm} \otimes P_{\mp}$ (also of dimension $d_A^2/4$), and arbitrary rank- k_1 and $r - k_1$ projectors Π_{++} and Π_{+-} . This is possible as long as $k_2 \leq d_A^2/4$, $d - r - k_2 \leq d_A^2/4$, $k_1 \leq d_A^2/4$ and $r - k_1 \leq s_A^2/4$. Substituting our choice of r , k_1 and k_2 , we find that it suffices to take $\lceil d/4 \rceil \leq d_A^2/4$. \square

Corollary 7 shows that, for suitable dimensions, a subspace chosen at random subject to the symmetry and orthogonality constraints of Eqs. (12c), (12d) and (12g) from Theorem 2 will, with probability 1, satisfy the strong unextendibility conditions of Eqs. (12a) and (12b). But Theorem 9 shows that there is a non-zero probability that such a random subspace will satisfy the positivity conditions of Eqs. (12e) and (12f). Therefore, for suitable dimensions, there must exist at least one subspace S satisfying all the conditions of Theorem 2. Hence, by that theorem, there exists a pair of channels $\mathcal{E}_{1,2}$ with $C_0(\mathcal{E}_{1,2}) = 0$ but $Q_0(\mathcal{E}_1 \otimes \mathcal{E}_2) \geq 1$.

Satisfying all the dimension requirements of Corollary 7 and Theorem 9 imposes constraints on the channel input and output dimensions d_A and d_B , and number of Kraus operators d_E (which corresponds to the subspace dimension d). Together, these constraints impose $d_A \geq 48$ and $d_E \geq 12(2d_A - 1)$, giving our main result:

Theorem 10 *Let $d_A = 48$, $d_E = 12(2d_A - 1) = 1140$ and $d_B = d_A d_E = 54720$. Then there exist channels $\mathcal{E}_1, \mathcal{E}_2$ such that:*

- *Each channel $\mathcal{E}_{1,2}$ maps \mathbb{C}^{d_A} to \mathbb{C}^{d_B} and has d_E Kraus operators.*
- *Each channel $\mathcal{E}_{1,2}$ has no classical zero-error capacity (hence no quantum zero-error capacity either).*
- *The joint channel $\mathcal{E}_1 \otimes \mathcal{E}_2$ has positive quantum zero-error capacity (hence all other capacities are non-zero).*

(This trivially implies that there exist channels with similar properties in all dimensions larger than these, too.)

5 Conclusions

There has been a recent surge of progress in the theory of quantum channels, especially their capacities. We now know that two uses of a quantum channel can sometimes, by using entangled signal states, transmit more than twice as much classical information as a single use [11]. This makes it (almost!) inevitable that any expression for the classical capacity will require regularisation, implying that it cannot be computed in general. We have known for some time that this is also the case for the quantum capacity [12], but we now also know that the quantum capacity itself is non-additive. Indeed, it exhibits the particularly extreme form of non-additivity known as superactivation [4]. This implies that the amount of quantum information that can be sent through a channel depends on what other channels are also available. Understanding these additivity violations is now a key goal of quantum information theory.

Both manifestations of non-additivity—regularisation and non-additive capacity—are already displayed by the *zero-error* capacity of *classical* channels [1, 13, 14], though superactivation remains impossible even in the zero-error setting. Zero-error capacities have been the subject of intense study in the classical information theory literature for over half a century. They are therefore an interesting area in which to probe *quantum* channel capacities, and attempt to understand non-additivity phenomena. Non-additivity in the purely classical setting obviously has nothing to do with entanglement. But quantum channels display even stronger non-additivity than their classical counterparts: in the quantum world, the presence of entanglement *does* lead to superactivation of the classical zero-error capacity of quantum channels [5].

The usual classical and quantum capacities are not at all closely related. There is no reason to expect that channels displaying additivity violations for the quantum capacity will possess any interesting additivity properties for the classical capacities, or vice versa. As a consequence, the recent non-additivity results for the usual capacities [4, 11] required very different mathematical techniques for the two cases.

However, in the zero-error setting, this work shows a striking non-additivity phenomenon that connects the classical and quantum capacities. We have proven the existence of pairs of channels that, individually, can not communicate *any* information with zero error, even classical information. But, when used together, even a single use of the joint channel suffices to communicate *all* forms of information, quantum and classical. These channels

therefore exhibit the most extreme possible form of additivity violation; their zero-error capacities *simultaneously* violate additivity for both classical and quantum information, and in the most extreme way (superactivation) to boot. This super-duper-activation is trivially impossible for classical channels, or for the usual capacities of quantum channels. Zero-error communication therefore provides a compelling setting in which to explore non-additivity phenomena in quantum information theory.

Acknowledgements

TSC would like to thank Nilanjana Datta and Francesco Buscemi for stimulating discussions about these ideas, and the physics of information group at IBM T. J. Watson Research Center for their hospitality during the visit in which this work was carried out. GS was supported by DARPA QUEST contract HR0011-09-C-0047. TSC is supported by a Leverhulme early-career fellowship, and through the integrated EC project “QAP” (contract no. IST-2005-15848).

References

- [1] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Trans. Inform. Theory*, IT-2:8, 1956.
- [2] J. Körner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Inform. Theory*, 44(6):2207, 1998.
- [3] R. A. C. Medeiros and F. M. de Assis. Quantum zero-error capacity. *Int. J. Quant. Inf.*, 3:135, 2005.
- [4] G. Smith and J. Yard. Quantum communication with zero-capacity channels. *Science*, 321:1812, 2008. (arXiv:0807.4935 [quant-ph]).
- [5] Toby S. Cubitt, Jianxin Chen, and Aram W. Harrow. Superactivation of the asymptotic zero-error classical capacity of a quantum channel. arXiv:0906.2547.
- [6] R. Duan. Superactivation of zero-error capacity of noisy quantum channels. arXiv:0906.2527 [quant-ph], 2009.
- [7] Joe Harris. *Algebraic Geometry*. Springer-Verlag, 1992.

- [8] H. Barnum and E. Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.*, 43(5):2097–2106, 2002.
- [9] Runyao Duan, Jianxin Chen, and Yu Xin. Unambiguous and zero-error classical capacity of noisy quantum channels. (Manuscript in preparation).
- [10] R. Bhat. A completely entangled subspace of maximal dimension. *Int. J. Quant. Inf.*, 4(2):325, 2006.
- [11] M. B. Hastings. A counterexample to additivity of minimum output entropy. *Nature Physics*, 5, 2009. (arXiv:0809.3972 [quant-ph]).
- [12] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin. Quantum channel capacity of very noisy channels. *Phys. Rev. A*, 57:830, 1998. (arXiv:quant-ph/9706061).
- [13] W. Haemers. On some problems of lovasz concerning the shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25:231–232, 1979.
- [14] N. Alon. The shannon capacity of a union. *Combinatorica*, 18(3):301–310, 1998.