Coding Theorem for a Class of Quantum Channels with Long-Term Memory

Nilanjana Datta
Statistical Laboratory
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road, Cambridge CB30WB
email: n.datta@statslab.cam.ac.uk

Tony C. Dorlas
Dublin Institute for Advanced Studies
School of Theoretical Physics
10 Burlington Road, Dublin 4, Ireland.
email: dorlas@stp.dias.ie

Keywords: quantum channels with long-term memory, classical capacity, Feinstein's Fundamental Lemma, Helstrom's Theorem.

Abstract

In this paper we consider the transmission of classical information through a class of quantum channels with long-term memory, which are given by convex combinations of product channels. Hence, the memory of such channels is given by a Markov chain which is aperiodic but not irreducible. We prove the coding theorem and weak converse for this class of channels. The main techniques that we employ, are a quantum version of Feinstein's Fundamental Lemma [6, 11] and a generalization of Helstrom's Theorem. [8].

1 Introduction

The biggest hurdle in the path of efficient information transmission is the presence of noise, in both classical and quantum channels. This noise causes a distortion of the information sent through the channel. Error–correcting codes are used to overcome this problem. Instead of transmitting the original messages, they are encoded into codewords, which are then sent through the channel. Information transmission is said to be reliable if the probability of error, in decoding the output of the channel, vanishes asymptotically in the number of uses of the channel (see e.g. [4] and [14]). The aim is to achieve reliable transmission, whilst optimizing the rate, i.e., the ratio between the size of the message and its correponding codeword. The optimal rate of reliable transmission is referred to as the capacity of the the channel.

Shannon, in his Noisy Channel Coding Theorem [19], obtained an explicit expression for the channel capacity of discrete, memoryless[1], classical channels. The first rigorous proof of this fundamental theorem was provided by Feinstein [6]. He used a packing argument (see e.g.[11]) to find a lower bound to the maximal number of codewords that can be sent through the channel reliably, i.e., with an arbitrarily low probability of error. More precisely, he proved that for any given $\delta > 0$, and sufficiently large number, n, of uses of a memoryless classical channel, the lower bound to the maximal number, N_n, of codewords that can be transmitted through the channel reliably, is given by

$$N_n \geq 2^{n(H(X:Y)-\delta)}.$$

Here $H(X:Y)$ is the mutual information of the random variables X and Y, corresponding to the input and the output of the channel, respectively. We refer to this result as *Feinstein's Fundamental Lemma*, following Khinchin [11]. It implies that for a real number $R < C$, where $C = \max H(X:Y)$, (the maximum being taken over all possible input distributions), $M_n \leq 2^{nR}$ classical messages can be transmitted through the channel reliably. In other words, any rate $R < C$ is *achievable*.

For real world communication channels, the assumption that noise is uncorrelated between successive uses of a channel cannot be justified. Hence memory effects need to be taken into account. This leads us to the consideration of quantum channels with memory. The first model of such a channel was studied by Macchiavello and Palma [13]. They showed that the transmission of classical information through two successive uses of a quantum depolarising channel, with Markovian correlated noise, is enhanced by using

[1]For such a channel, the noise affecting successive input states, is assumed to be perfectly uncorrelated.

inputs entangled over the two uses. An important class of quantum channels with memory consists of the so-called *forgetful channels*. The channel studied in [13] falls in this class. Roughly speaking, a forgetful channel is one for which the output after a large number of successive uses, does not depend on the initial input state. Forgetful channels have been studied by Bowen and Mancini [3] and more recently by Kretschmann and Werner [12]. In [12], coding theorems for arbitrary forgetful channels were proved. The proof of the direct channel coding theorem for a class of quantum channels with Markovian correlated noise, where the underlying Markov Chain was aperiodic and irreducible, was sketched out in [5]. Very recently Bjelaković and Bolche [2] have proved a coding theorem for causal ergodic classical-quantum channels with decaying input memory.

The capacities of channels with long-term memory (i.e., channels which are "not forgetful"), had remained an open problem to date. In this paper we evaluate the classical capacity of a class of quantum channels with long-term memory. The tool that we develop to prove the relevant coding theorem, can be considered to be a quantum analogue of Feinstein's Fundamental Lemma [5]. For a quantum memoryless channel, our method yields an alternative proof of the Holevo-Schumacher-Westmoreland (HSW) Theorem [10, 18], similar in spirit to the proof in [20].

We start the main body of our paper with some preliminaries in Section 2. Our main result is stated in Section 3. For clarity of exposition, we follow this with a proof of the quantum analogue of Feinstein's Fundamental Lemma for memoryless channels in Section 4. The proof of our main result, for a class of quantum channels with long-term memory, is given in Section 5.

In summary, in this paper we consider the transmission of classical information through a class of quantum channels with long-term memory, which are convex combinations of product channels (defined through (5) of Section 3). The memory of the channel is given by a Markov chain which is aperiodic but not irreducible. We prove the coding theorem and weak converse for this class of channels. The main techniques that we employ are a quantum version of Feinstein's Fundamental Lemma [6, 11] and a generalization of Helstrom's Theorem [8]. Our results can be extended to quantum channels with arbitrary Markovian correlated noise. The proofs in this case are technically more involved and will be presented in a subsequent paper.

2 Preliminaries

Let $\mathcal{B}(\mathcal{H})$ denote the algebra of linear operators acting on a finite–dimensional Hilbert space $\mathcal{H}$. The von Neumann entropy of a state ρ, i.e., a positive operator of unit trace in $\mathcal{B}(\mathcal{H})$, is defined as $S(\rho) = -\mathrm{Tr}\,\rho\log\rho$, where the logarithm is taken to base 2. A quantum channel is given by a completely positive trace–preserving (CPT) map $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$, where $\mathcal{H}$ and $\mathcal{K}$ are the input and output Hilbert spaces of the channel. Let $\dim \mathcal{H} = d$ and $\dim \mathcal{K} = d'$. For any ensemble $\{p_j, \rho_j\}$ of states ρ_j and probability distributions $\{p_j\}$, the Holevo χ quantity is defined as

$$\chi(\{p_j, \rho_j\}) := S\left(\sum_j p_j\,\rho_j\right) - \sum_j p_j\,S(\rho_j). \tag{1}$$

The Holevo capacity of a quantum channel Φ is given by

$$\chi^*(\Phi) := \max_{\{p_j,\rho_j\}} \chi(\{p_j, \Phi(\rho_j)\}), \tag{2}$$

where the maximum is taken over all ensembles $\{p_j, \rho_j\}$ of possible input states $\rho_j \in \mathcal{B}(\mathcal{H})$ occurring with probabilities p_j. It is known that the maximum in (2) can be achieved by using an ensemble of pure states, and that it suffices to restrict the maximum to ensembles of at most d^2 pure states.

Let us consider the transmission of classical information through successive uses of a quantum channel Φ. Let N uses of the channel be denoted by $\Phi^{(n)}$. Suppose Alice has a set of messages, labelled by the elements of the set $\mathcal{M}_n = \{1, 2, \ldots, M_n\}$, which she would like to communicate to Bob, using the quantum channel Φ. To do this, she encodes each message into a quantum state of a physical system with Hilbert space $\mathcal{H}^{\otimes n}$, which she then sends to Bob through n uses of the quantum channel. In order to infer the message that Alice communicated to him, Bob makes a measurement (described by POVM elements) on the state that he receives. The encoding and decoding operations, employed to achieve reliable transmission of information through the channel, together define a quantum error correcting code (QECC). More precisely, a code $\mathcal{C}^{(n)}$ of size N_n is given by a sequence $\{\rho_i^{(n)}, E_i^{(n)}\}_{i=1}^{N_n}$ where each $\rho_i^{(n)}$ is a state in $\mathcal{B}(\mathcal{H}^{\otimes n})$ and each $E_i^{(n)}$ is a positive operator acting in $\mathcal{K}^{\otimes n}$, such that $\sum_{i=1}^{N_n} E_i^{(n)} \leq I_n$. Here I_n denotes the identity operator in $\mathcal{B}(\mathcal{K}^{\otimes n})$. Defining $E_n^0 = I_n - \sum_{i=1}^{N_n} E_i^{(n)}$, yields a resolution of identity in $\mathcal{K}^{\otimes n}$. Hence, $\{E_i^{(n)}\}_{i=0}^{N_n}$ defines a POVM. An output $i \geq 1$ would lead to the inference that the state (or codeword) $\rho_i^{(n)}$ was transmitted through the channel $\Phi^{(n)}$, whereas the output 0 is interpreted as a failure of any inference. The

average probability of error for the code $\mathcal{C}^{(n)}$ is given by

$$P_e(\mathcal{C}^{(n)}) := \frac{1}{N_n}\sum_{i=1}^{N_n}\left(1 - \mathrm{Tr}\left(\Phi^{(n)}(\rho_i^{(n)})E_i^{(n)}\right)\right), \tag{3}$$

If there exists an $N \in \mathbf{N}$ such that for all $n \geq N$, there exists a sequence of codes $\{\mathcal{C}^{(n)}\}_{n=1}^{\infty}$, of sizes $N_n \geq 2^{nR}$, for which $P_e(\mathcal{C}^{(n)}) \to 0$ as $n \to \infty$, then R is said to be *achievable* rate.

The capacity of Φ is defined as

$$C(\Phi) := \sup R, \tag{4}$$

where R is an achievable rate. If the codewords $\rho_i^{(n)}$, $i = 1, 2, \ldots, N_n$, are restricted to product states in $\mathcal{B}(\mathcal{H}^{\otimes n})$, the capacity $C(\Phi)$ is referred to as the *product state capacity*.

3 Main Result

In this paper we study a class of channels with long-term memory. For a channel Φ in this class, $\Phi^{(n)} : \mathcal{B}(\mathcal{H}^{\otimes n}) \to \mathcal{B}(\mathcal{K}^{\otimes n})$ and the action of $\Phi^{(n)}$ on any state $\rho^{(n)} \in \mathcal{B}(\mathcal{H}^{\otimes n})$ is given as follows:

$$\Phi^{(n)}(\rho^{(n)}) = \sum_{i=1}^{M}\gamma_i\Phi_i^{\otimes n}(\rho^{(n)}), \tag{5}$$

where $\Phi_i : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$, $(i = 1, \ldots, M)$ are CPT maps and $\gamma_i > 0$, $\sum_{i=1}^{M}\gamma_i = 1$. Notice that this is an example of a quantum channel with memory given by a Markov chain, which is aperiodic but not irreducible [15].

Our main result is given by the following theorem.

Theorem 3.1 *The product state capacity of a channel Φ, with long-term memory, defined through (5), is given by*

$$C(\Phi) = \sup_{\{p_j,\rho_j\}}\left[\bigwedge_{i=1}^{M}\chi_i(\{p_j,\rho_j\})\right],$$

where $\chi_i(\{p_j,\rho_j\}) := \chi\left(\{p_j,\Phi_i(\rho_j)\}\right)$. The supremum is taken over all finite ensembles of states $\rho_j \in \mathcal{B}(\mathcal{H})$ with probabilities p_j.

Here we use the standard notation $\bigwedge$ to denote the minimum.

The product state capacity can be generalized to give the classical capacity of the channel Φ in the usual manner, that is, by considering inputs

which are product states over uses of blocks of n channels, but which may be entangled across different uses within the same block. The classical capacity $C_{\text{classical}}(\Phi)$ is obtained in the limit $n \to \infty$ and is given by

$$C_{\text{classical}}(\Phi) = \lim_{n\to\infty} \frac{1}{n} C(\Phi^{(n)}). \tag{6}$$

4 Analogue of Feinstein's Fundamental Lemma for a Memoryless Quantum Channel

In this section we prove an analogue of Feinstein's Fundamental Lemma [6] for a memoryless quantum channel Φ. This is given by Theorem 4.1 below. It provides an upper bound to the maximal number of codewords that can be sent reliably through Φ.

The proof of our main result, Theorem 3.1, employs a theorem which is a generalization of Theorem 4.1.

Theorem 4.1 *Let $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ be a memoryless quantum channel. Given $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ there exist at least $N_n \geq 2^{n(\chi^*(\Phi)-\epsilon)}$ product states $\tilde{\rho}_1^{(n)}, \ldots, \tilde{\rho}_{N_n}^{(n)} \in \mathcal{B}(\mathcal{H}^{\otimes n})$ and positive operators $E_1^{(n)}, \ldots, E_{N_n}^{(n)} \in \mathcal{B}(\mathcal{K}^{\otimes n})$ such that $\sum_{k=1}^{N_n} E_k^{(n)} \leq I_n$ and*

$$\text{Tr}\left[\Phi^{\otimes n}\left(\tilde{\rho}_k^{(n)}\right) E_k^{(n)}\right] > 1 - \epsilon, \tag{7}$$

for each k.

Here $\chi^*(\Phi)$ is the Holevo capacity (2) of the memoryless quantum channel Φ.

Before giving the proof of Theorem 4.1, let us briefly sketch the idea behind it. The proof employs the idea of construction of a maximal code. For a given $\epsilon > 0$, starting with an empty code, the proof gives a prescription for successively adding codewords $\rho_j^{(n)}$ and corresponding POVM elements $E_j^{(n)}$, $j = 1, 2, \ldots$, such that

$$\varepsilon_j^{(n)} := 1 - \text{Tr}\, \Phi^{(n)}(\rho_j^{(n)}) \leq \epsilon \tag{8}$$

Note that $\varepsilon_j^{(n)}$ is the probability of error in inferring the j^{th} codeword. This is done until no more codewords can be added without violating the condition (8). The resulting code is maximal. Let the size of this code be N_n. The proof ensures that the number N_n is large and provides a lower bound for it in terms of the Holevo capacity $\chi^*(\Phi)$.

Proof. Let the maximum in (2) be attained for an ensemble $\{p_j, \rho_j\}_{j=1}^J$. Denote $\sigma_j = \Phi(\rho_j)$, $\bar{\sigma} = \sum_{j=1}^J p_j \Phi(\rho_j)$ and $\bar{\sigma}_n = \bar{\sigma}^{\otimes n}$. Since $\bar{\sigma}_n$ is a product state, its eigenvalues and eigenvectors can be labelled by sequences $\underline{k} = (k_1, \ldots, k_n) \in J^n$.

Choose $\delta > 0$. We will relate δ to ϵ at a later stage. There exists $n_1 \in \mathbb{N}$ such that for $n \geq n_1$, there is a typical subspace $\overline{T}_\epsilon^{(n)}$ of $\mathcal{K}^{\otimes n}$, with projection $\bar{P}_n$ such that if $\bar{\sigma}_n$ has a spectral decomposition

$$\bar{\sigma}_n = \sum_{\underline{k}} \bar{\lambda}_{\underline{k}}^{(n)} |\psi_{\underline{k}}^{(n)}\rangle\langle\psi_{\underline{k}}^{(n)}| \tag{9}$$

then

$$\left| \frac{1}{n} \log \bar{\lambda}_{\underline{k}}^{(n)} + S(\bar{\sigma}) \right| < \frac{\epsilon}{3} \tag{10}$$

for all $\underline{k}$ such that $|\psi_{\underline{k}}^{(n)}\rangle \in \overline{T}_\epsilon^{(n)}$ and

$$\mathrm{Tr}\,(\bar{P}_n \bar{\sigma}_n) > 1 - \delta^2. \tag{11}$$

Further define

$$\bar{S} = \sum_{j=1}^J p_j \, S(\sigma_j). \tag{12}$$

Lemma 4.1 *Given a sequence $\underline{j} = (j_1, \ldots, j_n) \in J^n$, let $P_{\underline{j}}^{(n)}$ be the projection onto the subspace of $\mathcal{K}^{\otimes n}$ spanned by the eigenvectors of $\sigma_{\underline{j}}^{(n)} = \sigma_{j_1} \otimes \ldots \otimes \sigma_{j_n}$ with eigenvalues $\lambda_{\underline{j},\underline{k}}^{(n)} = \prod_{i=1}^n \lambda_{j_i,k_i}$ such that*

$$\left| \frac{1}{n} \log \lambda_{\underline{j},\underline{k}}^{(n)} + \bar{S} \right| < \frac{\epsilon}{3}. \tag{13}$$

For any $\delta > 0$ there exists $n_2 \in \mathbb{N}$ such that for $n \geq n_2$,

$$\mathbb{E}\left(\mathrm{Tr}\, \left(\sigma_{\underline{j}}^{(n)} P_{\underline{j}}^{(n)} \right) \right) > 1 - \delta^2. \tag{14}$$

Proof. Define i.i.d. random variables $X_1, \ldots, X_n$ with distribution given by

$$\mathbb{P}(X_i = \lambda_{j,k}) = p_j \, \lambda_{j,k}, \tag{15}$$

where $\lambda_{j,k}$, $k = 1, 2, \ldots, d'$ are the eigenvalues of σ_j. By the Weak Law of Large Numbers,

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^n \log X_i \to \mathbb{E}(\log X_i) &= \sum_{j=1}^J \sum_{k=1}^{d'} p_j \, \lambda_{j,k} \log \lambda_{j,k} \\ &= -\sum_{j=1}^J p_j \, S(\sigma_j) = -\bar{S}. \end{aligned} \tag{16}$$

It follows that there exists n_2 such that for $n \geq n_2$, the typical set $T_\epsilon^{(n)}$ of sequences of pairs $((j_1,k_1),\ldots,(j_n,k_n))$ such that

$$\left|\frac{1}{n}\sum_{i=1}^{n}\log\lambda_{j_i,k_i}+\bar{S}\right|<\frac{\epsilon}{3} \tag{17}$$

satisfies

$$\mathbb{P}\left(T_\epsilon^{(n)}\right)=\sum_{((j_1,k_1),\ldots,(j_n,k_n))\in T_\epsilon^{(n)}}\prod_{i=1}^{n}p_{j_i}\lambda_{j_i,k_i}>1-\delta^2. \tag{18}$$

Obviously,

$$P_{\underline{j}}^{(n)}\geq\sum_{((j_1,k_1),\ldots,(j_n,k_n))\in T_\epsilon^{(n)}}|\psi_{\underline{j},\underline{k}}^{(n)}\rangle\langle\psi_{\underline{j},\underline{k}}^{(n)}| \tag{19}$$

and

$$\mathbb{E}\left(\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}P_{\underline{j}}^{(n)}\right)\right)\geq\mathbb{P}\left(T_{\delta,\epsilon}^{(n)}\right)>1-\delta^2. \tag{20}$$

□

Continuing the proof of the theorem, let N_n be the maximal number N for which there exist product states $\tilde{\rho}_1^{(n)},\ldots,\tilde{\rho}_N^{(n)}$ on $\mathcal{H}^{\otimes n}$ and positive operators $E_1^{(n)},\ldots,E_N^{(n)}$ on $\mathcal{K}^{\otimes n}$ such that

(i) $\sum_{k=1}^{N_n}E_k^{(n)}\leq\bar{P}_n$ and

(ii) $\mathrm{Tr}\,[\,\tilde{\sigma}_k^{(n)}E_k^{(n)}]>1-\epsilon$ and

(iii) $\mathrm{Tr}\,[\,\bar{\sigma}_nE_k^{(n)}]\leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]}$.

Here $\tilde{\sigma}_k^{(n)}=\Phi^{\otimes n}(\tilde{\rho}_k^{(n)})$.

For any given $\underline{j}\in J^n$ define

$$V_{\underline{j}}^{(n)}=\left(\bar{P}_n-\sum_{k=1}^{N_n}E_k^{(n)}\right)^{1/2}\bar{P}_nP_{\underline{j}}^{(n)}\bar{P}_n\left(\bar{P}_n-\sum_{k=1}^{N_n}E_k^{(n)}\right)^{1/2}. \tag{21}$$

Clearly, $V_{\underline{j}}^{(n)}\leq\bar{P}_n-\sum_{k=1}^{N_n}E_k^{(n)}$, and we also have:

Lemma 4.2

$$\mathrm{Tr}\,(\bar{\sigma}_nV_{\underline{j}}^{(n)})\leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]}. \tag{22}$$

Proof. Put $Q_n = \sum_{k=1}^{N_n} E_k$. Note that Q_n commutes with $\bar{P}_n$. Using the fact that $\bar{P}_n \bar{\sigma}_n \bar{P}_n \leq 2^{-n[S(\bar{\sigma})-\frac{1}{3}\epsilon]}$ by (10), we have

$$\begin{aligned}
\mathrm{Tr}\,(\bar{\sigma}_n V_{\underline{j}}^{(n)}) &= \mathrm{Tr}\left[\bar{\sigma}_n(\bar{P}_n - Q_n)^{1/2}\bar{P}_n P_{\underline{j}}^{(n)}\bar{P}_n(\bar{P}_n - Q_n)^{1/2}\right] \\
&= \mathrm{Tr}\left[\bar{P}_n\bar{\sigma}_n\bar{P}_n(\bar{P}_n - Q_n)^{1/2}P_{\underline{j}}^{(n)}(\bar{P}_n - Q_n)^{1/2}\right] \\
&\leq 2^{-n[S(\bar{\sigma})-\frac{1}{3}\epsilon]}\mathrm{Tr}\left[(\bar{P}_n - Q_n)^{1/2}P_{\underline{j}}^{(n)}(\bar{P}_n - Q_n)^{1/2}\right] \\
&\leq 2^{-n[S(\bar{\sigma})-\frac{1}{3}\epsilon]}\mathrm{Tr}\,(P_{\underline{j}}^{(n)}) \leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]}, \qquad (23)
\end{aligned}$$

where, in the last inequality, we used the standard upper bound on the dimension of the typical subspace: $\mathrm{Tr}\,(P_{\underline{j}}^{(n)}) \leq 2^{n[\bar{S}+\frac{1}{3}\epsilon]}$, which follows from Lemma 4.1. □

Since N_n is maximal, it now follows that

$$\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}V_{\underline{j}}^{(n)}\right) \leq 1-\epsilon. \qquad (24)$$

and hence

Corollary 4.1

$$\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}V_{\underline{j}}^{(n)}\right]\right) < 1-\epsilon. \qquad (25)$$

Lemma 4.3 *For all $\eta > 0$, there exists $n_3 \in \mathbb{N}$ such that for all $n \geq n_3$,*

$$\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}\bar{P}_n P_{\underline{j}}^{(n)}\bar{P}_n\right]\right) > 1-\eta. \qquad (26)$$

Proof. We write

$$\begin{aligned}
\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}\bar{P}_n P_{\underline{j}}^{(n)}\bar{P}_n\right]\right) &= \mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}P_{\underline{j}}^{(n)}\right]\right) - \mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}(I_n-\bar{P}_n)P_{\underline{j}}^{(n)}\right]\right) \\
&\quad -\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}\bar{P}_n P_{\underline{j}}^{(n)}(I_n-\bar{P}_n)\right]\right). \qquad (27)
\end{aligned}$$

By Lemma 4.1, the first term is $> 1-\delta^2$ provided $n \geq n_2$. The last two terms can be bounded using the Cauchy-Schwarz inequality as follows:

$$\begin{aligned}
&\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}(I_n-\bar{P}_n)P_{\underline{j}}^{(n)}\right]\right) \\
&= \mathbb{E}\left(\mathrm{Tr}\,\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}(I_n-\bar{P}_n)P_{\underline{j}}^{(n)}\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right) \\
&\leq \left\{\mathbb{E}\left(\mathrm{Tr}\,\left[(I_n-\bar{P}_n)\sigma_{\underline{j}}^{(n)}(I_n-\bar{P}_n)\right]\right)\right\}^{1/2} \\
&\quad \times\left\{\mathbb{E}\left(\mathrm{Tr}\,\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}P_{\underline{j}}^{(n)}\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right)\right\}^{1/2}
\end{aligned}$$

$$
\begin{aligned}
&= \left\{\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}(I_n-\bar{P}_n)\right]\right)\right\}^{1/2}\left\{\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}P_{\underline{j}}^{(n)}\right]\right)\right\}^{1/2}\\
&\le \left\{\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}(I_n-\bar{P}_n)\right]\right)\right\}^{1/2}\\
&= \left(\mathrm{Tr}\,\left[\bar{\sigma}_n(I_n-\bar{P}_n)\right]\right)^{1/2}\le\delta \qquad (28)
\end{aligned}
$$

by (11) provided $n \ge n_1$. Analogously,

$$
\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}(I_n-\bar{P}_n)\right]\right)\le\delta. \qquad (29)
$$

Choosing $n_3 = n_1 \vee n_2$ and $\delta^2+2\delta<\eta$ the result follows. □

Lemma 4.4 *Assume $\eta < \frac{1}{3}\epsilon$. Then for $n \ge n_3$,*

$$
\mathrm{Tr}\,\left[\bar{\sigma}_n\sum_{k=1}^N E_k^{(n)}\right] = \mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{\underline{j}}^{(n)}\sum_{k=1}^N E_k^{(n)}\right]\right)\ge\eta^2. \qquad (30)
$$

Proof. Define

$$
Q_n' = \bar{P}_n - (\bar{P}_n - Q_n)^{1/2}. \qquad (31)
$$

By the above corollary,

$$
\begin{aligned}
1-\epsilon &\ge \mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}(\bar{P}_n-Q_n')P_{\underline{j}}^{(n)}(\bar{P}_n-Q_n')\right)\right\}\\
&= \mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}\bar{P}_n\right)\right\}\\
&\quad -\mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'P_{\underline{j}}^{(n)}\bar{P}_n\right)+\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}Q_n'\right)\right\}\\
&\quad +\mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'P_{\underline{j}}^{(n)}Q_n'\right)\right\}. \qquad (32)
\end{aligned}
$$

Since the last term is positive, we have, by Lemma 4.3,

$$
\mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'P_{\underline{j}}^{(n)}\bar{P}_n\right)+\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}Q_n'\right)\right\}\ge\epsilon-\eta>2\eta. \qquad (33)
$$

On the other hand, using Cauchy-Schwarz for each term, we have

$$
\begin{aligned}
&\mathbb{E}\left\{\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'P_{\underline{j}}^{(n)}\bar{P}_n\right)+\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}Q_n'\right)\right\}\\
&\le 2\left\{\mathbb{E}\left[\mathrm{Tr}\,\left(Q_n'\sigma_{\underline{j}}^{(n)}Q_n'\right)\right]\right\}^{1/2}\left\{\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}\bar{P}_nP_{\underline{j}}^{(n)}\bar{P}_n\right)\right]\right\}^{1/2}\\
&\le 2\left\{\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'^2\right)\right]\right\}^{1/2}. \qquad (34)
\end{aligned}
$$

Thus,

$$
\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{\underline{j}}^{(n)}Q_n'^2\right)\right]\ge\eta^2. \qquad (35)
$$

To complete the proof, we now claim that

$$Q_n \geq (Q'_n)^2. \tag{36}$$

Indeed, on the domain of $\bar{P}_n$, (36) follows from the inequality $1-(1-x)^2 \geq x^2$ for $0 \leq x \leq 1$. □

To complete the proof of Theorem 4.1, we now have by assumption,

$$\text{Tr } \left[\bar{\sigma}_n E_k^{(n)}\right] \leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]} \tag{37}$$

for all $k = 1, \ldots, N_n$. On the other hand, choosing $\eta < \frac{1}{3}\epsilon$ and $\delta < \frac{1}{3}\eta$, we have by Lemma 4.4,

$$\text{Tr } \left[\bar{\sigma}_n \sum_{k=1}^{N_n} E_k^{(n)}\right] \geq \eta^2 \tag{38}$$

provided $n \geq n_3$. It follows that

$$N_n \geq \eta^2 2^{n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]} \geq 2^{n[S(\bar{\sigma})-\bar{S}-\epsilon]} \tag{39}$$

for $n \geq n_3$ and $n \geq -\frac{6}{\epsilon}\log\eta$. □

5 A class of channels with long-term memory

We now consider the class of quantum channels with long-term memory, mentioned in the Introduction:

$$\Phi^{(n)}(\rho^{(n)}) = \sum_{i=1}^{M} \gamma_i \Phi_i^{\otimes n}(\rho^{(n)}), \tag{40}$$

where $\Phi_i : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$, $(i = 1, \ldots, M)$ are CPT maps and $\gamma_i > 0$, $\sum_{i=1}^{M} \gamma_i = 1$.

For an ensemble of states $\{p_j, \rho_j\}$ where $\rho_j \in \mathcal{B}(\mathcal{H})$, define

$$\widehat{\chi}(\{p_j, \rho_j\}) := \bigwedge_{i=1}^{M} \chi_i(\{p_j, \rho_j\}), \tag{41}$$

where $\chi_i(\{p_j, \rho_j\}) = \chi\left(\{p_j, \Phi_i(\rho_j)\}\right)$.

5.1 Proof of the direct part of Theorem 3.1

To prove the direct part of Theorem 3.1, i.e., the fact that a rate $R < C(\Phi)$ is achievable, we employ the quantum analogue of Feinstein's Fundamental Lemma for the class of channels defined by (40). This analogue is given by the following theorem, which we prove in Section 5.1.1

Theorem 5.1 *Given $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ there exist at least $N_n \geq 2^{n(C(\Phi)-\epsilon)}$ product states $\rho_1^{(n)}, \ldots, \rho_N^{(n)} \in \mathcal{B}(\mathcal{H}^{\otimes n})$ and positive operators $E_1^{(n)}, \ldots, E_{N_n}^{(n)} \in \mathcal{B}(\mathcal{K}^{\otimes n})$ such that $\sum_{k=1}^{N_n} E_k^{(n)} \leq I_n$ and such that for each $k = 1, \ldots, N_n$,*

$$\mathrm{Tr}\left[\Phi^{(n)}\left(\rho_k^{(n)}\right) E_k^{(n)}\right] > 1 - \epsilon. \tag{42}$$

Here

$$C(\Phi) := \sup_{\{p_j, \rho_j\}} \left[\bigwedge_{i=1}^{M} \chi_i(\{p_j, \rho_j\})\right] = \sup_{\{p_j, \rho_j\}} \widehat{\chi}(\{p_j, \rho_j\}), \tag{43}$$

where the supremum is over all finite ensembles of states ρ_j with probabilities p_j.

The above theorem implies that a rate $R < C(\Phi)$ is achievable. This can be seen as follows: Given an $R < C(\Phi)$, choose $\epsilon > 0$ such that $R < C(\Phi) - \epsilon$. Then, Theorem 5.1 guarantees the existence of codes $\mathcal{C}^{(n)}$ of size

$$N_n \geq 2^{n(C(\Phi)-\epsilon)} \geq 2^{nR},$$

with codewords given by product states $\rho_j^{(n)}$, and POVM elements $E_j^{(n)}$, for which the probability of error, $\varepsilon_j^{(n)}$, can be made arbitrarily small, for each $j \in \{1, 2, \ldots, N_n\}$ and n large enough. Hence the rate R is acheivable.

5.1.1 Proof of Theorem 5.1

Choose an ensemble $\{p_j, \rho_j\}_{j=1}^{J}$ such that

$$C(\Phi) < \widehat{\chi}(\{p_j, \rho_j\}) + \frac{1}{4}\epsilon. \tag{44}$$

Define $\sigma_{i,j} = \Phi_i(\rho_j)$, $\sigma_{i,\underline{j}}^{(n)} = \otimes_{r=1}^{n} \sigma_{i,j_r}$, $\bar{\sigma}_i = \sum_{j=1}^{J} p_j \Phi_i(\rho_j) = \Phi_i(\bar{\rho})$, and $\bar{\sigma}_i^{(n)} = \bar{\sigma}_i^{\otimes n}$. Let $\bar{P}_i^{(n)}$, $i = 1, \ldots, M$, be the orthogonal projections onto the typical subspaces for the states $\bar{\sigma}_i^{(n)}$ so that, as above,

$$\mathrm{Tr}\,(\bar{P}_i^{(n)} \bar{\sigma}_i^{(n)}) > 1 - \delta^2 \tag{45}$$

for n large enough, and

$$\bar{P}_i^{(n)} \bar{\sigma}_i^{(n)} \bar{P}_i^{(n)} \leq 2^{-n[S(\bar{\sigma}_i) - \frac{1}{4}\epsilon]}. \tag{46}$$

By Lemma 4.1 there also exist typical subspaces with projections $P_{i,\underline{j}}^{(n)}$ for which

$$\mathbb{E}\left(\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} P_{i,\underline{j}}^{(n)}\right)\right) > 1 - \delta^2 \tag{47}$$

for n large enough.

To distinguish between the different memoryless branches, Φ_i, of the quantum channel Φ, we add a preamble to the input state encoding each message in the set $\mathcal{M}_n$. This is given by an m-fold tensor product of a suitable state (as described below). Let us first sketch the idea behind adding such a preamble. Helstrom [8] showed that two states σ_1 and σ_2, occurring with a priori probabilities γ_1 and γ_2 respectively, can be distinguished, with an asymptotically vanishing probability of error, if a suitable collective measurement is performed on the m-fold tensor products $\sigma_1^{\otimes m}$ and $\sigma_2^{\otimes m}$, for a large enough $m \in \mathbb{N}$. The optimal measurement is projection-valued. The relevant projection operators, which we denote by Π^+ and Π^-, are the orthogonal projections onto the positive and negative eigenspaces of the difference operator $A_m = \gamma_1\sigma_1^{\otimes n} - \gamma_2\sigma_2^{\otimes n}$. Here we generalize this result to distinguish between the different branches Φ_i. If the preamble is given by a state $\omega^{\otimes m}$, then, by using Helstrom's result, we can construct a POVM which distinguishes between the output states $\sigma_i^{\otimes n} := (\Phi_i(\omega))^{\otimes n}$ corresponding to the different branches Φ_i, $i = 1, 2, \ldots, M$. The outcome of this POVM measurement would in turn serve to determine which branch of the channel is being used for transmission.

Notice that we may assume that all branches Φ_i are different. Indeed, otherwise we do not need to distinguish them and can introduce a compound probability for each set of identical branches. This assumption means that there exist states $\omega_{i,j}$ on $\mathcal{H}$ for each pair $1 \leq i < j \leq M$ such that $\Phi_i(\omega_{i,j}) \neq \Phi_j(\omega_{i,j})$. Introducing the fidelity of two states as in [14],

$$F(\sigma, \sigma') = \mathrm{Tr}\,\sqrt{\sigma^{1/2}\sigma'\,\sigma^{1/2}}, \tag{48}$$

we then have

$$F(\Phi_i(\omega_{i,j}), \Phi_j(\omega_{i,j})) \leq f < 1 \tag{49}$$

for all pairs (i, j). We now introduce, for any $m \in \mathbb{N}$ and $1 \leq i < j \leq M$, the difference operators

$$A_{i,j}^{(m)} = \gamma_i(\Phi_i(\omega_{i,j}))^{\otimes m} - \gamma_j(\Phi_j(\omega_{i,j}))^{\otimes m}. \tag{50}$$

Let $\Pi_{i,j}^{\pm}$ be the orthogonal projections onto the eigenspaces of $A_{i,j}^{(m)}$ corresponding to all non-negative, and all negative eigenvalues, respectively.

Lemma 5.1 *Suppose that for a given $\delta > 0$,*

$$|\mathrm{Tr}\,[|A_{i,j}^{(m)}|] - (\gamma_i + \gamma_j)| \leq \delta. \tag{51}$$

Then

$$|\mathrm{Tr}\,[\Pi^+_{i,j}(\Phi_i(\omega_{i,j}))^{\otimes m}] - 1| \leq \frac{\delta}{2\gamma_i} \tag{52}$$

and

$$|\mathrm{Tr}\,[\Pi^-_{i,j}(\Phi_j(\omega_{i,j}))^{\otimes m}] - 1| \leq \frac{\delta}{2\gamma_j}. \tag{53}$$

Proof. Write $A = A^{(m)}_{i,j}$ and $\Pi^\pm = \Pi^\pm_{i,j}$. First note that

$$\begin{aligned} \mathrm{Tr}\,[\Pi^\pm A] &= \frac{1}{2}\mathrm{Tr}\,[A \pm (\Pi^+ - \Pi^-)A] \\ &= \frac{1}{2}\left(\mathrm{Tr}\,[A] \pm \mathrm{Tr}\,[|A|]\right) \\ &= \frac{1}{2}(\gamma_i - \gamma_j) \pm \frac{1}{2}\mathrm{Tr}\,[|A|] \end{aligned} \tag{54}$$

so that we have by the assumption

$$|\mathrm{Tr}\,[\Pi^+ A] - \gamma_i| \leq \frac{1}{2}\delta \tag{55}$$

and

$$|\mathrm{Tr}\,[\Pi^- A] + \gamma_j| \leq \frac{1}{2}\delta. \tag{56}$$

Now, writing $\sigma_i = (\Phi_i(\omega_{i,j}))^{\otimes m}$ and $\sigma_j = (\Phi_j(\omega_{i,j}))^{\otimes m}$ we have obviously, $\mathrm{Tr}\,[\Pi^-\sigma_i] \geq 0$, and on the other hand,

$$\gamma_i\mathrm{Tr}\,[\Pi^-\sigma_i] = \mathrm{Tr}\,[\Pi^- A] + \gamma_j\mathrm{Tr}\,[\Pi^-\sigma_j] \leq -\gamma_j + \frac{1}{2}\delta + \gamma_j = \frac{1}{2}\delta. \tag{57}$$

The first result thus follows from $\Pi^+ + \Pi^- = I_m$ and $\mathrm{Tr}\,\sigma_i = 1$. Similarly,

$$\gamma_j\mathrm{Tr}\,[\Pi^+\sigma_j] = -\mathrm{Tr}\,[\Pi^+ A] + \gamma_i\mathrm{Tr}\,[\Pi^+\sigma_i] \leq -\gamma_i + \frac{1}{2}\delta + \gamma_i = \frac{1}{2}\delta. \tag{58}$$

□

To compare the outputs of all the different branches of the channel, we define projections $\tilde{\Pi}_i$ on the tensor product space $\bigotimes_{1\leq i<j\leq M}\mathcal{K}^{\otimes m} = \mathcal{K}^{\otimes mL}$ with $L = \binom{M}{2}$ as follows:

$$\tilde{\Pi}_i = \bigotimes_{1\leq i_1<i_2\leq M} \Gamma^{(i)}_{i_1,i_2}, \text{ where } \Gamma^{(i)}_{i_1,i_2} = \begin{cases} I_m & \text{if} \quad i_1 \neq i \text{ and } i_2 \neq i \\ \Pi^-_{i_1,i} & \text{if} \quad i_2 = i \\ \Pi^+_{i,i_2} & \text{if} \quad i_1 = i. \end{cases} \tag{59}$$

Notice that it follows from the fact that $\Pi^+_{i,j}\Pi^-_{i,j} = 0$, that the projections $\tilde{\Pi}_i$ are also disjoint:

$$\tilde{\Pi}_i\tilde{\Pi}_j = 0 \quad \text{for } i \neq j. \tag{60}$$

Introducing the notation

$$\omega^{(mL)} = \bigotimes_{i_1<i_2} \omega_{i_1,i_2}^{\otimes m}, \tag{61}$$

we now have

Lemma 5.2 *For all $i = 1, \ldots, M$,*

$$\lim_{m\to\infty} \mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] = 1. \tag{62}$$

Proof. Notice that for all $i < j$,

$$F(\gamma_i\Phi_i(\omega_{i,j})^{\otimes m}, \gamma_j\Phi_j(\omega_{i,j})^{\otimes m}) = \sqrt{\gamma_i\gamma_j}F(\Phi_i(\omega_{i,j}), \Phi_i(\omega_{i,j}))^m < f^m. \tag{63}$$

Using the inequalities [14]

$$\mathrm{Tr}\,(A_1) + \mathrm{Tr}\,(A_2) - 2F(A_1, A_2) \leq ||A_1 - A_2||_1 \leq \mathrm{Tr}\,(A_1) + \mathrm{Tr}\,(A_2) \tag{64}$$

for any two positive operators A_1 and A_2, we find that

$$|\,\mathrm{Tr}\,\,(|A_{i,j}^{(m)}|) - (\gamma_i + \gamma_j)| \leq 2f^m, \tag{65}$$

since

$$\mathrm{Tr}\,\,(|A_{i,j}^{(m)}|) = ||\gamma_i\Phi_i(\omega_{i,j})^{\otimes m} - \gamma_j\Phi_j(\omega_{i,j})^{\otimes m}||_1. \tag{66}$$

Using Lemma 5.1 we then have

$$\begin{aligned} 1 \geq \mathrm{Tr}\,\left[\tilde{\Pi}_i\Phi_i^{\otimes mL}\left(\bigotimes_{i_1<i_2}\omega_{i_1,i_2}^{\otimes m}\right)\right] = \\ = \prod_{i_1<i}\mathrm{Tr}\,\left[\Pi^-_{i_1,i}(\Phi_i(\omega_{i_1,i}))^{\otimes m}\right]\prod_{i_2>i}\mathrm{Tr}\,\left[\Pi^+_{i,i_2}(\Phi_i(\omega_{i,i_2}))^{\otimes m}\right] \\ \geq \left(1 - \frac{f^m}{\gamma_i}\right)^{M-1}. \end{aligned} \tag{67}$$

□

We now fix m so large that

$$\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] > 1 - \delta \tag{68}$$

for all $i = 1, \ldots, M$. The product state $\omega^{(mL)}$, defined through (61) is used as a preamble to the input state encoding each message, and serves to distinguish between the different branches, Φ_i, $i = 1, 2, \ldots, M$, of the channel. If $\rho_k^{(n)} \in \mathcal{B}(\mathcal{H}^{\otimes n})$ is a product state encoding the k^{th} classical message in the set $\mathcal{M}_n$, then the k^{th} codeword is given by the product state

$$\omega^{(mL)} \otimes \rho_k^{(n)}.$$

Continuing with the proof of Theorem 5.1, let $N = \tilde{N}(n)$ be the maximal number of product states $\tilde{\rho}_1^{(n)}, \ldots, \tilde{\rho}_N^{(n)}$ on $\mathcal{H}^{\otimes n}$ (each of which is a tensor product of states in the maximising ensemble $\{p_j, \rho_j\}_{j=1}^J$) for which there exist positive operators $E_1^{(n)}, \ldots, E_N^{(n)}$ on $\mathcal{K}^{\otimes mL} \otimes \mathcal{K}^{\otimes n}$ such that

(i) $E_k^{(n)} = \sum_{i=1}^M \tilde{\Pi}_i \otimes E_{k,i}^{(n)}$ and $\sum_{k=1}^N E_{k,i}^{(n)} \leq \bar{P}_i^{(n)}$ and

(ii) $\sum_{i=1}^M \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathrm{Tr}\left[\Phi_i^{\otimes n}\left(\tilde{\rho}_k^{(n)}\right) E_{k,i}^{(n)}\right] > 1 - \epsilon$ and

(iii) $\sum_{i=1}^M \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathrm{Tr}\left[\left(\Phi_i(\bar{\rho})\right)^{\otimes n} E_{k,i}^{(n)}\right] \leq 2^{-n[C(\Phi) - \frac{1}{2}\epsilon]}$.

for $\bar{\rho} = \sum_{j=1}^J p_j \rho_j$. For each $i = 1, \ldots, M$ and $\underline{j} = (j_1, \ldots, j_n) \in J^n$, we define, as before

$$V_{i,\underline{j}}^{(n)} = \left(\bar{P}_i^{(n)} - \sum_{k=1}^N E_{k,i}^{(n)}\right)^{1/2} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} \left(\bar{P}_i^{(n)} - \sum_{k=1}^N E_{k,i}^{(n)}\right)^{1/2}. \tag{69}$$

Clearly $V_{i,\underline{j}}^{(n)} \leq \bar{P}_i^{(n)} - \sum_{k=1}^N E_{k,i}^{(n)}$. Put

$$V_{\underline{j}}^{(n)} := \sum_{i=1}^M \tilde{\Pi}_i \otimes V_{i,\underline{j}}^{(n)}. \tag{70}$$

This is a candidate for an additional measurement operator, $E_{N+1}^{(n)}$, for Bob with corresponding input state $\tilde{\rho}_{N+1}^{(n)} = \rho_{\underline{j}}^{(n)} = \rho_{j_1} \otimes \rho_{j_2} \ldots \otimes \rho_{j_n}$. Clearly, the condition (i), given above, is satisfied and we also have

Lemma 5.3

$$\sum_{i=1}^M \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathrm{Tr}\left[\bar{\sigma}_i^{(n)} V_{i,\underline{j}}^{(n)}\right] \leq 2^{-n[C(\Phi) - \frac{1}{2}\epsilon]}, \tag{71}$$

where $\bar{\sigma}_i^{(n)} = \left(\Phi_i(\bar{\rho})\right)^{\otimes n}$.

Proof. By Lemma 4.2, replacing $\frac{1}{3}\epsilon$ by $\frac{1}{4}\epsilon$ in the definition of the typical subspaces, we have,

$$\mathrm{Tr}\,(\bar{\sigma}_i^{(n)} V_{i,\underline{j}}^{(n)}) \leq 2^{-n[S(\bar{\sigma}_i)-\bar{S}_i-\frac{1}{2}\epsilon]} = 2^{-n[\chi_i-\frac{1}{2}\epsilon]}. \tag{72}$$

for n large enough. Then

$$\begin{aligned}
\sum_{i=1}^{M} \gamma_i \mathrm{Tr}\,[\tilde{\Pi}_i\, \Phi^{\otimes mL)}\left(\omega^{(mL)}\right)]\,\mathrm{Tr}\,[\bar{\sigma}_i^{(n)} V_{i,\underline{j}}^{(n)}] &\leq \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\,[\bar{\sigma}_i^{(n)} V_{\underline{j}}^{(n)}] \\
&\leq \sum_{i=1}^{M} \gamma_i\, 2^{-n[S(\bar{\sigma}_i)-\bar{S}_i-\frac{1}{2}\epsilon]} \\
&\leq 2^{-n[\widehat{\chi}(\Phi)-\frac{1}{2}\epsilon]}, \\
&\leq 2^{-n[C(\Phi)-\frac{3}{4}\epsilon]},
\end{aligned} \tag{73}$$

where we used the obvious fact that $\mathrm{Tr}\,[\tilde{\Pi}_i\, \Phi_i^{\otimes mL}(\omega_i^{(mL)})] \leq 1$. □

By maximality of N it now follows that the condition (ii) above cannot hold, that is,

$$\sum_{i=1}^{M} \gamma_i \mathrm{Tr}\,\left[\tilde{\Pi}_i \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathrm{Tr}\,\left[\Phi_i^{\otimes n}\left(\rho_{\underline{j}}^{(n)}\right) V_{i,\underline{j}}^{(n)}\right] \leq 1-\epsilon \tag{74}$$

for every $\underline{j}$, and this yields the following:

Corollary 5.1

$$\sum_{i=1}^{M} \gamma_i \mathrm{Tr}\,\left[\tilde{\Pi}_i\, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left(\mathrm{Tr}\,\left[\Phi_i^{\otimes n}\left(\rho_{\underline{j}}^{(n)}\right) V_{i,\underline{j}}^{(n)}\right]\right) \leq 1-\epsilon. \tag{75}$$

We also need the following lemma:

Lemma 5.4 *For all $\eta' > \delta^2 + 3\delta$,*

$$\sum_{i=1}^{M} \gamma_i\, \mathrm{Tr}\,\left[\tilde{\Pi}_i\, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathrm{Tr}\,\left[\sigma_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right] > 1-\eta' \tag{76}$$

if n is large enough.

Proof. Using Lemma 4.3 and (68), we have

$$\sum_{i=1}^{M} \gamma_i\, \mathrm{Tr}\,\left[\tilde{\Pi}_i\, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left(\mathrm{Tr}\,\left[\sigma_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right]\right) > (1-\delta)(1-\eta) \tag{77}$$

provided $\eta > \delta^2 + 2\delta$. Hence the result follows. □

Lemma 5.5 *Assume $\eta' < \frac{1}{3}\epsilon$ and write*

$$Q_i^{(n)} = \sum_{k=1}^{N} E_{k,i}^{(n)}. \tag{78}$$

Then for n large enough,

$$\sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left(\mathrm{Tr}\left[\Phi_i^{(n)}\left(\rho_{\underline{j}}^{(n)}\right) Q_i^{(n)}\right]\right) \geq \eta'^2. \tag{79}$$

Proof. This is analogous to Lemma 4.4. Define

$$Q_i^{(n)\prime} = \bar{P}_i^{(n)} - (\bar{P}_i^{(n)} - Q_i^{(n)})^{1/2}. \tag{80}$$

By the Corollary 5.1,

$$\begin{aligned}
1-\epsilon \;\geq\; & \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left(\mathrm{Tr}\left[\Phi_i^{\otimes n}\left(\rho_{\underline{j}}^{(n)}\right) V_{i,\underline{j}}^{(n)}\right]\right) \\
= \; & \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left\{\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right)\right\} \\
& - \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left\{\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} Q_i^{(n)\prime} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right)\right. \\
& \qquad \left. + \mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} Q_i^{(n)\prime}\right)\right\} \\
& + \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left\{\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} Q_i^{(n)\prime} P_{i,\underline{j}}^{(n)} Q_i^{(n)\prime}\right)\right\}.
\end{aligned} \tag{81}$$

Since the last term is positive, we have, by Lemma 5.4,

$$\begin{aligned}
& \sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left\{\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} Q_i^{(n)\prime} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right)\right. \\
& \qquad \left. + \mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)} P_{i,\underline{j}}^{(n)} Q_i^{(n)\prime}\right)\right\} \geq \epsilon - \eta' > 2\eta'.
\end{aligned} \tag{82}$$

On the other hand, using the Cauchy-Schwarz inequality for each term, we have

$$\sum_{i=1}^{M} \gamma_i \mathrm{Tr}\left[\tilde{\Pi}_i \, \Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right] \mathbb{E}\left\{\mathrm{Tr}\left(\sigma_{i,\underline{j}}^{(n)} Q_i^{(n)\prime} P_{i,\underline{j}}^{(n)} \bar{P}_i^{(n)}\right)\right.$$

$$+\mathrm{Tr}\,\left(\sigma_{i,\underline{j}}^{(n)}\bar{P}_i^{(n)}P_{i,\underline{j}}^{(n)}Q_i^{(n)\prime}\right)\Big\}\leq$$

$$\leq 2\left\{\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{i,\underline{j}}^{(n)}(Q_i^{(n)\prime})^2\right)\right]\right\}^{1/2}$$

$$\times\left\{\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{i,\underline{j}}^{(n)}\bar{P}_i^{(n)}P_{i,\underline{j}}^{(n)}\bar{P}_i^{(n)}\right)\right]\right\}^{1/2}$$

$$\leq 2\left\{\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{i,\underline{j}}^{(n)}(Q_i^{(n)\prime})^2\right)\right]\right\}^{1/2}. \quad (83)$$

Thus,

$$\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathbb{E}\left[\mathrm{Tr}\,\left(\sigma_{i,\underline{j}}^{(n)}(Q_i^{(n)\prime})^2\right)\right]\geq\eta'^2. \quad (84)$$

To complete the proof, we remark as before that

$$Q_n\geq(Q_n')^2. \quad (85)$$

□

It now follows, as before, that for n large enough, $\tilde{N}(n)\geq(\eta')^2\,2^{n[C(\Phi)-\frac{3}{4}\epsilon]}$. We take the following states as codewords:

$$\rho_k^{(mL+n)}=\omega^{(mL)}\otimes\tilde{\rho}_k^{(n)}. \quad (86)$$

For n sufficiently large we then have

$$N_{n+mL}=\tilde{N}(n)\geq(\eta')^2\,2^{n[C(\Phi)-\frac{3}{4}\epsilon]}\geq 2^{(mL+n)[C(\Phi)-\epsilon]}. \quad (87)$$

To complete the proof we need to show that the set $E_k^{(n)}$ satisfies (42). But this follows immediately from condition (ii):

$$\begin{aligned}
&\mathrm{Tr}\,\left[\Phi^{(mL+n)}\left(\rho_k^{(mL+n)}\right)E_k^{(n)}\right]=\\
&=\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\Phi_i^{\otimes(mL+n)}\left(\omega^{(mL)}\otimes\tilde{\rho}_k^{(n)}\right)E_k^{(n)}\right]\\
&=\sum_{i,j=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_j\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathrm{Tr}\,\left[\Phi_i^{\otimes n}(\tilde{\rho}_k^{(n)})E_{k,j}^{(n)}\right]\\
&\geq\sum_{i=1}^{M}\gamma_i\mathrm{Tr}\,\left[\tilde{\Pi}_i\,\Phi_i^{\otimes mL}\left(\omega^{(mL)}\right)\right]\,\mathrm{Tr}\,\left[\Phi_i^{\otimes n}(\tilde{\rho}_k^{(n)})E_{k,i}^{(n)}\right]>1-\epsilon. \quad (88)
\end{aligned}$$

□

5.2 Proof of the converse of Theorem 3.1

In this section we prove that it is impossible for Alice to transmit classical messages reliably to Bob through the channel Φ defined in (40) at a rate $R > C(\Phi)$. This is the weak converse of Theorem 3.1 in the sense that the probability of error does not tend to zero asymptotically as the length of the code increases, for any code with rate $R > C(\Phi)$. To prove the weak converse, suppose that Alice encodes messages labelled by $\alpha \in \mathcal{M}_n$ by product states $\rho_\alpha^{(n)} = \rho_{\alpha,1} \otimes \ldots \otimes \rho_{\alpha,n}$ in $\mathcal{B}(\mathcal{H}^{\otimes n})$. Let the corresponding outputs for the i-th branch of the channel be denoted by $\sigma_{\alpha,i}^{(n)}$, i.e.

$$\sigma_{\alpha,i}^{(n)} = \Phi_i^{\otimes n}(\rho_\alpha^{(n)}) = \sigma_{\alpha,1}^i \otimes \ldots \otimes \sigma_{\alpha,n}^i,\ \sigma_{\alpha,j}^i = \Phi_i(\rho_{\alpha,j}). \tag{89}$$

Further define

$$\bar{\sigma}_i^{(n)} = \frac{1}{|\mathcal{M}_n|} \sum_{\alpha \in \mathcal{M}_n} \sigma_{\alpha,i}^{(n)} \tag{90}$$

and

$$\bar{\sigma}_{i,j} = \frac{1}{|\mathcal{M}_n|} \sum_{\alpha \in \mathcal{M}_n} \sigma_{\alpha,j}^i\ . \tag{91}$$

Let Bob's POVM elements corresponding to the codewords $\rho_\alpha^{(n)}$ be denoted by $E_\alpha^{(n)}$, $\alpha = 1, \ldots, |\mathcal{M}_n|$. We may assume that Alice's messages are produced uniformly at random from the set $\mathcal{M}_n$. Then Bob's average probability of error is given by

$$\bar{p}_e^{(n)} := 1 - \frac{1}{|\mathcal{M}_n|} \sum_{\alpha \in \mathcal{M}_n} \text{Tr}\ \left[\Phi^{(n)}(\rho_k^{(n)}) E_k \alpha^{(n)}\right]. \tag{92}$$

We also define the average error corresponding to the i^{th} branch of the channel as

$$\bar{p}_{i,e}^{(n)} := 1 - \frac{1}{|\mathcal{M}_n|} \sum_{\alpha \in \mathcal{M}_n} \text{Tr}\ \left[\Phi_i^{\otimes n}(\rho_k^{(n)}) E_\alpha^{(n)}\right]. \tag{93}$$

so that

$$\bar{p}_e^{(n)} = \sum_{i=1}^{M} \gamma_i \bar{p}_{i,e}^{(n)}. \tag{94}$$

Let $X^{(n)}$ be a random variable with a uniform distribution over the set $\mathcal{M}_n$, characterizing the classical message sent by Alice to Bob. Let $Y_i^{(n)}$ be the random variable corresponding to Bob's inference of Alice's message, when the codeword is transmitted through the i^{th} branch of the channel. It is defined by the conditional probabilities

$$\mathbb{P}\left[Y_i^{(n)} = \beta \,|\, X^{(n)} = \alpha\right] = \text{Tr}\ [\Phi_i^{\otimes n}(\rho_\alpha^{(n)}) E_\beta^{(n)}]. \tag{95}$$

By Fano's inequality,

$$h(\bar{p}_{i,e}^{(n)}) + \bar{p}_{i,e}^{(n)} \log(|\mathcal{M}_n| - 1) \geq H(X^{(n)} \,|\, Y_i^{(n)}) = H(X^{(n)}) - H(X^{(n)} \,:\, Y_i^{(n)}). \tag{96}$$

Here $h(\cdot)$ denotes the binary entropy and $H(\cdot)$ denotes the Shannon entropy. Using the Holevo bound and the subadditivity of the von Neumann entropy we have

$$\begin{aligned}
H(X^{(n)}\,,:,Y_i^{(n)}) &\leq S\left(\frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n}\Phi_i^{\otimes n}(\rho_\alpha^{(n)})\right) - \frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n} S\left(\Phi_i^{\otimes n}(\rho_\alpha^{(n)})\right) \\
&= S\left(\frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n}\sigma_{\alpha,i}^{(n)}\right) - \frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n} S(\sigma_{\alpha_i}^{(n)}) \\
&\leq \sum_{j=1}^{n}\left[S\left(\bar{\sigma}_{i,j}\right) - \frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n} S\left(\sigma_{\alpha,j}^{i}\right)\right] \\
&= \sum_{j=1}^{n}\chi_i\left(\left\{\frac{1}{|\mathcal{M}_n|},\rho_{\alpha,j}\right\}_{\alpha\in\mathcal{M}_n}\right) \\
&= \sum_{j=1}^{n}\frac{1}{|\mathcal{M}_n|}\sum_{\alpha\in\mathcal{M}_n} S\left(\sigma_{\alpha,j}^{i}\,||\,\bar{\sigma}_{i,j}\right).
\end{aligned} \tag{97}$$

The latter expression can be rewritten using Donald's identity:

$$\sum_j p_j S(\omega_j\,||\,\rho) = \sum_j p_j S(\omega_j\,||\,\omega) + S(\bar{\omega}\,||\,\rho), \tag{98}$$

where $\bar{\omega} = \sum_j p_j\omega_j$. We apply this with ρ replaced by

$$\bar{\sigma}_i = \frac{1}{n|\mathcal{M}_n|}\sum_{j=1}^{n}\sum_{\alpha\in\mathcal{M}_n}\sigma_{\alpha,j}^{i} \tag{99}$$

and the sum replaced by a double sum over j and α with states $\sigma_{\alpha,j}^{i}$. This yields

$$\frac{1}{n|\mathcal{M}_n|}\sum_{j=1}^{n}\sum_{\alpha\in\mathcal{M}_n} S(\sigma_{\alpha,j}^{i}\,||\,\bar{\sigma}_{i,j}) = \frac{1}{n|\mathcal{M}_n|}\sum_{j=1}^{n}\sum_{\alpha\in\mathcal{M}_n} S(\sigma_{\alpha,j}^{i}\,||\,\bar{\sigma}_i) + S(\bar{\sigma}_i\,||\,\bar{\sigma}_{i,j}). \tag{100}$$

But, it follows from convexity of the relative entropy that the second term on the right-hand side is zero:

$$0 \leq S(\bar{\sigma}_i\,||\,\bar{\sigma}_{i,j}) \leq \frac{1}{n}\sum_{j=1}^{n} S(\bar{\sigma}_{i,j}\,||\,\bar{\sigma}_{i,j}) = 0. \tag{101}$$

Inserting into (97) we now have:

$$\frac{1}{n}H(X^{(n)} : Y_i^{(n)}) \leq \frac{1}{n|\mathcal{M}_n|}\sum_{j=1}^{n}\sum_{\alpha\in\mathcal{M}_n} S(\sigma_{\alpha,j}^i \,||\, \bar{\sigma}_i) = \chi_i\left(\left\{\frac{1}{n|\mathcal{M}_n|}, \rho_{\alpha,j}\right\}_{(\alpha,j)}\right). \tag{102}$$

Fano's inequality (96) now yields

$$h(\bar{p}_{i,e}^{(n)}) + \bar{p}_{i,e}^{(n)} \log\, |\mathcal{M}_n| \geq \log\, |\mathcal{M}_n| - n\,\chi_i\left(\left\{\frac{1}{n|\mathcal{M}_n|}, \rho_{\alpha,j}\right\}_{(\alpha,j)}\right), \tag{103}$$

However, since

$$C(\Phi) \geq \bigwedge_{i=1}^{M} \chi_i\left(\left\{\frac{1}{n|\mathcal{M}_n|}, \rho_{\alpha,j}\right\}_{(\alpha,j)}\right) \tag{104}$$

and $R = \frac{1}{n}\log|\mathcal{M}_n| > C(\Phi)$, there must be at least one branch i such that

$$\bar{p}_{i,e}^{(n)} \geq 1 - \frac{C(\Phi) + 1/n}{R} > 0. \tag{105}$$

We conclude from (94) and (105) that

$$\bar{p}_e^{(n)} \geq \left(1 - \frac{C(\Phi) + 1/n}{R}\right) \bigwedge_{i=1}^{M} \gamma_i. \tag{106}$$

□

Acknowledgements

The authors would like to thank Andreas Winter for a helpful suggestion. This work was supported by the European Commission through the Integrated Project FET/QIPC "SCALA".

References

[1] I. Bjelaković, T. Krüger, R. Siegmund-Schultze & A. Szkoła, "The Shannon-McMillan theorem for ergodic quantum lattice systems," *Invent. math.* **155**, 203–222, 2004.

[2] I. Bjelaković and H. Boche, "Ergodic Classical-Quantum Channels: Structure and Coding Theorems", *quant-ph/0609229*.

[3] G. Bowen and S. Mancini, "Quantum channels with a finite memory", *Phys. Rev. A* **69**, 01236, 2004.

[4] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* John Wiley & Sons, Inc.

[5] N.Datta and T.Dorlas, "A Quantum Version of Feinstein's Lemma and its application to Channel Coding", *Proc. of Int. Symp. Inf. Th. ISIT 2006, Seattle,* 441-445 (2006).

[6] A. Feinstein, " A new basic theorem of information theory," *IRE Trans. PGIT,* **4**, pp. 2–22, 1954.

[7] M.Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inform. Theory* **49**, pp. 1753–1768, 2003.

[8] *Quantum Detection and Estimation Theory,* Mathematics in Science and Engineering, **vol. 123**, Academic Press, London 1976.

[9] F. Hiai & D. Petz, "The proper formula for the relative entropy and its asymptotics in quantum probability". *Commun. Math. Phys.* **143**, 257–281, 1991.

[10] A.S. Holevo, "The capacity of a quantum channel with general signal states," *IEEE Trans. Info. Theory*, **44**, 269-273, 1998.

[11] A. I. Khinchin, *Mathematical Foundations of Information Theory,* Dover Publications, 1957. Part II: On the Fundamental Theorems of Information Theory, Chapter IV.

[12] D. Kretschmann and R.F.Werner, "Quantum channels with memory," *quant-ph/0502106.*

[13] C. Macchiavello and G. M. Palma, "Entanglement–enhanced information transmission over a quantum channel with correlated noise", *Phys. Rev. A* **65**, 050301, 2002.

[14] M.A. Nielson and I. L. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press, Cambridge, 2000.

[15] J.R.Norris, *Markov Chains, Cambridge Series in Statistical and Probabilistic Mathematics* Cambridge University Press, Cambridge, 1997.

[16] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, 1993.

[17] B. Schumacher, "Quantum Coding", *Phys. Rev. A* **51**, 2738-2747, 1995.

[18] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A* **56**, 131-138, 1997.

[19] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pt. I, pp. 379–423, 1948; pt. II, pp. 623–656, 1948.

[20] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. Info. Theory*, **45**, 2481–2485, 1999.