Quantum Version of Shannon's Noisy Coding Theorem

N. Datta
Statistical Laboratory
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road, Cambridge CB3 0WB
Email: n.datta@statslab.cam.ac.uk

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

February 17, 2006

Abstract

We prove an analogue of Feinstein's lemma for a memoryless quantum channel and use it to prove a quantum version of Shannon's noisy coding theorem.

1 A quantum channel with classical memory

Let $\mathcal{H}$ and $\mathcal{K}$ be given finite-dimensional Hilbert spaces and denote by $\mathcal{B}(\mathcal{H})$ the algebra of linear operators on $\mathcal{H}$. We also consider the tensor product algebras $\mathcal{A}_n = \mathcal{B}(\mathcal{H}^{\otimes n})$ and the infinite tensor product C*-algebra obtained as the strong closure

$$\mathcal{A}_\infty = \overline{\bigcup_{n=1}^{\infty} \mathcal{A}_n}, \tag{1.1}$$

where we include $\mathcal{A}_n$ into $\mathcal{A}_{n+1}$ in the obvious way. Similarly, we define $\mathcal{B}_n = \mathcal{B}(\mathcal{K}^{\otimes n})$ and $\mathcal{B}_\infty$. We denote the states on $\mathcal{A}_\infty$ by $\mathcal{S}(\mathcal{A}_\infty)$, etc.

Let there be given a Markov chain on a finite state space I given by transition probabilities $q_{i'|i}$ and let $(q_i)_{i\in I}$ be an equilibrium distribution for this chain, i.e.

$$q_{i'} = \sum_{i\in I} q_i q_{i'|i}. \tag{1.2}$$

Moreover, let $V_i : \mathcal{H} \to \mathcal{K}$ be given isometries for each $i \in I$. Then we define a quantum channel by the completely positive trace-preserving (CPT) map $\Phi_\infty : \mathcal{S}(\mathcal{A}_\infty) \to \mathcal{S}(\mathcal{B}_\infty)$ given by

$$\begin{aligned}\Phi_\infty(\phi)(A) \quad = \quad & \sum_{i_1,\dots,i_n\in I} q_{i_1} q_{i_2|i_1} \dots q_{i_n|i_{n-1}} \\ & \times \phi_n\left((V_{i_1}^* \otimes \dots \otimes V_{i_n}^*)\, A\, (V_{i_1} \otimes \dots \otimes V_{i_n}) \right)\end{aligned} \tag{1.3}$$

for $A \in \mathcal{B}_n$. Here, ϕ_n is the restriction of ϕ to $\mathcal{A}_n$. It is easily seen that this defines a CPT map on the states, and moreover, that it is translation-invariant (stationary).

We now define the **product state capacity** of this channel. Suppose that $\{p_j, \rho_j\}_{j=1}^M$ is a sequence of states ρ_j on $\mathcal{H}$ with probabilities p_j, $\sum_{j=1}^M p_j = 1$. For a multi-index $\underline{j} = (j_1, \dots, j_n)$ we denote $p_{\underline{j}}^{(n)} = p_{j_1} \dots p_{j_n}$ and $\rho_{\underline{j}}^{(n)} = \rho_{j_1} \otimes \dots \otimes \rho_{j_n}$. Then

$$\bar{\sigma}_n = \sum_{j_1\dots,j_n=1}^{M} p_{\underline{j}}^{(n)} \Phi_n(\rho_{\underline{j}}^{(n)}) \tag{1.4}$$

is a projective system of states on $\mathcal{B}_\infty$ defining a translation-invariant state $\bar{\sigma}_\infty$ on $\mathcal{B}_\infty$, and the mean entropy

$$S_M(\bar{\sigma}_\infty) = \lim_{n\to\infty} \frac{1}{n} S\left(\bar{\sigma}_n\right) = \inf_{n\in\mathbb{N}} \frac{1}{n} S\left(\bar{\sigma}_n\right) \tag{1.5}$$

exists.

2 Quantum Version of Feinstein's Lemma

Theorem 2.1 *Let a quantum channel be given by a completely positive map $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$, and define the channel (product state) capacity by*

$$\chi(\Phi) = \sup_{\{p_j\}_{j=1}^J, \{\rho_j\}_{j=1}^J} \left\{ S\left(\sum_{j=1}^J p_j\, \Phi(\rho_j) \right) - \sum_{j=1}^J p_j\, S(\Phi(\rho_j)) \right\}, \tag{2.6}$$

where the supremum is taken over all finite sets of states $\rho_j \in \mathcal{B}(\mathcal{H})$ and probability distributions $\{p_j\}_{j=1}^J$. Given $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ there exists $N \geq 2^{n(\chi(\Phi)-\epsilon)}$ and there exist states $\tilde{\rho}_1^{(n)}, \dots, \tilde{\rho}_N^{(n)} \in \mathcal{B}(\mathcal{H})$ and positive operators $E_1, \dots, E_N \in \mathcal{B}_+(\mathcal{K})$ such that $\sum_{k=1}^N E_k \leq \mathbf{1}$ and

$$\mathrm{Trace}\left[\Phi^{\otimes n} \left(\tilde{\rho}_k^{(n)} \right) E_k \right] > 1 - \epsilon. \tag{2.7}$$

Proof. Let the supremum in (2.6) be attained for a collection $\{p_j, \rho_j\}_{j=1}^J$. Denote $\sigma_j = \Phi(\rho_j)$, $\bar{\sigma} = \sum_{j=1}^J p_j \Phi(\rho_j)$, $\sigma_n = \bar{\sigma}^{\otimes n}$, and $\tilde{\sigma}_k^{(n)} = \Phi^{\otimes n}(\tilde{\rho}_k^{(n)})$.

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 $\overline{\mathcal{T}}_{\delta,\epsilon}$ with projection P_n such that if $\bar{\sigma}_n$ has a spectral decomposition

$$\bar{\sigma}_n = \sum_{\underline{k}} \bar{\lambda}_{\underline{k}}^{(n)} |\psi_{\underline{k}}^{(n)}\rangle\langle\psi_{\underline{k}}^{(n)}| \tag{2.8}$$

then

$$\left| \frac{1}{n} \log \bar{\lambda}_{\underline{k}}^{(n)} + S(\bar{\sigma}) \right| < \frac{\epsilon}{3} \tag{2.9}$$

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

$$\mathrm{Trace}(P_n \bar{\sigma}_n) > 1 - \delta^2. \tag{2.10}$$

Define

$$\bar{S} = \sum_{j=1}^{J} p_j \, S(\sigma_j). \tag{2.11}$$

Lemma 2.1 *Given a sequence* $\underline{j} = (j_1, \dots, j_n)$ *let* $P_{\underline{j}}^{(n)}$ *be the projection onto the subspace spanned by the eigenvectors of* $\sigma_{\underline{j}}^{(n)} = \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_n}$ *with eigenvalues* $\lambda_{\underline{j},\underline{k}}^{(n)} = \prod_{i=1}^n \lambda_{j_i,k_i}$ *such that*

$$\left| \frac{1}{n} \log \lambda_{\underline{j},\underline{k}}^{(n)} + \bar{S} \right| < \frac{\epsilon}{3}. \tag{2.12}$$

Let $\delta > 0$*. There exists* $n_2 \in \mathbb{N}$ *such that for* $n \geq n_2$*,*

$$\mathbb{E}\left(\mathrm{Trace}\left(\sigma_{\underline{j}}^{(n)} P_{\underline{j}}^{(n)} \right) \right) > 1 - \delta^2. \tag{2.13}$$

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

$$\mathbb{P}(X_i = \lambda_{j,k}) = p_j \, \lambda_{j,k}, \tag{2.14}$$

where $\lambda_{j,k}, \; k = 1, 2, \dots, d'$ are the eigenvalues of σ_j. By the weak law of large numbers,

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^{n} \log X_i \to \mathbb{E}(\log X_i) &= \sum_{j=1}^{J} \sum_{k=1}^{d'} p_j \, \lambda_{j,k} \log \lambda_{j,k} \\ &= -\sum_{j=1}^{J} p_j \, S(\sigma_j) = -\bar{S}. \end{aligned} \tag{2.15}$$

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

$$\left| \frac{1}{n} \sum_{i=1}^{n} \log \lambda_{j_i,k_i} + \bar{S} \right| < \frac{\epsilon}{3} \tag{2.16}$$

satisfies

$$\mathbb{P}\left(T_{\delta,\epsilon}^{(n)} \right) = \sum_{((j_1,k_1),\dots,(j_n,k_n)) \in T_{\delta,\epsilon}^{(n)}} \prod_{i=1}^{n} p_{j_i} \lambda_{j_i,k_i} > 1 - \delta^2. \tag{2.17}$$

Obviously,

$$P_{\underline{j}}^{(n)} \geq \sum_{\underline{k}:(\underline{j},\underline{k})\in T_{\delta,\epsilon}^{(n)}} |\psi_{\underline{j},\underline{k}}^{(n)}\rangle\langle\psi_{\underline{j},\underline{k}}^{(n)}| \tag{2.18}$$

and

$$\mathbb{E}\left(\text{Trace}\left(\sigma_{\underline{j}}^{(n)} P_{\underline{j}}^{(n)}\right)\right) \geq \mathbb{P}\left(T_{\delta,\epsilon}^{(n)}\right) > 1-\delta^2. \tag{2.19}$$

$\square$

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

(i) $\sum_{k=1}^N E_k \leq P_n$ and

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

(iii) $\text{Trace}[\,\bar{\sigma}_n E_k] \leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]}$.

For any given $\underline{j}$ define

$$V_{\underline{j}}^{(n)} = \left(P_n - \sum_{k=1}^N E_k\right)^{1/2} P_n P_{\underline{j}}^{(n)} P_n \left(P_n - \sum_{k=1}^N E_k\right)^{1/2}. \tag{2.20}$$

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

Lemma 2.2 *Define*

$$W_n = \{\underline{j} \mid \text{Trace}(\sigma_{\underline{j}}^{(n)} P_{\underline{j}}^{(n)}) > 1-\delta\}. \tag{2.21}$$

Then, for all $\underline{j} \in W_n$,

$$\text{Trace}(\bar{\sigma}_n V_{\underline{j}}^{(n)}) \leq 2^{-n[S(\bar{\sigma})-\bar{S}-\frac{2}{3}\epsilon]}. \tag{2.22}$$

Proof. Put $Q_n = \sum_{k=1}^{N(n)} E_k$. Note that Q_n commutes with P_n. Using the fact that $P_n \bar{\sigma}_n P_n \leq 2^{-n[S(\bar{\sigma})-\frac{1}{3}\epsilon]}$ by (2.9), we have

$$\begin{aligned} \mathrm{Trace}(\bar{\sigma}_n V_{\underline{j}}^{(n)}) &= \mathrm{Trace}\left[\bar{\sigma}_n (P_n - Q_n)^{1/2} P_n P_{\underline{j}}^{(n)} P_n (P_n - Q_n)^{1/2}\right] \\ &= \mathrm{Trace}\left[P_n \bar{\sigma}_n P_n (P_n - Q_n)^{1/2} P_{\underline{j}}^{(n)} (P_n - Q_n)^{1/2}\right] \\ &\leq 2^{-n[S(\bar{\sigma}_n)-\frac{1}{3}\epsilon]}\, \mathrm{Trace}\left[(P_n - Q_n)^{1/2} P_{\underline{j}}^{(n)} (P_n - Q_n)^{1/2}\right] \\ &\leq 2^{-n[S(\bar{\sigma}_n)-\frac{1}{3}\epsilon]}\, \mathrm{Trace}\,(P_{\underline{j}}^{(n)}) \leq 2^{-n[S(\bar{\sigma}_n)-\bar{S}-\frac{2}{3}\epsilon]}, \end{aligned} \tag{2.23}$$

where, in the last inequality, we used the standard upper bound on the dimension of the typical subspace: $\mathrm{Trace}(P_{\underline{j}}^{(n)}) \leq 2^{n[\bar{S}+\frac{1}{3}\epsilon]}$, which follows from Lemma 2.1. □

Since $N(n)$ is maximal it follows that for $\underline{j} \in W_n$,

$$\mathrm{Trace}\left(\sigma_{\underline{j}}^{(n)} V_{\underline{j}}^{(n)}\right) \leq 1 - 2\epsilon. \tag{2.24}$$

Lemma 2.3 *For all $\eta > 0$, there exists $n_3 \in \mathbb{N}$ such that for all $n \geq n_3$,*

$$\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} P_n\right]\right) > 1 - \eta. \tag{2.25}$$

Proof. We write

$$\begin{aligned} &\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} P_n\right]\right) = \\ &= \mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)} P_{\underline{j}}^{(n)}\right]\right) - \mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)} (\mathbf{1} - P_n) P_{\underline{j}}^{(n)}\right]\right) \\ &\quad - \mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} (\mathbf{1} - P_n)\right]\right). \end{aligned} \tag{2.26}$$

By Lemma 2.1, the first term is $> 1 - \delta^2$ provided $n \geq n_2$. The last two terms can be bounded using Cauchy-Schwarz as follows:

$$\begin{aligned}
&\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)P_{\underline{j}}^{(n)}\right]\right) = \\
&= \mathbb{E}\left(\mathrm{Trace}\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}(\mathbf{1}-P_n)P_{\underline{j}}^{(n)}\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right) \\
&\le \left\{\mathbb{E}\left(\mathrm{Trace}\left[(\mathbf{1}-P_n)\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right)\right\}^{1/2} \\
&\qquad \times\left\{\mathbb{E}\left(\mathrm{Trace}\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}P_{\underline{j}}^{(n)}\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right)\right\}^{1/2} \\
&= \left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right)\right\}^{1/2}\left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}P_{\underline{j}}^{(n)}\right]\right)\right\}^{1/2} \\
&\le \left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right)\right\}^{1/2} \\
&= \left(\mathrm{Trace}\left[\bar{\sigma}_n(\mathbf{1}-P_n)\right]\right)^{1/2} \le \delta \qquad (2.27)
\end{aligned}$$

by (2.10) provided $n \ge n_1$. Similarly,

$$\begin{aligned}
&\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}P_nP_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right) = \\
&= \mathbb{E}\left(\mathrm{Trace}\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}P_nP_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right) \\
&\le \left\{\mathbb{E}\left(\mathrm{Trace}\left[P_{\underline{j}}^{(n)}P_n\sigma_{\underline{j}}^{(n)}P_nP_{\underline{j}}^{(n)}\right]\right)\right\}^{1/2} \\
&\qquad \times\left\{\mathbb{E}\left(\mathrm{Trace}\left[\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}(\mathbf{1}-P_n)\left(\sigma_{\underline{j}}^{(n)}\right)^{1/2}\right]\right)\right\}^{1/2} \\
&= \left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}P_nP_{\underline{j}}^{(n)}P_n\right]\right)\right\}^{1/2}\left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right)\right\}^{1/2} \\
&\le \left\{\mathbb{E}\left(\mathrm{Trace}\left[\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_n)\right]\right)\right\}^{1/2} \le \delta. \qquad (2.28)
\end{aligned}$$

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

We now show that the set W_n has high probability:

Lemma 2.4 $\mu(W_n) > 1 - \delta$.

Proof. If $\underline{j} \notin W_n$ then $\mathrm{Trace}\left(\sigma_{\underline{j}}^{(n)}P_{\underline{j}}^{(n)}\right) \le 1-\delta$. Hence

$$\sum_{\underline{j}\notin W_n} p_{\underline{j}}^{(n)}\,\mathrm{Trace}\left(\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_{\underline{j}}^{(n)})\right) \ge \delta\,\mu(W_n^c). \qquad (2.29)$$

On the other hand,

$$\sum_{\underline{j}\notin W_n} p_{\underline{j}}^{(n)} \operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_{\underline{j}}^{(n)})\right) \leq \mathbb{E}\left(\operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)}(\mathbf{1}-P_{\underline{j}}^{(n)})\right)\right) < \delta^2. \quad (2.30)$$

It follows that $\mu(W_n^c) < \frac{\delta^2}{\delta} = \delta$. □

Corollary 2.1 *Assume $\delta < \frac{1}{2}\epsilon$. Then*

$$\mathbb{E}\left(\operatorname{Trace}\left[\sigma_{\underline{j}}^{(n)} V_{\underline{j}}^{(n)}\right]\right) < 1 - \frac{1}{2}\epsilon. \quad (2.31)$$

Proof. Using (2.24), we have

$$\begin{aligned} &\mathbb{E}\left(\operatorname{Trace}\left[\sigma_{\underline{j}}^{(n)} V_{\underline{j}}^{(n)}\right]\right) = \\ &= \sum_{\underline{j}\in W_n} p_{\underline{j}}^{(n)} \operatorname{Trace}\left[\sigma_{\underline{j}}^{(n)} V_{\underline{j}}^{(n)}\right] + \sum_{\underline{j}\in W_n^c} p_{\underline{j}}^{(n)} \operatorname{Trace}\left[\sigma_{\underline{j}}^{(n)} V_{\underline{j}}^{(n)}\right] \\ &\leq 1 - \epsilon + \mu(W_n^c) < 1 - \epsilon \end{aligned} \quad (2.32)$$

provided $\delta < \epsilon$. □

Lemma 2.5 *Assume $\eta < \frac{1}{6}\epsilon$. Then for $n \geq n_3$,*

$$\operatorname{Trace}\left[\bar{\sigma}_n \sum_{k=1}^N E_k\right] = \mathbb{E}\left(\operatorname{Trace}\left[\sigma_{\underline{j}}^{(n)} \sum_{k=1}^N E_k\right]\right) \geq \eta^2. \quad (2.33)$$

Proof. Define

$$Q_n' = P_n - (P_n - Q_n)^{1/2}. \quad (2.34)$$

By the above corollary,

$$\begin{aligned} 1 - \frac{1}{2}\epsilon \;\geq\; & \mathbb{E}\left\{\operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)}(P_n - Q_n')P_{\underline{j}}^{(n)}(P_n - Q_n')\right)\right\} \\ = \;& \mathbb{E}\left\{\operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} P_n\right)\right\} \\ & -\mathbb{E}\left\{\operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)} Q_n' P_{\underline{j}}^{(n)} P_n\right) + \operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} Q_n'\right)\right\} \\ & +\mathbb{E}\left\{\operatorname{Trace}\left(\sigma_{\underline{j}}^{(n)} Q_n' P_{\underline{j}}^{(n)} Q_n'\right)\right\}. \end{aligned} \quad (2.35)$$

Since the last term is positive, we have, by Lemma 2.3,

$$\mathbb{E}\left\{\text{Trace}\left(\sigma_{\underline{j}}^{(n)} Q'_n P_{\underline{j}}^{(n)} P_n\right) + \text{Trace}\left(\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} Q'_n\right)\right\} \geq \frac{1}{2}\epsilon - \eta > 2\eta. \quad (2.36)$$

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

$$\begin{aligned} &\mathbb{E}\left\{\text{Trace}\left(\sigma_{\underline{j}}^{(n)} Q'_n P_{\underline{j}}^{(n)} P_n\right) + \text{Trace}\left(\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} Q'_n\right)\right\} \leq \\ &\leq \; 2\left\{\mathbb{E}\left[\text{Trace}\left(Q'_n \sigma_{\underline{j}}^{(n)} Q'_n\right)\right]\right\}^{1/2} \left\{\mathbb{E}\left[\text{Trace}\left(\sigma_{\underline{j}}^{(n)} P_n P_{\underline{j}}^{(n)} P_n\right)\right]\right\}^{1/2} \\ &\leq \; 2\left\{\mathbb{E}\left[\text{Trace}\left(\sigma_{\underline{j}}^{(n)} Q_n'^2\right)\right]\right\}^{1/2}. \end{aligned} \quad (2.37)$$

Thus,

$$\mathbb{E}\left[\text{Trace}\left(\sigma_{\underline{j}}^{(n)} Q_n'^2\right)\right] \geq \eta^2. \quad (2.38)$$

To complete the proof, we now claim that

$$Q_n \geq (Q'_n)^2. \quad (2.39)$$

Indeed, this follows on the domain of P_n from the inequality $1-(1-x)^2 \geq x^2$ for $0 \leq x \leq 1$. □

To complete the proof of the theorem, we now have by assumption,

$$\text{Trace}\left[\bar{\sigma}_n E_k\right] \leq 2^{-n[S(\bar{\sigma}) - \bar{S} - \frac{2}{3}\epsilon]} \quad (2.40)$$

for all $k = 1, \ldots, N(n)$. On the other hand, choosing $\eta < \frac{1}{6}\epsilon$ and $\delta < \frac{1}{3}\eta$, we have by Lemma 2.5,

$$\text{Trace}\left[\bar{\sigma}_n \sum_{k=1}^{N} E_k\right] \geq \eta^2 \quad (2.41)$$

provided $n \geq n_3$. It follows that

$$N(n) \geq \eta^2 2^{n[S(\bar{\sigma}) - \bar{S} - \frac{2}{3}\epsilon]} \geq 2^{n[S(\bar{\sigma}) - \bar{S} - \epsilon]} \quad (2.42)$$

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