A Proof of Everett's Correlation Conjecture.

Matthew J. Donald

The Cavendish Laboratory, JJ Thomson Avenue, Cambridge CB3 0HE, Great Britain.

e-mail: **mjd1014@cam.ac.uk**

web site: **http://people.bss.phy.cam.ac.uk/~mjd1014**

Abstract In his long 1957 paper, "The Theory of the Universal Wave Function", Hugh Everett III made some significant preliminary steps towards the application and generalization of Shannon's information theory to quantum mechanics. In the course of doing so, he conjectured that, for a given wavefunction on a compound space, the Schmidt decomposition maximises the correlation between subsystem bases. This is proved here.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be separable Hilbert spaces and $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be their tensor product. Let $\Psi \in \mathcal{H}$ be a wavefunction – by which I mean simply that $||\Psi|| = 1$. Suppose that $\mathcal{H}_1$ has dimension $D_1 \leq \infty$ and $\mathcal{H}_2$ has dimension $D_2 \leq \infty$. Without loss of generality, suppose that $D_1 \leq D_2$.

A Schmidt decomposition (von Neumann 1932, Everett 1957, and many modern textbooks) of Ψ is an expansion of the form $\Psi = \sum_{n=1}^{D_1} \sqrt{p_n} \varphi_n \psi_n$ where $(\varphi_n)_{n=1}^{D_1}$ is an orthornormal basis of $\mathcal{H}_1$, $(\psi_n)_{n=1}^{D_2}$ is an orthornormal basis of $\mathcal{H}_2$, $0 \leq p_n \leq 1$ and $\sum_{n=1}^{D_1} p_n = 1$. Schmidt decompositions always exist. They are unique, up to phase factors, as long as $D_1 = D_2$ and the p_n are all distinct.

Mixtures of notations from both mathematics and physics will be used and abused throughout this note. For example, $\varphi_n \psi_n$ is written here for $\varphi_n \otimes \psi_n$. In notation used later, the same wavefunction would appear as $|\varphi_n, \psi_n\rangle$ or simply as $|n, n\rangle$.

Set $\sigma = |\Psi\rangle\langle\Psi|$. σ is a pure state on the algebra $\mathcal{B}(\mathcal{H})$ of bounded operators on $\mathcal{H}$ and for $B \in \mathcal{B}(\mathcal{H})$ we shall write $\sigma(B) = \langle\Psi|B|\Psi\rangle = \text{tr}(|\Psi\rangle\langle\Psi|B)$.

Define σ_1 to be the reduced density matrix of σ on $\mathcal{H}_1$. In other words, $\sigma_1 = \text{tr}_{\mathcal{H}_2}(\sigma)$ is the partial trace of σ over $\mathcal{H}_2$, and, for all $B_1 \in \mathcal{B}(\mathcal{H}_1)$, $\sigma_1(B_1) = \sigma(B_1 \otimes 1_2)$ where 1_2 is the identity operator on $\mathcal{H}_2$. $\sigma_2 = \text{tr}_{\mathcal{H}_2}(\sigma)$ and 1_1 are defined similarly.

The Schmidt decomposition gives

$$\sigma_1 = \sum_{n=1}^{D_1} p_n |\varphi_n\rangle\langle\varphi_n| \quad \text{and} \quad \sigma_2 = \sum_{n=1}^{D_1} p_n |\psi_n\rangle\langle\psi_n|.$$

Suppose that $\mathcal{Z}_1 = (P_i)_{i=1}^{I}$ (respectively $\mathcal{Z}_2 = (Q_j)_{j=1}^{J}$) is a sequence of orthogonal projections in $\mathcal{B}(\mathcal{H}_1)$ (resp. $\mathcal{B}(\mathcal{H}_2)$) such that $\sum_{i=1}^{I} P_i = 1_1$ (resp. $\sum_{j=1}^{J} Q_j = 1_2$). We shall write $P_i Q_j$ for $P_i \otimes Q_j \in \mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

In particular, write $\widetilde{P}_n = |\varphi_n\rangle\langle\varphi_n|$ for $n = 1, \ldots, D_1$, $\widetilde{Q}_n = |\psi_n\rangle\langle\psi_n|$ for $n = 1, \ldots, D_2$, $\widetilde{\mathcal{Z}}_1 = (\widetilde{P}_n)_{n=1}^{D_1}$, and $\widetilde{\mathcal{Z}}_2 = (\widetilde{Q}_n)_{n=1}^{D_2}$.

In all cases,

$$\sum_{j=1}^{J} \sigma(P_i Q_j) = \sigma(P_i \otimes 1_2) = \sigma_1(P_i) \quad \text{and} \quad \sum_{i=1}^{I} \sigma(P_i Q_j) = \sigma(1_1 \otimes Q_j) = \sigma_2(P_j). \quad (1)$$

When discussing relative entropies, we shall also use $\mathcal{Z}_1$ and $\mathcal{Z}_2$ to denote the abelian von Neumann algebras generated by $(P_i)_{i=1}^{I}$ and $(Q_j)_{j=1}^{J}$, while $\mathcal{Z}$ will denote the abelian von Neumann algebra $\mathcal{Z}_1 \otimes \mathcal{Z}_2 \subset \mathcal{B}(\mathcal{H})$ generated by $(P_i Q_j)_{i=1\,j=1}^{I\quad J}$.

Define

$$\{\mathcal{Z}_1, \mathcal{Z}_2\}_\Psi = \sum_{i,j} \big[\sigma(P_i Q_j) \log \sigma(P_i Q_j) - \sigma(P_i Q_j) \log(\sigma_1(P_i)\sigma_2(Q_j))$$

$$-\sigma(P_i Q_j) + \sigma_1(P_i)\sigma_2(Q_j) \big]. \quad (2)$$

Of course $\sum_{i,j} \sigma(P_i Q_j) = \sum_{i,j} \sigma_1(P_i)\sigma_2(Q_j) = 1$ so that the final terms in definition (1) are redundant in the finite-dimensional case. They are added for the general case, however, because, then, by the standard inequality

$$s \geq 0, r \geq 0 \Rightarrow s \log s - s \log r - s + r \geq 0,$$

each term in the sum is non-negative, and the sum is well-defined even if it is infinite. Note that with the convention that $0 \log 0 = 0$, each term in the sequence is finite because

$$\sigma_1(P_i)\sigma_2(Q_j) = 0 \Rightarrow \sigma(P_i Q_j) = 0.$$

This holds by the Cauchy-Schwarz inequality, or alternatively because, $\sigma(P_i Q_j) \geq 0$ for each j and so, by (1),

$$\sigma_1(P_i) = 0 \Rightarrow \sigma(P_i Q_j) = 0 \text{ for all } j.$$

(2) is the mutual information of random variables X on $\{i = 1, \ldots, I\}$ and Y on $\{j = 1, \ldots, J\}$ with joint distribution $\mathrm{P}_{joint}(i,j) = \sigma(P_i Q_j)$ (Cover and Thomas 1991). In other words, with the convention in which relative entropy is negative, it is the absolute value of the relative entropy of the joint distribution $\mathrm{P}_{joint}(i,j)$ with respect to the product distribution of the marginals $\mathrm{P}_{marg}(i,j) = \sigma_1(P_i)\sigma_2(Q_j)$. This means that the greater the mutual information, the more different the joint distribution is from the product distribution, and thus the more that X and Y are correlated.

Generalizing to the quantum case, Everett considers operators $A = \sum_i a_i P_i$ on $\mathcal{H}_1$ and $B = \sum_j b_j Q_j$ on $\mathcal{H}_2$ and calls $\{\mathcal{Z}_1, \mathcal{Z}_2\}_\Psi$ the correlation between A and B on Ψ. He then conjectures theorem 3.

Theorem 3

$$0 \leq \{\mathcal{Z}_1, \mathcal{Z}_2\}_\Psi \leq \{\widetilde{\mathcal{Z}}_1, \widetilde{\mathcal{Z}}_2\}_\Psi = -\sum_n p_n \log p_n.$$

proof Begin by assuming that $\dim \mathcal{H}_1 = \dim \mathcal{H}_2 = D < \infty$.

Using (1), we can write the result in the form

$$-\sum_j \sigma_2(Q_j) \log \sigma_2(Q_j) - \sum_i \sigma_1(P_i) \log \sigma_1(P_i)$$

$$\leq -\sum_n p_n \log p_n - \sum_{i,j} \sigma(P_i Q_j) \log \sigma(P_i Q_j). \quad (4)$$

2

Inequalities of this sort between quantum entropies involving sequences of operators which need not commute such as the (P_i) and $(\widetilde{P}_n)$ and the (Q_j) and $(\widetilde{Q}_n)$ can be difficult to prove (even when they are true). The fundamental result in this area is strong subadditivity conjectured, in a statistical mechanical context, by Lanford and Robinson (1968) and proved by Lieb and Ruskai (1973). This says that if we have a state ρ on a Hilbert space $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_c$ and we define $\rho_b = \mathrm{tr}_{\mathcal{H}_a \otimes \mathcal{H}_c}(\rho)$, $\rho_{ab} = \mathrm{tr}_{\mathcal{H}_c}(\rho)$, and $\rho_{bc} = \mathrm{tr}_{\mathcal{H}_a}(\rho)$, then

$$S(\rho) + S(\rho_b) \leq S(\rho_{ab}) + S(\rho_{bc}) \tag{5}$$

where, for any state ω, $S(\omega) = -\mathrm{tr}(\omega \log \omega)$.

Suppose that $\dim \mathcal{H}_a = D < \infty$, and let τ_a be the totally mixed state on $\mathcal{H}_a$. For σ and ω any states on a Hilbert space $\mathcal{H}$, the relative entropy of σ with respect to ω is defined as

$$\mathrm{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \,|\, \omega) = \mathrm{tr}(-\sigma \log \sigma + \sigma \log \omega).$$

This definition uses the convention that relative entropy is negative. In Donald (1986) and Donald (1992), I explain that $\exp\{\mathrm{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \,|\, \omega)\}$ can be interpreted as the probability per trial of information given by operators in $\mathcal{B}(\mathcal{H})$ of mistaking the state ω for the state σ. To apply this to understand why equation (5) should be true, note that, using the definition of the partial trace,

$$\mathrm{ent}_{\mathcal{B}(\mathcal{H})}(\rho \,|\, \tau_a \otimes \rho_{bc}) = S(\rho) - S(\rho_{bc}) - \log D$$

and

$$\mathrm{ent}_{\mathcal{B}(\mathcal{H}_{ab})}(\rho_{ab} \,|\, \tau_a \otimes \rho_b) = S(\rho_{ab}) - S(\rho_b) - \log D.$$

This means that (5) is equivalent to

$$\mathrm{ent}_{\mathcal{B}(\mathcal{H})}(\rho \,|\, \tau_a \otimes \rho_{bc}) \leq \mathrm{ent}_{\mathcal{B}(\mathcal{H}_{ab})}(\rho_{ab} \,|\, \tau_a \otimes \rho_b). \tag{6}$$

(6) can be interpreted as saying that we are more likely to mistake the state $\tau_a \otimes \rho_{bc}$ for the state ρ if we can look at all the operators in $\mathcal{B}(\mathcal{H})$ than if we just get to look at the operators in $\mathcal{B}(\mathcal{H}_{ab})$. In other words, (6) is an example of the monotonicity of the relative entropy; a fundamental result with a wide variety of proofs and extensions (Ohya and Petz 1993).

The difficulty now is to equate each of the terms in (4) with the entropy of a state restriction as in (5). But first some preliminaries:

$$\sigma(\widetilde{P}_n \widetilde{Q}_m) = p_n \delta_{n,m} \text{ and } \sigma_1(\widetilde{P}_n) = \sigma_2(\widetilde{Q}_n) = p_n \text{ so that}$$

$$\{\widetilde{\mathcal{Z}}_1, \widetilde{\mathcal{Z}}_2\}_\Psi = \sum_n p_n \log p_n/(p_n)^2 = -\sum_n p_n \log p_n.$$

This determines the right hand side of theorem 3, and shows that, like the sequence (p_n), it is independent of the choice of Schmidt decomposition of Ψ.

remark It is tempting to try to prove Everett's conjecture using the monotonicity of the relative entropy under quantum operations (Lindblad 1974, Uhlmann 1977), with the quantum operation $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ defined by $\mathcal{E}(B) = \sum_{ij} P_i Q_j B P_i Q_j$, or alternatively, by using monotonicity under restriction to the subalgebra $\mathcal{Z}$. Everett's

conjecture, however, seems remarkably strong in the sense that a direct use of these theorems just gives

$$\text{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \,|\, \sigma_1 \otimes \sigma_2) \le \text{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \circ \mathcal{E} \,|\, (\sigma_1 \otimes \sigma_2) \circ \mathcal{E}) \le \text{ent}_{\mathcal{Z}}(\sigma \,|\, \sigma_1 \otimes \sigma_2) \le 0.$$

The useful terms here work out as

$$2 \sum_n p_n \log p_n = \text{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \,|\, \sigma_1 \otimes \sigma_2) \le \text{ent}_{\mathcal{Z}}(\sigma \,|\, \sigma_1 \otimes \sigma_2) = -\{\mathcal{Z}_1, \mathcal{Z}_2\}_\Psi \le 0.$$

The problematic factor of 2 arises because σ is a pure state on the algebra $\mathcal{B}(\mathcal{H})$.

$$-\text{ent}_{\mathcal{B}(\mathcal{H})}(\sigma \,|\, \sigma_1 \otimes \sigma_2) = S(\sigma_1) + S(\sigma_2) - S(\sigma)$$

is also the quantum mutual information in this situation, so various inequalities involving that property are also not quite as strong as Everett's conjecture. $\{\widetilde{\mathcal{Z}}_1, \widetilde{\mathcal{Z}}_2\}_\Psi$ is in fact the negative of the relative entropy $\text{ent}_{\widetilde{\mathcal{Z}}}(\sigma \,|\, \sigma_1 \otimes \sigma_2)$ (or in strict notation $\text{ent}_{\widetilde{\mathcal{Z}}}(\sigma|_{\widetilde{\mathcal{Z}}} \,|\, \sigma_1|_{\widetilde{\mathcal{Z}}_1} \otimes \sigma_2|_{\widetilde{\mathcal{Z}}_2}))$ where, as von Neumann algebras, $\widetilde{\mathcal{Z}} = \widetilde{\mathcal{Z}}_1 \otimes \widetilde{\mathcal{Z}}_2$. Despite this failure, the quantum operation $\mathcal{E}$ and its components $\mathcal{E}^1$ and $\mathcal{E}^2$, defined by $\mathcal{E}^1(B_1) = \sum_i P_i B_1 P_i$ and $\mathcal{E}^2(B_2) = \sum_j Q_j B Q_j$, are central to the proof of the full result, in which we will use standard techniques to represent $\mathcal{E}^1$ and $\mathcal{E}^2$ as compositions of unitary maps and partial traces.

There are strong similarities between the proof I shall give here, and Schumacher and Nielsen's (1996) proof of the quantum data processing inequality. Nevertheless, it is not clear to me that Everett's inequality can be interpreted as an application of Schumacher and Nielsen's result. On the other hand, it may well come within the scope of exercise 12.15 of Nielsen and Chuang (2000) which begins: "Apply all possible combinations of the subadditivity and strong subadditivity inequalities to deduce other inequalities for [a] two stage quantum process"! Over the last twenty years, the literature on quantum information theory has explored a vast variety of such combinations to the point where I would quite surprised if Everett's inequality was not out there somewhere. As yet, however, I have failed to find it. Anyway, it seems worth having a leisurely exposition of a direct and fairly simple proof linked to the historical context.

lemma Suppose that $P_i = \sum_k P_{i,k}$. Then

$$\sum_{i,j} \sigma(P_i Q_j) \log \sigma(P_i Q_j) / (\sigma_1(P_i) \sigma_2(Q_j))$$

$$\le \sum_{i,j,k} \sigma(P_{i,k} Q_j) \log \sigma(P_{i,k} Q_j) / (\sigma_1(P_{i,k}) \sigma_2(Q_j)).$$

proof By the log sum inequality (Everett 1957 Appendix I.2 lemma 2, Cover and Thomas 1991 theorem 2.71) which is a consequence of the convexity of $x \log x$,

$$\sigma(P_i Q_j) \log \sigma(P_i Q_j) / (\sigma_1(P_i) \sigma_2(Q_j))$$

$$= \sum_k \sigma(P_{i,k} Q_j) \log \sum_{k'} \sigma(P_{i,k'} Q_j) / \sum_{k''} (\sigma_1(P_{i,k''}) \sigma_2(Q_j))$$

$$\le \sum_k \sigma(P_{i,k} Q_j) \log \sigma(P_{i,k} Q_j) / (\sigma_1(P_{i,k}) \sigma_2(Q_j)). \qquad \blacksquare$$

4

It follows that it is sufficient to prove the theorem for P_i and Q_j one-dimensional projections. Assume therefore that $P_i = |\alpha_i><\alpha_i|$ and $Q_j = |\beta_j><\beta_j|$ where $\{\alpha_i : i = 1, \ldots, D\}$ (resp. $\{\beta_j : j = 1, \ldots, D\}$) is an orthonormal basis of $\mathcal{H}_1$ (resp. $\mathcal{H}_2$).

Now return to the problem of finding a way to express each term in (4) as the entropy of a state restriction. Note first that there is a similarity between the two terms on the left of (4) which does not seem to be matched by the form of the spaces used in (5). This issue can be dealt with by introducing a fourth space $\mathcal{H}_d$ and a pure state on the total space $\mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_c \otimes \mathcal{H}_d$. Using a Schmidt decomposition shows that the entropy of the partial trace of that pure state over $\mathcal{H}_d$ will equal the entropy of its partial trace over $\mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_c$.

Introduce auxiliary spaces $\mathcal{H}'_1$ and $\mathcal{H}'_2$ with $\dim \mathcal{H}'_1 = \dim \mathcal{H}'_2 = D$ and orthonormal bases $\{|i> : i = 0, \ldots, D - 1\}$ and set

$$|\Psi_0> = |0> \otimes |\Psi> \otimes |0> \in \mathcal{H}'_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}'_2.$$

Define a linear map U on $\mathcal{H}'_1 \otimes \mathcal{H}_1$ by linear extension from

$$U(|n> \otimes |\alpha_i>) = |n \oplus i> \otimes |\alpha_i>$$

where $\oplus$ is addition modulo D. U is defined on an orthonormal basis, which it maps to another orthonormal basis:

$$<m \otimes \alpha_{i'}|U^*U|n \otimes \alpha_i> = <m \oplus i'|n \oplus i><\alpha_{i'}|\alpha_i> = <m \oplus i'|n \oplus i>\delta_{i,i'} = \delta_{m,n}\delta_{i,i'}$$

and so U is unitary. Note that, for $\varphi \in \mathcal{H}_1$,

$$U(|0> \otimes |\varphi>) = U(\sum_i |0> \otimes P_i|\varphi>) = \sum_i |i> \otimes P_i|\varphi> = \sum_i <\alpha_i|\varphi>|i, \alpha_i>.$$

Similarly, define a unitary map V on $\mathcal{H}_2 \otimes \mathcal{H}'_2$ by

$$V(|\beta_j> \otimes |n>) = |\beta_j> \otimes |n \oplus j>$$

and note that

$$V(|\psi> \otimes |0>) = \sum_j Q_j|\psi> \otimes |j> = \sum_j <\beta_j|\psi>|\beta_j, j>.$$

Set $|\Psi'> = (U \otimes V)|\Psi_0>$. Then

$$|\Psi'> = \sum_n \sqrt{p_n}U(|0> \otimes |\varphi_n>) \otimes V(|\psi_n> \otimes |0>) \tag{7}$$

$$= \sum_{ijn} \sqrt{p_n}|i> \otimes P_i|\varphi_n> \otimes Q_j|\psi_n> \otimes |j> = \sum_{ij} |i> \otimes P_iQ_j|\Psi> \otimes |j>.$$

Now set $\rho = |\Psi'><\Psi'|$. It is straightforward to calculate all of the partial traces of this state, either directly, or by identifying Schmidt decompositions. Note that as that ρ is pure, if $A \subset \{1', 1, 2, 2'\}$ and A^c is its complement, a Schmidt decomposition

5

of $|\Psi'\rangle$ will show that $S(\rho_A) = S(\rho_{A^c})$. The results give

$$S(\rho_1) = S(\rho_{1'}) = S(\rho_{1'22'}) = S(\rho_{122'}) = -\sum_i \sigma_1(P_i) \log \sigma_1(P_i)$$

$$S(\rho_2) = S(\rho_{2'}) = S(\rho_{1'12'}) = S(\rho_{1'12}) = -\sum_j \sigma_2(Q_j) \log \sigma_2(Q_j)$$

$$S(\rho_{1'2}) = S(\rho_{12}) = S(\rho_{12'}) = S(\rho_{1'2'}) = -\sum_{i,j} \sigma(P_i Q_j) \log \sigma(P_i Q_j)$$

$$S(\rho_{1'1}) = S(\rho_{22'}) = -\sum_n p_n \log p_n.$$

Several choices are now available to apply (5), including $a = 1'$, $b = 1$ and $c = 2$, and so the theorem is proved in the finite-dimensional case.

To confirm that the entropies of the partial traces are as given, first note that, as U and V are unitary, (7) provides the Schmidt decomposition of $|\Psi'\rangle$ with respect to the decomposition

$$(\mathcal{H}_1' \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2') = (\mathcal{H}_1' \otimes \mathcal{H}_1) \otimes (\mathcal{H}_2 \otimes \mathcal{H}_2').$$

This gives $S(\rho_{1'1}) = S(\rho_{22'}) = -\sum_n p_n \log p_n$.

Next, write

$$|\Psi'\rangle = \sum_{ij} |i\rangle \otimes P_i Q_j |\Psi\rangle \otimes |j\rangle = \sum_i |i\rangle \otimes \left(\sum_j \langle \alpha_i, \beta_j | \Psi \rangle | \alpha_i, \beta_j, j \rangle \right).$$

For $i \neq i'$, the vectors $\sum_j \langle \alpha_i, \beta_j | \Psi \rangle | \alpha_i, \beta_j, j \rangle$ and $\sum_j \langle \alpha_{i'}, \beta_j | \Psi \rangle | \alpha_{i'}, \beta_j, j \rangle$ are orthogonal. Moreover,

$$\left\| \sum_j \langle \alpha_i, \beta_j | \Psi \rangle | \alpha_i, \beta_j, j \rangle \right\|^2 = \sum_j |\langle \alpha_i, \beta_j | \Psi \rangle|^2 = \sum_j \sigma(P_i Q_j) = \sigma_1(P_i)$$

so we have the Schmidt decomposition of $|\Psi'\rangle$ with respect to the decomposition

$$(\mathcal{H}_1' \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2') = (\mathcal{H}_1') \otimes (\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2')$$

giving $S(\rho_{1'}) = S(\rho_{122'}) = -\sum_i \sigma_1(P_i) \log \sigma_1(P_i)$.

For the decomposition

$$(\mathcal{H}_1' \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2') = (\mathcal{H}_1' \otimes \mathcal{H}_2') \otimes (\mathcal{H}_1 \otimes \mathcal{H}_2),$$

$$|\Psi'\rangle = \sum_{ij} |i\rangle \otimes P_i Q_j |\Psi\rangle \otimes |j\rangle$$

already presents a Schmidt decomposition, as for $(i, j) \neq (i', j')$ the vectors $P_i Q_j |\Psi\rangle$ and $P_{i'} Q_{j'} |\Psi\rangle$ are orthogonal. $\|P_i Q_j |\Psi\rangle\|^2 = \sigma(P_i Q_j)$ and so

$$S(\rho_{12}) = S(\rho_{1'2'}) = -\sum_{i,j} \sigma(P_i Q_j) \log \sigma(P_i Q_j).$$

With the underlying symmetry of formalism under the exchange of $\mathcal{H}_1$ and $(P_i)_i$ with $\mathcal{H}_2$ and $(Q_j)_j$, it only remains to consider the decompositions

$$(\mathcal{H}_1' \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2') = (\mathcal{H}_1) \otimes (\mathcal{H}_1' \otimes \mathcal{H}_2 \otimes \mathcal{H}_2')$$

and

$$(\mathcal{H}_1' \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2') = (\mathcal{H}_1' \otimes \mathcal{H}_2) \otimes (\mathcal{H}_1 \otimes \mathcal{H}_2').$$

For these, write

$$|\Psi'> = \sum_{ij} <\alpha_i, \beta_j|\Psi>|i, \alpha_i, \beta_j, j>.$$

For $i \neq i'$, the pairs $|\alpha_i>$ and $|\alpha_{i'}>$ and $\sum_j <\alpha_i, \beta_j|\Psi>|i, \beta_j, j>$ and $\sum_j <\alpha_{i'}, \beta_j|\Psi>|i', \beta_j, j>$ are orthogonal, and

$$||\sum_j <\alpha_i, \beta_j|\Psi>|i, \beta_j, j>||^2 = \sum_j |<\alpha_i, \beta_j|\Psi>|^2 = \sum_j \sigma(P_iQ_j) = \sigma_1(P_i).$$

This yields $S(\rho_1) = S(\rho_{1'22'}) = -\sum_i \sigma_1(P_i) \log \sigma_1(P_i)$.

For $(i,j) \neq (i',j')$, the pairs $|i\beta_j>$ and $|i'\beta_{j'}>$ and $|\alpha_i, j>$ and $|\alpha_{i'}, j'>$ are orthogonal, and

$$|<\alpha_i, \beta_j|\Psi>|^2 = \sigma(P_iQ_j)$$

so that $S(\rho_{1'2}) = S(\rho_{12'}) = -\sum_{i,j} \sigma(P_iQ_j) \log \sigma(P_iQ_j)$.

Before dealing with the extension to infinite dimensions, note that the restriction $\dim \mathcal{H}_1 = \dim \mathcal{H}_2$ has only been used for notational convenience. Considering subspaces of such a situation is sufficient to yield the result for any pair of finite dimensional spaces.

lemma The theorem holds whenever the sequences $(P_i)_{i=1}^I$ and $(Q_j)_{j=1}^J$ are finite, and there are only finitely many $p_n > 0$.

proof Suppose $p_n > 0$ for $n = 1, \ldots, N < \infty$.

Let $\mathcal{K}_1$ be the Hilbert space spanned by the vectors

$$\{P_i\varphi_n : i = 1, \ldots, I; n = 1, \ldots, N\}.$$

$\mathcal{K}_1$ is finite-dimensional. Let P_i' be the restriction of P_i to $\mathcal{K}_1$.

Define $\mathcal{K}_2$ and (Q_j') similarly.

Then $\Psi = \sum_n \sqrt{p_n}\varphi_n \otimes \psi_n = \sum_{ijn} \sqrt{p_n}P_i\varphi_n \otimes Q_j\psi_n \in \mathcal{K}_1 \otimes \mathcal{K}_2$ and the finite-dimensional result can be applied, giving

$$-\sum_n p_n \log p_n \geq \sum_{i,j} \sigma(P_i'Q_j') \log \sigma(P_i'Q_j')/(\sigma_1(P_i')\sigma_2(Q_j'))$$

$$= \sum_{i,j} \sigma(P_iQ_j) \log \sigma(P_iQ_j)/(\sigma_1(P_i)\sigma_2(Q_j)). \qquad \blacksquare$$

Now suppose that the sequences $(P_i)_{i=1}^I$ and $(Q_j)_{j=1}^J$ remain finite, but consider general $\Psi = \sum_n \sqrt{p_n}\varphi_n\psi_n$. Let R^N be the projection on $\mathcal{H}$ onto the finite-dimensional space spanned by $\{\varphi_m\psi_n : m = 1, \ldots, N; n = 1, \ldots, N\}$. Assume, without loss of generality, that $p_1 > 0$ and set $r_n^N = p_n/\sum_{n=1}^N p_n$ and $\sigma^N = |\Psi^N><\Psi^N|$ where

$$\Psi^N = \sum_{n=1}^N \sqrt{r_n^N}\varphi_n\psi_n.$$

The lemma shows that

$$-\sum_{n=1}^N r_n^N \log r_n^N \geq \sum_{i,j} \sigma^N(P_iQ_j) \log \sigma^N(P_iQ_j)/(\sigma_1^N(P_i)\sigma_2^N(Q_j)).$$

This is equivalent to

$$\sum_{n=1}^{N} r_n^N \log r_n^N \leq \mathrm{ent}_{\mathcal{Z}}(\sigma^N|_{\mathcal{Z}} \,|\, \sigma_1^N|_{\mathcal{Z}_1} \otimes \sigma_2^N|_{\mathcal{Z}_2}).$$

W*-upper semicontinuity of relative entropy (Donald 1986), or, in this abelian situation, Fatou's lemma, then implies that

$$\mathrm{ent}_{\mathcal{Z}}(\sigma|_{\mathcal{Z}} \,|\, \sigma_1|_{\mathcal{Z}_1} \otimes \sigma_2|_{\mathcal{Z}_2}) \geq \limsup_{N \to \infty} \mathrm{ent}_{\mathcal{Z}}(\sigma^N|_{\mathcal{Z}} \,|\, \sigma_1^N|_{\mathcal{Z}_1} \otimes \sigma_2^N|_{\mathcal{Z}_2})$$

$$\geq \limsup_{N \to \infty} \sum_{n=1}^{N} r_n^N \log r_n^N = \limsup_{N \to \infty} \left(\frac{\sum_{n=1}^{N} p_n \log p_n}{\sum_{n=1}^{N} p_n} - \log\left(\sum_{n=1}^{N} p_n\right) \right) = \sum_{n=1}^{\infty} p_n \log p_n.$$

Finally, for the case of infinite sequences $(P_i)_{i=1}^{\infty}$ and $(Q_j)_{j=1}^{\infty}$, write $P^I = \sum_{i=I+1}^{\infty} P_i$, $Q^J = \sum_{j=J+1}^{\infty} Q_j$.

Then, we have just proved that, for all finite I and J,

$$-\sum_{n=1}^{\infty} p_n \log p_n \geq \sum_{i=1}^{I} \sum_{j=1}^{J} \left[\sigma(P_i Q_j) \log \sigma(P_i Q_j) - \sigma(P_i Q_j) \log(\sigma_1(P_i)\sigma_2(Q_j)) \right.$$

$$\left. -\sigma(P_i Q_j) + \sigma_1(P_i)\sigma_2(Q_j) \right]$$

$$+ \left[\sigma(P^I Q^J) \log \sigma(P^I Q^J) - \sigma(P^I Q^J) \log(\sigma_1(P^I)\sigma_2(Q^J)) - \sigma(P^I Q^J) + \sigma_1(P^I)\sigma_2(Q^J) \right]$$

$$\geq \sum_{i=1}^{I} \sum_{j=1}^{J} \left[\sigma(P_i Q_j) \log \sigma(P_i Q_j) - \sigma(P_i Q_j) \log(\sigma_1(P_i)\sigma_2(Q_j)) \right.$$

$$\left. -\sigma(P_i Q_j) + \sigma_1(P_i)\sigma_2(Q_j) \right].$$

Taking the limits $I \to \infty$, $J \to \infty$ gives the required bound and completes the proof of the theorem. ∎

References.

Cover, T.M. and Thomas, J.A. (1991) *Elements of Information Theory.* (Wiley)

DeWitt, B.S. and Graham, N. (1973) *The Many-Worlds Interpretation of Quantum Mechanics.* (Princeton)

Donald, M.J. (1986) "On the relative entropy." *Commun. Math. Phys.* **105**, 13–34.

Donald, M.J. (1992) "A priori probability and localized observers." *Foundations of Physics,* **22**, 1111–1172.

Everett, H., III (1957) "The theory of the universal wave function." Pages 1–140 of DeWitt and Graham (1973).

Lanford, O.E., III and Robinson, D.W. (1968) "Mean entropy of states in quantum-statistical mechanics." *J. Math. Phys.* **9**, 1120–1125.

Lieb, E.H. and Ruskai, M.B. (1973) "Proof of the strong subadditivity of quantum-mechanical entropy." *J. Math. Phys.* **14**, 1938–1941.

Lindblad, G. (1974) "Expectations and entropy inequalities for finite quantum systems." *Commun. Math. Phys.* **39**, 111–119.

Nielsen, M.A. and Chuang, I.L. (2000) *Quantum Computation and Quantum Information.* (Cambridge)

Ohya, M. and Petz, D. (1993) *Quantum Entropy and Its Use.* (Springer-Verlag)

Schumacher, B. and Nielsen M.A. (1996) "Quantum data processing and error correction." *Phys. Rev. A***54**, 2629–2635. *quant-ph/9604022*

Uhlmann, A. (1977) "Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory." *Commun. Math. Phys.* **54**, 21–32.

von Neumann, J. (1932) *Mathematische Grundlagen der Quantenmechanik.* (Springer). Everett cites the 1955 translation *Mathematical Foundations of Quantum Mechanics.* (Princeton)

August 2010