Characterization of Non Negative Conditional Von Neumann Entropy

Introduction— Entanglement, while conceptually fascinating, is the fundamental resource due to which several information processing tasks such as teleportation, superdense coding, key generation and secret sharing are possible, and is the reason several other information processing tasks have an advantage over their classical counterparts, as can be seen via non-local games. Hence, to study quantum states that are useful for such tasks, one has to classify them according to whether they are entangled or separable, and according to how much entanglement they possess.

Although it is known that the set of separable states is a convex set, the task of finding whether a general state is entangled or not, given the density matrix, is NP Hard [7]. Hence, characterizing the set of separable states and creating meaures to quantify entanglement is of utmost importance so as to come up with heuristics to comment on the usefulness of a state for the several information processing tasks. In this scenario, providing separating hyperplanes (witnesses) between the set of separable states and an entangled state is both theoretically and experimentally motivated, as such witnesses provide valuable information about the entanglement of a state even if all parameters of the density matrix are known (theoretical), or if one has to perform suitable measurements to comment on the entanglement possessed by an unknown state in the laboratory.

However, there are several information processing tasks for which a measure of entanglement of a quantum state alone is insufficient to provide complete information about the usefulness of the state in the context of these tasks.

In particular, for tasks in which merging of a state is involved, that is—the protocol involves transfer of a quantum state shared between two parties to one of the parties—both a quantification of the correlations present in the state, as well as entropy (information content) of the subsystem that needs to be transferred is necessary.

The Conditional von Neumann Entropy of a state χ^{AB}, given by $S_{A|B}(\chi^{AB}) = S(\chi^{AB}) - S(\chi^{B})$ takes into consideration these two quantities and acts as a precise measure for the usefulness of tasks involving state merging. This can be seen more intuitively when written it is written in terms of mutual information, $S_{A|B}(\chi^{AB}) = S(\chi^{A}) - I[A : B]$. In fact, the amount of quantum resource required to perform state merging is equal to the conditional von Neumann entropy of a state. In the case that this quantity is negative, it means that not only does the state require no resource for state merging, but also that even after completion of the process, further quantum communication is possible via the shared state.

These states with negative quantum conditional entropy are the ones that provide an advantage in information processing tasks such as superdense coding and distributed private randomness distillation.

In this Letter, we prove that the class of states with non-negative conditional von Neumann entropy (CVENN) is convex and compact, with it's boundary being well defined as all the states having 0 conditional von Neumann entropy. Therefore, the useful states lie outside this well-defined class.

We provide a separating hyperplane (a witness) between any state outside of CVENN and the class, making it possible to experimentally comment on the usefulness of an unknown state. We probe into the structure of the density matrix space and take advantage of the closed form boundary to provide analytical witnesses for the class and study the geometry of the class via illustrative examples.

We then discuss the applications, that is, the information processing tasks for which our result is necessary for being able to distinguish useful quantum states from useless ones.

Note: Through out the paper, the inner product used is the matrix inner product, that is, $\langle A, B\rangle = Tr(A^{\dagger}B)$. Both notations have been used interchangably. The norm used is the Frobenius norm, $||A|| = \sqrt{Tr(A^{\dagger}A)}$, and distance between two matrices is given by the norm of their difference. Throughout the paper, CVENN refers to the class of non-negative conditional von Neumann entropy states of a $d \times d$ dimensional bipartite quantum system.

Actual: ρ is any density matrix outside, σ, any density matrix inside, χ, general density matrix. ρ_s, the ρ we want to separate, σ_c is the closest σ, σ_i is the σ at the intersection. χ^{AB}, χ^{A} and χ^{B} refer to the complete matrix χ, and its partial trace wrt the A and B subsystem. Explain:

Characterization of the Class— (i) Conditional von Neumann entropy is a continuous function.[13] By definition, inverse images of continuous functions take closed sets to closed sets. Hence, to prove CVENN is closed, it is sufficient to prove that the range set of conditional von Neumann entropy on CVENN is closed. By definition, $S_{A|B}(\sigma^{AB}) \geq 0 \; \forall \; \sigma^{AB} \in$ CVENN. The value 0 is attained for several states, for example: $|00\rangle\langle 00|$, where $|0\rangle$ refers to any pure state in the d dimensional subsystem. Also, note that we have $S_{A|B}(\chi^{AB}) = S(\chi^{A}) - I[A : B]$ where $I[A : B]$ is the quantum mutual information between χ^{A} and χ^{B}, and is non-negative quantity. Entropy of a d-dimensional system is upper bounded by $log_2 d$, so we have $S(\chi^{A}) \leq log_2 d$. Therefore, $S_{A|B}(\chi^{AB}) \leq log_2 d$. This value is attained for the state I/d^2.

Hence, CVENN is the inverse image of a continuous

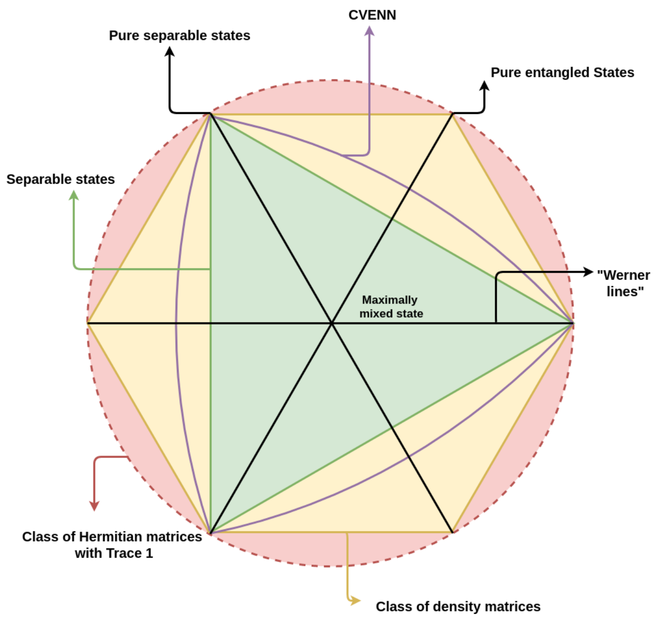

FIG. 1. Schematic diagram of CVENN class

function on a closed set $[0, log_2 d]$. Therefore, CVENN is a closed set.

CVENN is also bounded as every density matrix has a bounded spectrum, that is, their eigenvalues $\in$ [0,1]. Thus, by Heine-Borel theorem, since CVENN is closed and bounded, it is a compact set.

(ii) Consider two states σ_1 $\in$CVENN and σ_2 $\in$CVENN. By definition, we have: $S_{A|B}(\sigma_1) \geq 0$ and $S_{A|B}(\sigma_2) \geq 0$. Consider a convex combination of these two states. As conditional von Neumann Entropy is a concave function [11], we have:

$$S_{A|B}(\lambda\sigma_1 + (1-\lambda)\sigma_2) \geq \lambda S_{A|B}(\sigma_1) + (1-\lambda) S_{A|B}(\sigma_2) \geq 0$$

Therefore, $\lambda\sigma_1 + (1-\lambda)\sigma_2 \in$ CVENN. Thus, CVENN is a convex set.

By Hahn Banach theorem, since CVENN is convex and compact, there exists a hyperplane separating it from any state outside the set.

Numerical witness for CVENN class — A witness for a given set S is defined as a Hermitian operator W with atleast one negative eigenvalue such that (i) $Tr(W\sigma) \geq 0 \ \forall \ \sigma \in S$ and (ii) $\exists \ \rho \notin S$ such that $Tr(W\rho) < 0$.

To numerically find a witness operator W_n separating a state ρ_s from CVENN, given that σ_c is the closest(defined below) CVENN state to ρ_s, we proceed as follows: We consider the expression $e = \langle \chi - \sigma_c, \sigma_c - \rho_s \rangle$ defined at all density matrices χ. We show that (i) $\forall \ \sigma \in S$, $\langle \sigma - \sigma_c, \sigma_c - \rho_s \rangle \geq 0$ and (ii) $\exists \ \rho \notin S$ such that $\langle \rho - \sigma_c, \sigma_c - \rho_s \rangle < 0$. We then find the W_n such that $Tr(W_n\chi) = \langle \chi - \sigma_c, \sigma_c - \rho_s \rangle \ \forall \ \chi$, and thus find the witness.

$$\sigma_c = \arg\min_{\sigma} ||\rho_s - \sigma|| \ \forall \ \sigma \in S$$

Proof (ii) To show that expression e is negative for atleast one point outside the set, we consider the point ρ_s itself, that we wish to separate. It is easy to see that the expression gives a negative value for the point $\chi = \rho_s$ lying outside the set:

$$\langle \chi - \sigma_c, \sigma_c - \rho_s \rangle = \langle \rho_s - \sigma_c, \sigma_c - \rho_s \rangle = -||\rho_s - \sigma_c||^2 < 0$$

as the square of norm of the difference between two different points is always positive.

(i) To prove that the expression e is non-negative for all $\sigma \in S$, we assume otherwise:

$$\exists \sigma' \in S | \langle \sigma' - \sigma_c, \sigma_c - \rho_s \rangle < 0 \tag{1}$$

Within this, we consider two cases. Intuitively, these two cases correspond to having an (i) obtuse or right angle between $\sigma_c - \sigma'$ and $\rho_s - \sigma'$ and having an (ii) acute angle between them as shown in Fig (2) and Fig(3).

Case 1: $\langle \rho_s - \sigma', \sigma_c - \sigma' \rangle \leq 0$. Here, we show that σ' is closer to ρ_s than σ_c, hence leading to a contradiction.

Consider the expression,

$$\langle \rho_s - \sigma_c, \rho_s - \sigma_c \rangle - \langle \rho_s - \sigma', \rho_s - \sigma' \rangle \tag{2}$$

which can be rewritten as:

$$\langle \sigma' - \sigma_c, \sigma' - \sigma_c \rangle - 2\langle \rho_s - \sigma', \sigma_c - \sigma' \rangle$$

We know that $\sigma' \neq \sigma_c$, as that would make the initial assumption 1 untrue. Hence, the first term is always positive by definition of inner product and the second term is non-positive by the assumption in Case 1.

Hence, we have $\langle \rho_s - \sigma_c, \rho_s - \sigma_c \rangle - \langle \rho_s - \sigma', \rho_s - \sigma' \rangle > 0$ or $\sqrt{\langle \rho_s - \sigma_c, \rho_s - \sigma_c \rangle} > \sqrt{\langle \rho_s - \sigma', \rho_s - \sigma' \rangle}$.

Therefore $||\rho_s - \sigma_c|| > ||\rho_s - \sigma'||$, which is a contradiction.

Case 2: $\langle \rho_s - \sigma', \sigma_c - \sigma' \rangle > 0$. Here, we show that there will exist a point σ'' such that Case 1 is satisfied. Then, following the argument present there, σ'' will be closer to ρ_s than σ_c, and the contradiction is attained.

Since, $\sigma' \in S$ and $\sigma_c \in S$, by the convexity of the set S, we have:

$$\forall \lambda \in [0,1], \lambda\sigma_c + (1-\lambda)\sigma' \in S \tag{3}$$

Consider $\lambda' = \frac{\langle \sigma' - \rho_s, \sigma' - \sigma_c \rangle}{\langle \sigma' - \sigma_c, \sigma' - \sigma_c \rangle}$. By the assumption in Case 2, the numerator is positive, and by the definition of inner product, the denominator is positive. Therefore $\lambda' > 0$. When we rewrite λ' as $1 - \frac{\langle \sigma' - \sigma_c, \rho_s - \sigma_c \rangle}{\langle \sigma' - \sigma_c, \sigma' - \sigma_c \rangle}$, by the initial contradiction assumption, the second term is positive, hence $\lambda' < 1$.

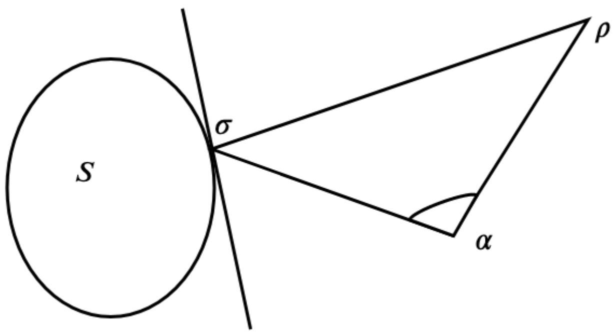

FIG. 2. Case 1: Corresponds to angle at α being obtuse.

Therefore, $\lambda' \in (0,1)$. Consider a state $\sigma'' = \lambda'\sigma_c + (1-\lambda')\sigma'$. Notice that this point belongs to the set S and $\langle \sigma'' - \sigma', \sigma_c - \sigma' \rangle = 0$, therefore satisfying Case 1. Thus both cases lead to a contradiction rendering the initial assumption untrue and all points σ in S satisfy $\langle \sigma - \sigma_c, \sigma_c - \rho_s \rangle \geq 0$.

Remark: Note that a hyperplane of the above form has been used for witnessing entangled states from the separable class of states as given in [2]. We have proved that such a witness can be used for any set as long as it is convex and compact, and hence can also be used for the CVENN class of states. An alternative proof of the same is given in [3], [1].

We now find the witness operator W_n such that $Tr(W_n\chi) = \langle \chi - \sigma_c, \sigma_c - \rho_s \rangle = Tr((\chi - \sigma_c)(\sigma_c - \rho_s))$.

On solving the above, $W_n = Tr(\sigma_c\rho_s - \sigma_c^2)I + \sigma_c - \rho_s$. After normalising, we have:

$$A = \frac{Tr(\sigma_c\rho_s - \sigma_c^2)I + \sigma_c - \rho_s}{\sqrt{Tr(\sigma_c - \rho_s)^2}} \tag{4}$$

Now, it remains that we find σ_c, the closest CVENN state to ρ_s. Note that trace distance $||\rho_s - \sigma||$ is a convex function in σ for a fixed ρ_s, and it needs to be optimised over all $\sigma \in$ the convex set CVENN. Also, unlike the entanglement problem, the conditional von Neumann entropy expression can be evaluated for any given dimension at any state, and membership in CVENN can be tested. Thus, this is a convex optimization problem and there exist several solvers to tackle this. We use MATLAB's CVX solver, a package for specifying and solving convex programs [9], [8] and a few quantum function libraries [6],[5] to find the closest CVENN state for several 2-qubit states.

Examples In the 2×2 dimensional space, consider the state $|\phi^+\rangle\langle\phi^+|$. We find that the closest CVENN state to this state is the following:

$$\begin{bmatrix} 0.4369 & 0 & 0 & 0.3738 \\ 0 & 0.0631 & 0 & 0 \\ 0 & 0 & 0.0631 & 0 \\ 0.3738 & 0 & 0 & 0.4369 \end{bmatrix}$$

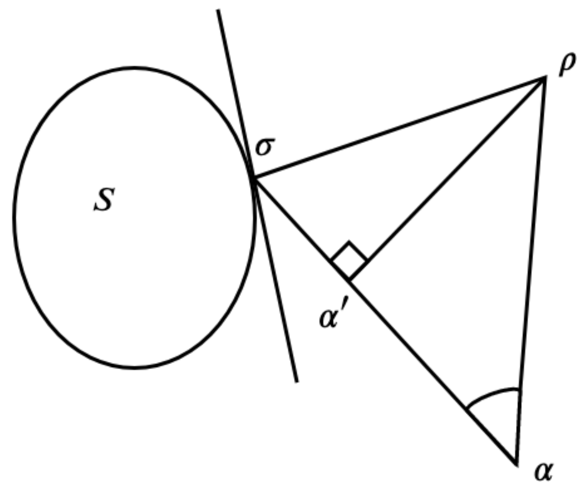

FIG. 3. Case 2: Corresponds to the angle at α being acute.

We note that this is the state where the Werner line $p|\phi^+\rangle\langle\phi^+| + (1-p)I_4$ touches the CVENN class. Therefore, this state is the closest CVENN state for all states with negative conditional entropy that lie on the the given Werner line at $p \approx 0.7476$. Hence the witness created using this state witnesses all negative conditional von Neumann entropy states of the form $p|\phi^+\rangle\langle\phi^+| + (1-p)I_4$.

Applying 4, we find the witness to this state is:

$$W_{nw} = \begin{bmatrix} a & 0 & 0 & c \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ c & 0 & 0 & a \end{bmatrix}$$

where $a = 0.3588$, $b = 0.9361$ and $c = -0.5774$. This state can readily be decomposed in the form of Pauli matrices as follows and be implemented in the laboratory for measurement:

$$W_{nw} = \frac{a+b}{2} I \otimes I + \frac{a-b}{2} Z \otimes Z + \frac{c}{2} X \otimes X - \frac{c}{2} Y \otimes Y$$

We take a state on this Werner line just outside CVENN and look at the action of the witness on it. Consider the state $\rho_w = 0.75|\phi^+\rangle\langle\phi^+| + 0.25I_4$

$$Tr(W_{nw}\rho_w) = -0.0021$$

which is a negative value as it is outside the class, as expected.

We now consider entangled states of the form $|\chi_e\rangle = \frac{a}{\sqrt{1+a^2}}|00\rangle + \frac{1}{\sqrt{1+a^2}}|11\rangle$. When $a = 0$, this is the pure state $|11\rangle$, and when $a = 1$, this is the maximally entangled state $|\phi^+\rangle$.

We then study Werner-like states made from each of these states, $p|\chi_e\rangle\langle\chi_e| + (1-p)I_4$. As expected, we no-

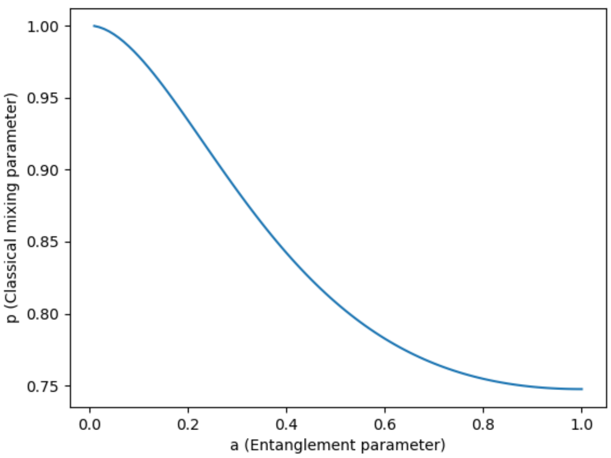

FIG. 4. Mixing parameter at which Werner-like states touch CVENN

tice that the Werner-like states made from more entangled states touch the CVENN class at lower values of the mixing parameter p as shown in 4.

Analytical Witness for CVENN class Analytically, the witness W_a that seprarates a state ρ_s from the CVENN class is given by:

$$W_a = \frac{Tr(\sigma_i g_i)I - g_i}{\sqrt{Tr(g_i)^2}} \tag{5}$$

where σ_i is the state at the intersection of the set of states $\chi = p\rho_s + (1-p)\frac{I}{d^2}$ where $0 \leq p \leq 1$, and the boundary of the CVENN class: $-Tr(\chi log\chi) + Tr(\chi^B log\chi^B) = 0$. The gradient at any σ on the boundary, g is given by:

$$g = (log(\sigma) - I \otimes log(\sigma^B))^T \tag{6}$$

Therefore, the gradient at σ_i, given by g_i is $(log(\sigma_i) - I \otimes log(\sigma_i^B))^T$

Proof structure: To prove the above, (i) we first show that given a state ρ_s, there is a unique solution to the line segment between ρ_s and $\frac{I}{d^2}$, and the boundary of the CVENN class - we call this solution σ_i.(ii) We then find the gradient at the boundary of the class. (iii) We show that the gradient always exists at such a point σ_i. (iv) We use this gradient to find the tangent (or supporting hyperplane) at σ_i and hence the witness W_a. (v) We prove that the hyperplane obtained separates the point ρ_s from the class.

Proof (i) Firstly, note that no supporting hyperplane of a set passes through an interior point of the set as an interior point has an open neighbourhood around it in all directions that belongs to the set, and a hyperplane through the point will necessary separate points that belong in the set and cannot be a supporting hyperplane. Proof by contradiction: Consider the case where there is more than one solution to the system of equations, that is, the line $p\rho_s + (1-p)\frac{I}{d^2}$ touches the boundary of CVENN $-Tr(\chi log\chi) + Tr(\chi^B log\chi^B) = 0$ at more than one point. Let these points be $b_1, b_2...$ and so on where b_1 is the point closest to $\frac{I}{d^2}$. If b_1 is a boundary point, then by the definition of a convex set, a supporting hyperplane must exist at b_1. Let this hyperplane be h. Note that as this is a convex, compact set, both b_2 and $\frac{I}{d^2}$ must lie on the same side of this hyperplane. Since b_1 lies on the line joining b_2 and $\frac{I}{d^2}$,we have $b_1 = pb_2 + (1-p)\frac{I}{d^2}$. Since it also lies on h, we have $\langle h, b_1\rangle = 0 \Rightarrow \langle h, pb_2 + (1-p)\frac{I}{d^2}\rangle = 0 \Rightarrow p\langle h, b_2\rangle + (1-p)\langle h, \frac{I}{d^2}\rangle = 0$. where $0 < p < 1$. Since both b_2 and $\frac{I}{d^2}$ must lie on the same side of the plane, we have either $\langle h, b_2\rangle$ and $\langle h, \frac{I}{d^2}\rangle$, both must be ≥ 0 or both ≤ 0. Therefore, the only possibility is $\langle h, b_2\rangle = 0$ and $\langle h, \frac{I}{d^2}\rangle = 0$. Therefore, both points lie on the plane. However, this is a contradiction as interior point $\frac{I}{d^2}$ cannot lie on a supporting hyperplane. Therefore, the line $p\rho_s + (1-p)\frac{I}{d^2}$ touches the boundary at only one point σ_i.

(ii) Let e_i be the basis vectors for a d dimensional system. $E_i = I_d \otimes e_i$ where I_d is the $d \times d$ identity matrix. Then, the reduced density matrix σ^B for the $d \times d$ system σ can be represented as follows:

$$\begin{aligned}
\sigma^B &= Tr_A(\sigma) \\
&= \sum_{ij} e_i e_j^T \left(\sum_k \langle ki|\sigma|kj\rangle \right) \\
&= \sum_{ij} e_i e_j^T \sum_k Tr\left(|kj\rangle\langle ki|\sigma\right) \\
&= \sum_{ij} e_i e_j^T \sum_k Tr(|k\rangle\langle k| \otimes |j\rangle\langle i|\sigma) \\
&= \sum_{ij} e_i e_j^T Tr(I \otimes |j\rangle\langle i|\sigma) \\
&= \sum_{ij} e_i e_j^T Tr(I \otimes e_j e_i^T \sigma) \\
&= \sum_{ij} e_i e_j^T Tr((I \otimes e_j)(I \otimes e_i^T)\sigma) \\
&= \sum_{ij} e_i e_j^T Tr(E_j E_i^T \sigma)
\end{aligned}$$

Using Einstein notation, and using the notation: $A : B \equiv Tr(A^T B)$ we have,

$$\sigma^B = e_i e_j^T (E_i E_j^T : \sigma)$$

In this notation, note that we have, if $\phi = Tr(Alog(A))$ then $d\phi = (log(A) + I)^T : dA$. The gradient of the entropy function f is given below:

$$\begin{aligned}
f &= Tr(\sigma log(\sigma) - Tr(\sigma^B log\sigma^B)) \\
df &= Tr(log(\sigma)^T + I \otimes I) : d\sigma - (log(\sigma^B)^T + I) : d\sigma^B \\
&= (log(\sigma)^T + I \otimes I) : d\sigma \\
&\quad - (log(\sigma^B)^T + I) : e_i e_j^T (E_i E_j^T : d\sigma) \\
&= (log(\sigma)^T + I \otimes I) : d\sigma \\
&\quad - (e_i^T log(\sigma^B)^T e_j + \delta_{ij})(E_i E_j^T : d\sigma) \\
\frac{df}{d\sigma} &= log(\sigma)^T + I \otimes I - e_i^T log(\sigma^B)^T e_j E_i E_j^T - E_i E_j^T \\
&= log(\sigma)^T - e_i^T log(\sigma^B)^T e_j E_i E_j^T - E_i E_j^T \\
&= log(\sigma)^T - e_i^T log(\sigma^B)^T e_j E_i E_j^T \\
&= log(\sigma)^T - e_i^T log(\sigma^B)^T e_j (e_i e_j^T \otimes I) \\
&= \left(log(\sigma) - I \otimes log(\sigma^B)\right)^T
\end{aligned}$$

(iii) The state $\sigma_i = p\rho_s + (1-p)\frac{I}{d^2}$ can be written in the diagonal basis of ρ_s. Since ρ_s is also a density matrix, let its eigenvalues be a_1,a_2,a_3 and a_4 where $a_i \geq 0$. Therefore the eigenvalues of σ_i are all of the form $s_i = (1-p)\frac{1}{d^2} + pa_i$. Since $p < 1$, $s_i > 0$. Hence log is defined at σ_i and hence the gradient is defined (need to check for σ^B).

(iv) Given the gradient g_i, the supporting hyperplane constitutes all points χ such that $\langle g_i, \chi - \sigma_i\rangle = 0$. To find the witness operator W_a, while adjusting for sign convention, we have

$$\begin{aligned}
\langle W_a, \chi\rangle &= \langle g_i, \sigma_i - \chi\rangle \\
Tr(W_a\chi) &= Tr(g_i(\sigma_i - \chi)) \\
&= Tr(g_i\sigma_i - g_i\chi) \\
&= Tr(g_i\sigma_i) - Tr(g_i\chi) \\
&= Tr((Tr(g_i\sigma)I - g_i)\chi)
\end{aligned}$$

Therefore, after normalization, we have

$$W_a = \frac{Tr(\sigma_i g_i)I - g_i}{\sqrt{Tr(g_i)^2}}$$

(v) (Prove that $Tr(W_a\rho_s)$ always gives a negative value. That is, prove that $-Tr((\rho_s - \sigma_i)g_i)$ is always negative.)

Examples Consider isotropic states in any dimension d. To find the state at which the line $\alpha|\phi^+\rangle\langle\phi^+| + (1-\alpha)\frac{I}{d^2}$ touches the boundary of the CVENN class, we find an expression for the entropy of the system, and the entropy of the subsystem:

Note: The state $|\phi^+\rangle$ in d dimensions refers to:

$$\frac{1}{\sqrt{d}}\left(\sum_{j=1}^{d} |j\rangle \otimes |j\rangle\right)$$

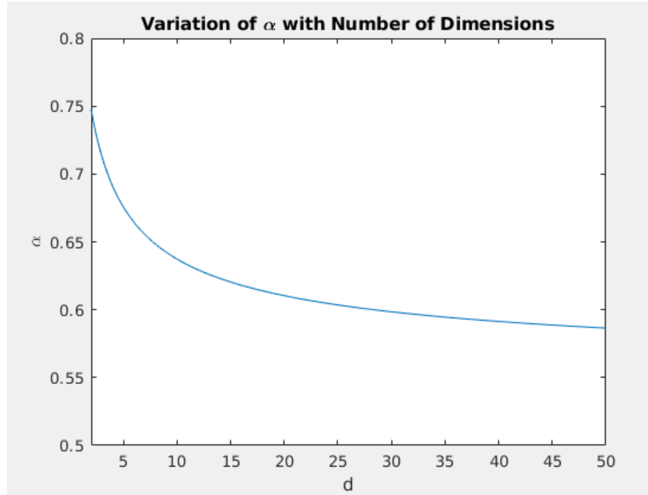

FIG. 5. Variation of α, the mixing parameter, with d, the number of dimensions

In the diagonal basis of $|\phi^+\rangle\langle\phi^+|$, we notice we have one eigenvalue of the form $\alpha(1) + (1-\alpha)\frac{1}{d^2}$ and $d^2 - 1$ eigenvalues of the form $(1-\alpha)\frac{1}{d^2}$.

Therefore the entropy of the system is:

$$-\left(\frac{1-\alpha}{d^2} + \alpha\right) log\left(\frac{1-\alpha}{d^2} + \alpha\right) - (d^2-1)\frac{(1-\alpha)}{d^2} log\left(\frac{1-\alpha}{d^2}\right)$$

Notice that the subsystem is always $\frac{I}{d}$ where I is the identity matrix in $d \times d$ dimensions. Therefore the entropy of the subsystem is always $log(d)$. For a given dimension d, we need to find α such that:

$$-\left(\frac{1-\alpha}{d^2} + \alpha\right) log\left(\frac{1-\alpha}{d^2} + \alpha\right) - (d^2-1)\frac{(1-\alpha)}{d^2} log\left(\frac{1-\alpha}{d^2}\right) - log(d) = 0$$

The graph for the variation of α as the number of dimensions increases is shown in Fig(5)

For a 3×3 system, we find that $\alpha = 0.7129$. Using this, we find σ_i, and therefore find the witness is: $W_{ai} = a(|00\rangle\langle00| + |11\rangle\langle11| + |22\rangle\langle22|) + b(|01\rangle\langle01| + |02\rangle\langle02| + |10\rangle\langle10| + |12\rangle\langle12| + |20\rangle\langle20| + |21\rangle\langle21|) + c(|00\rangle\langle11| + |00\rangle\langle22| + |11\rangle\langle00| + |11\rangle\langle22| + |22\rangle\langle00| + |22\rangle\langle11|)$

where $a = 0.0721, b = 0.1306$ and $c = -0.0584$

The Gell-Mann basis vectors are as follows: $\lambda_1, \lambda_2, \lambda_3 ... \lambda_8$ as defined here and the 3×3 Identity matrix I. For measurement in the lab, the above witness can easily be decomposed into the Gell-Mann basis, and is infact diagonal in the basis:

$W_{ai} = -a\lambda_1 \otimes \lambda_1 + a\lambda_2 \otimes \lambda_2 - b\lambda_3 \otimes \lambda_3 - a\lambda_4 \otimes \lambda_4 + a\lambda_5 \otimes \lambda_5 - a\lambda_6 \otimes \lambda_6 + a\lambda_7 \otimes \lambda_7 - b\lambda_8 \otimes \lambda_8 + I_3 \otimes I_3$

where $a = 0.02920, b = 0.02925$ and $c = 0.1111$

Applications Conditional von Neumann Entropy gets its operational meaning from state merging [10]. State merging refers to the complete transfer of a state that has been divided among two parties to one party. The amount of quantum resource required for such a transfer is equal to the Conditional von Neumann entropy of the state. When this quantity is negative, asymptotically, it means that not only does it take no resource to perform state merging, but also that extra resource is left over after the process for further quantum communication.

State merging makes the assumption that if the shared state is pure, it can always be prepared locally. However, if the shared state is mixed, then it may be correlated with another state, and this correlation needs to be maintained. Hence quantum resource may be required to teleport the state or apply some other protocol to maintain external correlation.

Not only does state merging give an operational meaning to conditional von Neumann entropy, it also gives an intuitive understanding of the possible applications for which calculation of von Neumann entropy of a state gives the efficiency attained when the state is used in an information processing task. Superdense coding and private distributed randomness generation, two applications that have been discussed below, both contain state merging in some sense as part of their protocols.

Superdense Coding: Given a shared state between two parties, superdense coding is the ability to convey more than $log_2 d$ bits worth of information while performing local operations and sending only a d-dimensional subsystem across [4].

The superdense coding capacity for a mixed state ρ_{AB} in $D(H_d \otimes H_d)$ is defined by [12]:

$$C_{AB} = max\{log_2 d, log_2 d + S(\rho_B) - S(\rho_{AB})\}$$

Therefore states with negative conditional von Neumann entropy give non-zero advantage while performing superdense coding.

As shown above, we have provided a witness to recognise if a state is dense codable or not.

Distributed Private Randomness Distillation The Private Randomness Distribution problem setting is as follows: Assuming a state ρ_{AE} is shared between Alice and Eve, how much randomness can Alice extract from her state without Eve's knowledge?

The distributed setting of the same problem assumes another party, Bob is in possession of the purification ρ_{ABE} of the state ρ_{AE} [14]. Then, given that Alice and Bob are allowed to cooperate, how much independent randomness can each of them extract without Eve's knowledge?

Notice that these problems are well motivated, as Eve may be a malicious dealer claiming to provide randomness devices, while actually correlating them with states in her possession.

It is noticed that local noise, that is, the local mixed subsystem of a maximally entangled state, which is usually useless for distilling private randomness can prove to be useful if combinedly measured with another such state shared with another party, effectively performing entanglement swapping.

Yang, Horodecki and Winter, in their publication on distributed private randomness distillation provide a protocol called Virtual Quantum State Merging (VQSM) to increase local noise, and hence increase the amount of randomness that is privately distillable.

States that do not require external resource to perform VQSM are in fact states with negative conditional von Neumann entropy.

By providing a witness for CVENN, we are able to witness states that have an advantage in this protocol that then helps increase the randomness distillable by Alice and Bob.

[1] Reinhold A. Bertlmann, Katharina Durstberger, Beatrix Hiesmayr, and Philipp Krammer. Optimal entanglement witnesses for qubits and qutrits. *Physical Review A*, 72, 08 2005.

[2] Reinhold A. Bertlmann and Philipp Krammer. Entanglement witnesses and geometry of entanglement of two-qutrit states. *Annals of Physics*, 324:1388–1407, 07 2009.

[3] RA Bertlmann, Heide Narnhofer, and W Thirring. A geometric picture of entanglement and bell inequalities. *Physical Review A*, 66, 11 2001.

[4] D. Bruß, G. M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sende, and U. Sen. Distributed Quantum Dense Coding. *Phys. Rev. Lett.*, 93(21):210501, Nov 2004.

[5] Tony Cubitt. Quantinf package.

[6] Hamza Fawzi, James Saunderson, and Pablo A. Parrilo. Semidefinite approximations of the matrix logarithm. *Foundations of Computational Mathematics*, 2018. Package cvxquad at `https://github.com/hfawzi/cvxquad`.

[7] Leonid Gervitz. Classical complexity and quantum entanglement. *ScienceDirect*.

[8] Michael Grant and Stephen Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. `http://stanford.edu/~boyd/graph_dcp.html`.

[9] Michael Grant and Stephen Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. `http://cvxr.com/cvx`, March 2014.

[10] MichałHorodecki, Jonathan Oppenheim, and Andreas

Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1):107–136, Jan 2007.

[11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[12] Subhasree Patro, Indranil Chakrabarty, and Nirman Ganguly. Non-negativity of conditional von Neumann entropy and global unitary operations. *Phys. Rev. A*, 96(6):062102, Dec 2017.

[13] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347, 07 2015.

[14] Dong Yang, Karol Horodecki, and Andreas Winter. Distributed private randomness distillation. *arXiv e-prints*, page arXiv:1803.09989, Mar 2018.