Tip of the Quantum Entropy Cone

Christandl, Matthias; Durhuus, Bergfinnur; Wolff, Lasse Harboe

Published in:
Physical Review Letters

DOI:
10.1103/PhysRevLett.131.240201

Publication date:
2023

Document version
Publisher's PDF, also known as Version of record

Document license:
CC BY

Citation for published version (APA):
Tip of the Quantum Entropy Cone

Matthias Christandl, Bergfinnur Durhuus, and Lasse Harboe Wolff

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Denmark

(Received 13 June 2023; accepted 30 October 2023; published 13 December 2023)

Relations among von Neumann entropies of different parts of an $N$-partite quantum system have direct impact on our understanding of diverse situations ranging from spin systems to quantum coding theory and black holes. Best formulated in terms of the set $\Sigma_N$ of possible vectors comprising the entropies of the whole and its parts, the famous strong subadditivity inequality constrains its closure $\overline{\Sigma_N}$, which is a convex cone. Further homogeneous constrained inequalities are also known. In this Letter we provide (nonhomogeneous) inequalities that constrain $\Sigma_N$ near the apex (the vector of zero entropies) of $\overline{\Sigma_N}$, in particular showing that $\Sigma_N$ is not a cone for $N \geq 3$. Our inequalities apply to vectors with certain entropy constraints saturated and, in particular, they show that while it is always possible to upscale an entropy vector to arbitrary integer multiples it is not always possible to downscale it to arbitrarily small size, thus answering a question posed by Winter.

DOI: 10.1103/PhysRevLett.131.240201

Introduction.—Entropy is a very important concept in physics, whose role and status have vastly expanded past its original boundaries within thermodynamics. It is a main object of study in many areas of research, including quantum cryptography, information theory, black holes, and more.

In models of the world, it is often very advantageous and natural to consider large systems as composed of smaller distinct subsystems. This calls for a good understanding of the relations among entropies of different subsystems of a joint system. The most important such relation is without a doubt the strong subadditivity inequality [1], which entails all other known entropy inequalities for multipartite quantum systems and has long been appreciated in quantum information theory. There has naturally been a great interest in finding new such inequalities. The problem of finding new entropy inequalities is an aspect of a more general research endeavour to adequately describe the set of possible values that the different allocations of entropy in a multipartite system can take, i.e., to determine whether or not any given ordered set of numbers corresponds to an achievable entropy vector, by which we mean the entropy values of the marginals of some quantum state.

In this Letter, we prove a new relationship between the entropies of a multipartite system, which rules out the possibility of constructing certain small entropy vectors that otherwise satisfy strong subadditivity and related inequalities. This result, interestingly, entails that the set of achievable entropy vectors is neither a cone nor a closed set—thus answering a question left open in an influential paper by Pippenger [2]. We additionally discuss applications of the new results to a diverse set of areas—namely, topological materials, entanglement theory, and quantum cryptography.

In the remainder of this introduction, we shall introduce some necessary notation and relevant background concerning the quantum entropy cone. The main results are presented in the following section, after which we discuss some applications and provide a conclusion and outlook for this Letter.

Given a quantum system $X$ in a state described by a density operator $\rho$, i.e., a non-negative operator of trace 1 on a (finite dimensional) Hilbert space $\mathcal{H}_X$, its von Neumann entropy is given by

$$H_\rho = -\text{Tr}[\rho \log(\rho)] = -\sum_i \lambda_i \log(\lambda_i),$$

where $\lambda_i$ are the eigenvalues of $\rho$, and log denotes the binary logarithm. We shall be concerned with multipartite systems $\mathcal{N}$ consisting of $N$ constituent systems $X_1, \ldots, X_N$ with associated Hilbert spaces $\mathcal{H}_{X_1}, \ldots, \mathcal{H}_{X_N}$, such that the state of $\mathcal{N}$ is given by a density operator $\rho$ on $\mathcal{H}_{X_1} \otimes \cdots \otimes \mathcal{H}_{X_N}$. The reduced state of a subsystem $\mathcal{A} \subseteq \mathcal{N}$ is then given by

$$\rho_\mathcal{A} := \text{Tr}_{\mathcal{N}\setminus\mathcal{A}}[\rho],$$

where $\text{Tr}_{\mathcal{N}\setminus\mathcal{A}}[\cdot]$ denotes the partial trace over $\otimes_{X_i \notin \mathcal{A}} \mathcal{H}_{X_i}$ (and in particular $\rho = \rho_\mathcal{N}$). The entropy $H_{\rho_\mathcal{A}}$ of the reduced
state will also be denoted by $H(\mathcal{X})_\rho$ or by $H(X_i\ldots X_n)_\rho$ if $\mathcal{X} = \{X_1,\ldots,X_n\}$. These marginal entropies define a vector $\vec{H}_\rho \in \mathbb{R}^{2^n-1}$, called the entropy vector of $\rho$, whose coordinates are labeled by the nonempty subsystems of $\mathcal{N}$. E.g., for $N = 2$ and $\mathcal{N} = \{A,B\}$ we have $\vec{H}_\rho = [H(A), H(B), H(AB)]_\rho \in \mathbb{R}^3$, while for $N = 3$ and $\mathcal{N} = \{A,B,C\}$ we write

$$\vec{H}_\rho = [H(A), H(B), H(C), H(BC), H(AC), H(AB), H(ABC)]_\rho \in \mathbb{R}^7. \quad (2)$$

The main object of study in this context is the set $\Sigma_N$ of all possible entropy vectors associated to $N$-partite systems,

$$\Sigma_N = \{\vec{H}_\rho \in \mathbb{R}^{2^n-1}| \rho \text{ is a density operator on } \mathcal{N}\}.$$

It is a fundamental result of Pippenger [2] that the topological closure $\Sigma^\beta_N$ of $\Sigma_N$ in $\mathbb{R}^{2^n-1}$ is a convex cone, called the quantum entropy cone of $N$-partite systems, i.e., $\Sigma^\beta_N$ is closed under addition and under multiplication by positive scalars. It is also known, and easy to demonstrate, that $\Sigma^\beta_N$ has full dimension, i.e., it spans all of $\mathbb{R}^{2^n-1}$ as a vector space, and that $\Sigma_N$ and $\Sigma^\beta_N$ have identical interiors and hence also identical boundaries. For $N = 2$ it is even true that $\Sigma^\beta_N = \Sigma_N$ as will be commented on further below. But for general $N \geq 3$ an appropriate characterization of the boundary entropy vectors is missing [3].

A related but different long-standing problem is to determine whether or not $\Sigma^\beta_N$ is a polyhedral cone, i.e., if it can be specified in terms of a finite number of linear inequalities. The known general inequalities of this sort are of two types:

$$H(\mathcal{X}) + H(\mathcal{Y}) \geq H(\mathcal{X} \cap \mathcal{Y}) + H(\mathcal{X} \cup \mathcal{Y}), \quad (3)$$

$$H(\mathcal{X}) + H(\mathcal{Y}) \geq H(\mathcal{X}\backslash \mathcal{Y}) + H(\mathcal{Y}\backslash \mathcal{X}), \quad (4)$$

called strong subadditivity and weak monotonicity, respectively. Here, $\mathcal{X}$ and $\mathcal{Y}$ are arbitrary subsystems, and by convention we have $H(\emptyset) = 0$. We emphasize that not all inequalities of the forms above are independent. Strong subadditivity was first established in [5], but a variety of proofs exist in the literature, see, e.g., Refs. [1,6–10]. To obtain weak monotonicity one makes use of the fact, referred to as purification [8], that given a state $\rho$ of $\mathcal{N}$ it is always possible to extend $\mathcal{N}$ by a system $Y$ and to define a pure state $\eta = |Y\rangle\langle Y|$ of $\mathcal{N} \cup Y$ such that $\rho = \eta_N$.

The polyhedral cone defined by (3) and (4) is a closed convex cone, and will here be denoted $\Sigma_N$. The question of whether $\Sigma_N = \Sigma^\beta_N$, or if there exist further independent linear inequalities beyond (3) and (4), remains open for $N \geq 4$. For $N \leq 3$ the two closed cones coincide as shown in [2]. While it is quite easy to see that $\Sigma_N = \Sigma^\beta_N = \Sigma_N$ hold for $N \leq 2$, the case $N \geq 3$ is different. It has been shown that for $N \geq 4$ there exist further constrained homogeneous linear inequalities [11–13].

We shall now delve a bit deeper into the details of the case $N = 3$, where the relevant inequalities are

$$I_{XY} := H(X) + H(Y) - H(XY) \geq 0, \quad (5)$$

$$I_{XY} := H(XZ) + H(YZ) - H(Z) - H(XYZ) \geq 0, \quad (6)$$

$$I_{XY} := H(Z) + H(XYZ) - H(XY) \geq 0, \quad (7)$$

$$I_{XY} := H(XZ) + H(YZ) - H(X) - H(Y) \geq 0, \quad (8)$$

valid for $\{X,Y\}$ equaling $\{A,B\}$, $\{A,C\}$, or $\{B,C\}$ with $Z \neq X,Y$. This makes a total of twelve inequalities, three of each type. A key observation is that

$$M := I_{XY} - I_{XY} = II_{XY} - IV_{XY} \quad (9)$$

is independent of the choice of $\{X,Y\}$. It follows that $\Sigma_3$ is a union of two cones

$$\Sigma^+_3 : I_{XY} \geq 0, \quad IV_{XY} \geq 0, \quad M \geq 0, \quad (10)$$

$$\Sigma^-_3 : I_{XY} \geq 0, \quad III_{XY} \geq 0, \quad M \leq 0, \quad (11)$$

each of which has seven facets, corresponding to their seven defining inequalities. By a slight elaboration of Pippenger’s approach [2] it can be shown that $\Sigma^+_3 \subset \Sigma^\beta_3$, while $\Sigma^-_3$ behaves differently. For any $\vec{H} \in \Sigma^-_3$ one finds that there exists a quantum state $\rho$ and a vector $\vec{l}$ belonging to the one-dimensional face (half-line) $\vec{e}$ of $\Sigma^-_3$ defined by the six equations

$$\vec{e} : I_{XY} = 0, \quad III_{XY} = 0, \quad (12)$$

such that

$$\vec{H} = \vec{l} + \vec{H}_\rho. \quad (13)$$

If it so happened that $\vec{e} \subset \Sigma^+_3$, it would follow by the additivity of entropy vectors in suitably constructed product states that $\Sigma^+_3 \subset \Sigma^+_3$, and hence that $\Sigma_3 = \Sigma^+_3$. However, as a consequence of Theorem 1 below there is an open line segment of $\vec{e}$ ending at the apex which is not contained in $\Sigma^+_3$, and so $\Sigma_3 \neq \Sigma^+_3$. On the other hand, Pippenger identifies a state $\rho'$ such that $\vec{H}_\rho' \in \vec{e}$, which by the cone property implies that $\vec{e} \subset \Sigma^\beta_3$. Using (9) one then obtains that $\Sigma^-_3 \subset \Sigma^\beta_3$, and, consequently, $\Sigma_3 = \Sigma^\beta_3$, which is the already mentioned main result of [2].

In order to satisfy (8), the entropy vector $\vec{H}_\rho'$ must satisfy

$$I(X;Y)_\rho' = 0, \quad H(X)_\rho' + H(XYZ)_\rho' = H(YZ)_\rho', \quad (14)$$

240201-2
for any pair \( \{X, Y\} \) in \( \mathcal{N} = \{A, B, C\} \) with \( Z \neq X, Y \), where the more standard notation \( I(X:Y) \) has been used instead of \( I_{XY} \) for the quantum mutual information. By purification one can alternatively consider a state \( \eta = |V\rangle\langle V| \) on a 4-partite system \( \{A, B, C, D\} \) such that \( \rho^l = \eta^N \). Such a pure state makes the equations (10) take on the more symmetric form

\[
I(X_i; X_j)_\eta = 0
\]

(11)

for all pairs \( X_i, X_j \) in \( \{A, B, C, D\} \). Indeed, the state \( \rho^l \) is obtained in [2] by first constructing such a pure state \( \eta \). Our main theorem below concerns pure states of arbitrary \( N \)-partite systems that fulfill the conditions (11) for fixed \( i \), showing that sufficiently small scalar multiples of their entropy vectors lie outside \( \Sigma_N \), i.e., cannot be realized by quantum states. For the sake of completeness we exhibit in the Supplemental Material [14], for arbitrary \( N \geq 4 \), states which fulfill the stated conditions, and thus generalizing the pure state \( \eta \) mentioned above.

**Main results.**—The goal of this section is to establish the following entropy bound.

**Theorem 1.**—Let \( \rho \) be a pure state of the \( N \)-partite system \( \mathcal{N} = \{X_1, \ldots, X_N\} \) such that \( H(X_i)_\rho \neq 0 \). Suppose further that

\[
I(X_1; X_i)_\rho = 0 \quad \text{for all } i = 2, \ldots, N.
\]

Then the following bound holds:

\[
\sum_{i=1}^{N} H(X_i)_\rho > 1.
\]

(12)

The conditions in the theorem are illustrated in Fig. 1. Note that they can only be satisfied if \( N \geq 4 \).

To establish Theorem 1, we first list three lemmas below which are the main ingredients in the subsequent proof. Their demonstrations are provided in Sec. A of the Supplemental Material [14]. We will use the following notation. Given a state \( \rho \) of \( \mathcal{N} \), we denote by \( \lambda_1^i \geq \lambda_2^i \geq \ldots \) the eigenvalues of \( \rho_{X_i} \) in decreasing order and by \( |e_1^i \rangle, |e_2^i \rangle, \ldots \) a corresponding orthonormal eigenstate basis

\[
\begin{align*}
\bullet & \quad \ldots \quad \bullet \\
X_1 & \quad \leftrightarrow \quad X_2 \quad \leftrightarrow \quad \ldots \quad \leftrightarrow \quad X_N-1 \\
\text{X} & \quad \leftrightarrow \quad \text{X} \quad \leftrightarrow \quad \text{X} \quad \leftrightarrow \quad \text{X} \\
X_1 & \quad \leftrightarrow \quad X_2 \quad \leftrightarrow \quad \ldots \quad \leftrightarrow \quad X_N
\end{align*}
\]

FIG. 1. The conditions of Theorem 1 are here represented with each circle denoting a constituent system \( X_i \). The double lines indicate that the mutual information between the two systems is 0, and it is assumed that the total state is pure.

such that

\[
\langle \rho_{X_i} \rangle_{ab} := \langle e_a^i | \rho_{X_i} | e_b^i \rangle = \lambda_a^i \delta_{ab}.
\]

(13)

Moreover, we define

\[
e_i := 1 - \lambda_i^i \quad \text{and} \quad \epsilon := \sum_{i=1}^{N} e_i.
\]

(14)

Clearly, \( \sum_{x_i \geq 1} \lambda_x^i = e_i \) and one easily verifies that

\[
H(X_i) \geq \max \{h(e_i), -\log(1 - e_i)\} \geq 2e_i,
\]

(15)

where \( h \) denotes the binary entropy function,

\[
h(x) = -x \log x - (1 - x) \log (1 - x).
\]

Assuming \( \rho \) to be pure, i.e., \( \rho = |V\rangle\langle V| \) where \( \langle V|V\rangle = 1 \), we represent \( |V\rangle \) with respect to the basis for \( \mathcal{H}_N \) consisting of tensor products of eigenstates \( |e_a^i \rangle \) for the single-party density matrices; that is

\[
|V\rangle = \sum_{x_1, \ldots, x_N} V_{x_1 \ldots x_N} |e_{x_1}^1 \ldots e_{x_N}^N\rangle,
\]

(16)

where

\[
\sum_{x_1, \ldots, x_N} |V_{x_1 \ldots x_N}|^2 = 1.
\]

(17)

A sum over dummy indices \( x_i \in \mathbb{N} \) will here always run up to \( \dim(\mathcal{H}_{X_i}) \). The matrix elements of \( \rho_{X_i} \) and the reduced states are quadratic expressions of the components of \( |V\rangle \); e.g.,

\[
\langle \rho_{X_1} \rangle_{ab} := \sum_{x_2, \ldots, x_N} V_{x_2 \ldots x_N}^a V_{x_2 \ldots x_N}^b.
\]

(18)

\[
\langle \rho_{X_1 X_2} \rangle_{a_1 a_2 b_1 b_2} := \sum_{x_3, \ldots, x_N} V_{a_1 a_2 x_3 \ldots x_N}^a V_{b_1 b_2 x_3 \ldots x_N}^b.
\]

(19)

Extensive use will be made of the fact that \( I(X_i; X_j) = 0 \) holds if and only if \( \rho_{X_i X_j} \) is a product state, which in our notation and choice of basis means that

\[
\langle \rho_{X_i X_j} \rangle_{a_1 a_2 b_1 b_2} = \lambda_{a_1} \lambda_{a_2} \delta_{a_1 b_1} \delta_{a_2 b_2}.
\]

(20)

The announced lemmas relate the \( e_i \)'s to the components of \( V \) as follows.

**Lemma 1.**—For any pure state \( \rho \) it holds that

\[
|V_1| \geq 1 - \epsilon.
\]

(21)
Lemma 2.—For any pure state $\rho$ such that $I(X_1 : X_j) = 0$ for all $j \neq 1$ we have

$$\sum_{x_1 > 1} |V_{x_1 \ldots 1}|^2 \geq \epsilon_1 (1 + \epsilon_1 - \epsilon).$$  \hspace{1cm} (22)

Lemma 3.—For any pure state $\rho$ it holds that

$$(1 - \epsilon_1)\sum_{x_1 > 1} |V_{x_1 \ldots 1}|^2 \leq \epsilon_1 (\epsilon - \epsilon_1).$$  \hspace{1cm} (23)

We remark that Lemma 1 is used for the proof of Lemma 3, while only Lemma 2 and Lemma 3 are used in the proof of Theorem 1.

Proof of Theorem 1.—Combining Lemma 2 and Lemma 3 we get

$$(1 - \epsilon_1)\epsilon_1 (1 + \epsilon_1 - \epsilon) \leq \epsilon_1 (\epsilon - \epsilon_1).$$

Since $\epsilon_1 > 0$ as a consequence of the assumption $H(X_1) \neq 0$, this is equivalent to

$$1 + (1 + \epsilon - \epsilon_1)\epsilon_1 \leq 2\epsilon.$$

Since the left-hand side of this inequality is larger than 1, it follows that $\epsilon > \frac{1}{2}$ which in turn implies (12) by use of (15) and the definition of $\epsilon$. This completes the proof of Theorem 1.

In case the given state $\rho$ is not pure, we can apply Theorem 1 to its purification and obtain (see Sec. B of the Supplemental Material [14] for more details).

Corollary 1.—Let $\vec{H}$ be a realizable entropy vector for a system $\mathcal{N} = \{X_1, \ldots, X_N\}$ which fulfills

$$H(\mathcal{N}) > 0 \quad \text{and} \quad H(X_i) + H(\mathcal{N}) = H(\mathcal{N}\setminus X_i)$$

for all $i \in \{1, \ldots, N\}$. Then the following bound holds:

$$H(\mathcal{N}) + \sum_{i=1}^{N} H(X_i) > 1.$$  \hspace{1cm} (24)

We note that the conditions in the corollary can be satisfied if $N \geq 3$. This result excludes a range of vectors in $\Sigma_N$ from $\Sigma_N$ that satisfy $N$ linear constraints and hence can be labeled by $2^N - N - 1$ parameters. See Fig. 2 for a visualization in case $N = 3$. In Sec. C of the Supplemental Material [14] we provide a four-parameter family of realizable entropy vectors on the boundary of $\Sigma_N$ satisfying the conditions of the corollary.

Applications.—The entropy concept itself originally arose from thermodynamical considerations of macroscopic systems consisting of many particles, such as gases. Quantum correlations of such systems can be quantified in terms of the scaling of the entanglement entropy, that is the entropy of a subregion $A$. It has been found for many systems that this entropy is roughly proportional to the size of the boundary $\partial A$ and not to the volume, a statement known as the area law [15]. For topologically ordered systems it is expected that

$$H(A) = a|\partial A| - \gamma$$

up to terms vanishing as the “area” $|\partial A|$ gets large. Moreover, the constant additive term $-\gamma$ is expected to be universal and is dubbed the topological entanglement entropy. Actually, $\gamma$ equals an alternating sum of entropies, called $M_1$, encountered above in (5). As shown in [16,17] the value of $\gamma$ in a class of systems is always positive, and $M_1$ is thus negative. This is precisely the regime in which we identified restrictions on entropy vectors and they may therefore have implications for the attainable values of the topological entropy. We point out, however, that the entropy vectors of the particular finite systems calculated in [16,17] in terms of their total quantum dimension do not satisfy the conditions of our theorem. Also, as the constraints we obtained are not balanced [12], our results have no direct bearing on the usual situation when a large system size is considered.

Many functions in quantum information theory are defined in terms of optimizations of von Neumann entropies [18] or even optimization with entropic constraints [19]. An example from entanglement theory is the squashed entanglement [20]

$$E_{sq}(\rho_{AB}) = \inf \frac{1}{2} \left( I(A : BE)_{\rho} - I(A : B)_{\rho} \right),$$

where the minimization is over extensions $\rho_{ABE}$ of $\rho_{AB}$. The results of the present work constrain such optimization and
it remains to be explored whether they could lead to simplified computations in specific cases.

Finally, let us consider a cryptographic situation, known as quantum secret sharing [21–23]: Alice (A) wishes to distribute information to $N - 1$ parties ($N \geq 4$) (i) purely, in the sense that the overall state of her and the constituent systems is pure (ii) secretly, in the sense that every share is in product with hers (iii) nontrivially, in the sense that $H(A) > 0$. These are precisely the conditions of Theorem 1 and thus it follows from our Letter that she cannot do so unless the average share carries a minimum entropy, equal to $1/N$, putting a lower bound on the communication required.

Conclusion.—We conclude this Letter by summarizing the new results. Theorem 1 concerns pure states and establishes, for general values of $N \geq 4$, that inside certain faces of $\Sigma_N$, defined by requiring one constituent system, say $X_i$, to have vanishing mutual information with all others, there is a strictly positive lower bound on the distance from the apex to any entropy vector corresponding to a pure state with $H(X_i) \neq 0$.

Corollary 1 concerns arbitrary states for $N$-partite system with $N \geq 3$. In particular, for the case $N = 3$, it entails a positive lower bound on the distance from the apex to any realizable entropy vector on any given ray within the four-dimensional face of $\Sigma_3$ defined by

$$III_{XY} = 0 \text{ for all } X, Y, \text{ and } H(ABC) \neq 0.$$  

This answers, in particular, a question posed by Winter [24] concerning the possibility of downscaling certain realizable entropy vectors. For general values of $N \geq 3$, Corollary 1 provides nonhomogeneous bounds (24), which rule out downscaled versions of realizable entropy vectors—such as those presented in Supplemental Material [14] Sec. C. It follows that $\Sigma_N$ is not a cone for $N \geq 3$. On the other hand, the closure of $\Sigma_N^*$ is a cone [2], so it likewise follows that $\Sigma_N$ is not closed for $N \geq 3$. This confirms a previous statement from [11] and solves an open problem from [2].

We emphasize that our results apply to the case of finite dimensional as well as infinite dimensional state spaces, provided the states in question have well-defined entropies.

In the applications, we highlighted the potential impact in macroscopic systems, quantum information theory, and quantum cryptography—pointing to the importance of a further investigation of the shape of $\Sigma_N$.

We acknowledge financial support from the VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059), the European Research Council (ERC Grant Agreement No. 81876) and the Novo Nordisk Foundation (Grant No. NNF20OC0059939 “Quantum for Life”).

3. A restricted class of boundary states has been studied in [4].
14. See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.240201 for Sec. A: proofs of Lemma 1,2, and 3, Sec. B: further elaboration and refinement of the main theorem and Corollary 1, and Sec. C: higher-$N$ generalizations of Pippenger’s state $\eta$ and the construction of a four-parameter family of realizable entropy vectors satisfying the conditions from the main theorem.


