

Entropy inequalities:
beyond
strong subadditivity(?)

Andreas Winter

(ICREA & Universitat Autònoma de Barcelona)

Outline

1. Von Neumann entropy $S(\rho)$ & inequalities
2. The laws of information theory
3. Shannon entropy $H(X)$: ∞ inequalities
4. New constrained inequalities for $S(\rho)$
5. Interlude: Rényi entropies
6. Quo vadis quantum?

1. Von Neumann entropy

$$S(\rho) = -\text{Tr} \rho \log \rho \text{ for } \rho \geq 0, \text{Tr} \rho = 1.$$

Common in many-body physics and information theory: system composed of several subsystems, i.e. $A_1 \otimes A_2 \otimes \dots \otimes A_n$.

Fundamental: relations between entropies of the parts $A_I = \otimes_{i \in I} A_i$ (up to 2^n subsets $I \subseteq [n]$)?

$$S(I) = S(A_I) := S(\rho_{A_I}) = S(\text{Tr}_{A_{[n] \setminus I}} \rho)$$

1. Von Neumann entropy

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

SSA is equivalent to the contractivity of the Umegaki relative entropy under ctp maps N :

$$\begin{aligned} \text{Tr } \rho(\log \rho - \log \sigma) &=: D(\rho || \sigma) \\ &\geq D(N(\rho) || N(\sigma)) \end{aligned}$$

1. Von Neumann entropy

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

For n parties: disjoint subsets $I, J, K \subseteq [n]$.

Purifying the state to $n+1$ parties, and with $S(A_I) = S(A_{[n+1] \setminus I})$, get furthermore:

$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$

$$S(AC) + S(BC) - S(A) - S(B) \geq 0 \quad (WMO)$$

1. Von Neumann entropy

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$

$$S(AC) + S(BC) - S(A) - S(B) \geq 0 \quad (WMO)$$

These obviously hold also for p.d.'s (classical case). In addition:

$$S(AB) - S(A) \geq 0 \quad (MO)$$

More generally for separable states!

1. Von Neumann entropy

$$S(A) \geq 0 \quad (P)$$

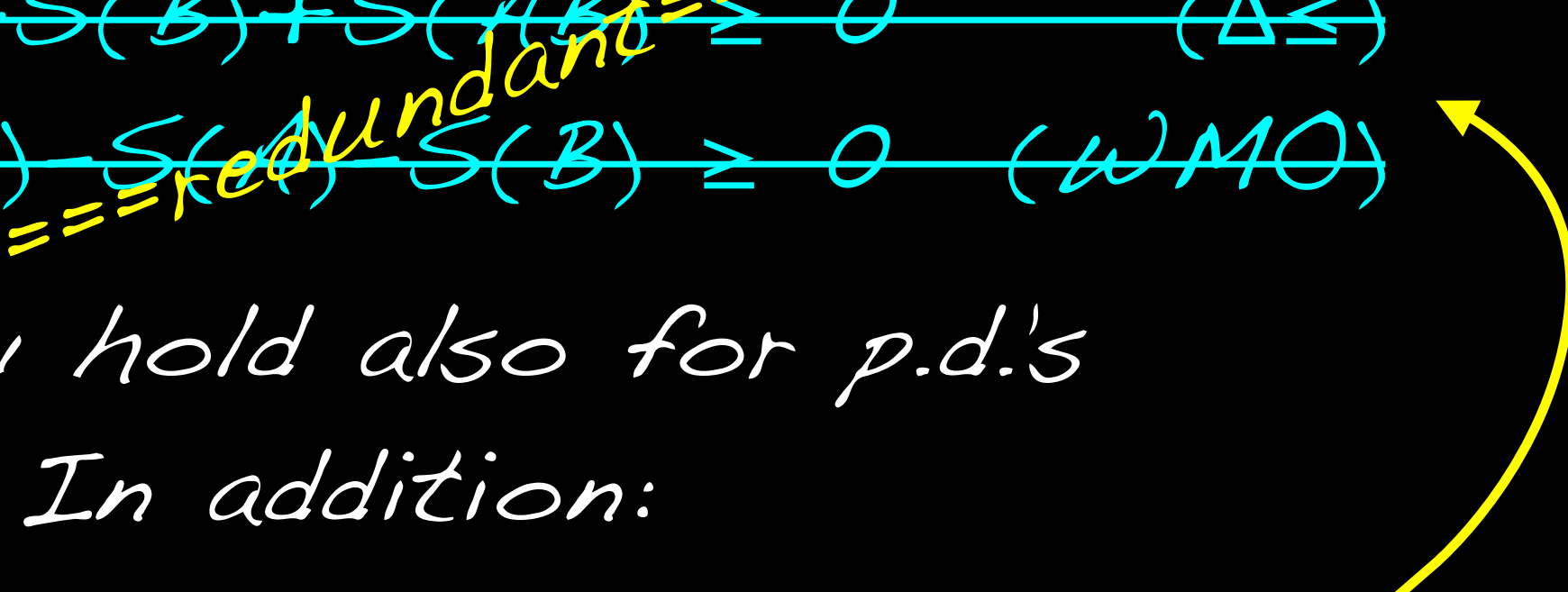
$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

~~$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$~~

~~$$S(AC) + S(BC) - S(ABC) - S(B) \geq 0 \quad (WMO)$$~~

redundant



These obviously hold also for p.d.'s (classical case). In addition:

$$S(AB) - S(A) \geq 0 \quad (MO)$$

More generally for separable states!

2. The laws of info theory

Why are they all linear inequalities?

To ask for the universal constraints on n -party entropies...

...consider the set of all entropy vectors:

$\Sigma_n^* := \{ (S(I) : \emptyset \neq I \subseteq [n]) \text{ for some } n\text{-party system and state} \}$

Restricted to classical states (p.d.'s): Γ_n^*

Restricted to separable states: Π_n^*

2. The laws of info theory

Fact: The topological closures of these sets, $\overline{\Sigma}_n^*$, $\overline{\Gamma}_n^*$, and $\overline{\Pi}_n^*$, are convex cones.

Hence, they are intersections of closed half-spaces; in other words, they are described by linear inequalities.

(More generally: homogeneous convex inequalities.)

Proof sketch: For states ρ on $A_{[n]}$ and σ on $B_{[n]}$, consider $C_i = A_i \otimes B_i$ and $\rho \otimes \sigma$ on $C_{[n]}$; clearly, $S(C_I) = S(A_I) + S(B_I)$, so Shannon cone closed under addition, non-negative integer linear combination.

Proof sketch: For states ρ on $A_{[n]}$ and σ on $B_{[n]}$, consider $C_i = A_i \otimes B_i$ and $\rho \otimes \sigma$ on $C_{[n]}$; clearly, $S(C_I) = S(A_I) + S(B_I)$, so Shannon cone closed under addition, non-negative integer linear combination.

For state ρ on $A_{[n]}$ and $0 < p < 1$, $k \in \mathbb{N}$, let $\omega := p \rho^{\otimes k} \otimes |1\rangle\langle 1| + (1-p) |0\rangle\langle 0| \otimes |0\rangle\langle 0|$ on $D_i = A_i^{\otimes k} \otimes \mathbb{C}^2$. Clearly, $S(D_I) = pkS(A_I) + h_2(p)$, thus can approximately scalar-multiply by $\lambda \geq 0$ via $k \gg 1$ and $p = \lambda/k \ll 1$.

2. The laws of info theory

$\Sigma_n :=$ polyhedral cone defined by the
Shannon-type inequalities

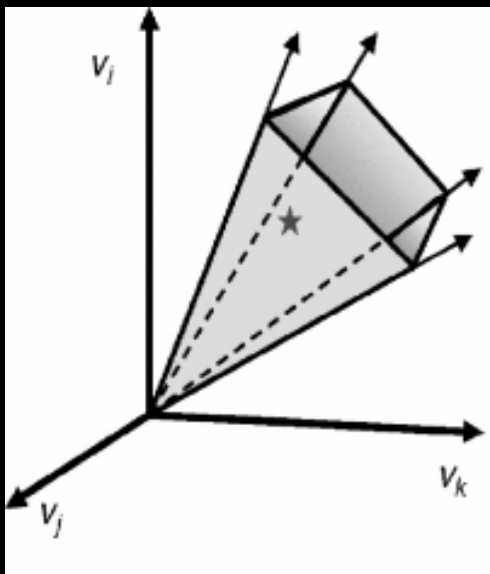
$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$

$$S(AC) + S(BC) - S(A) - S(B) \geq 0 \quad (WMO)$$



2. The laws of info theory

$\Sigma_n :=$ polyhedral cone defined by the
Shannon-type inequalities

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$

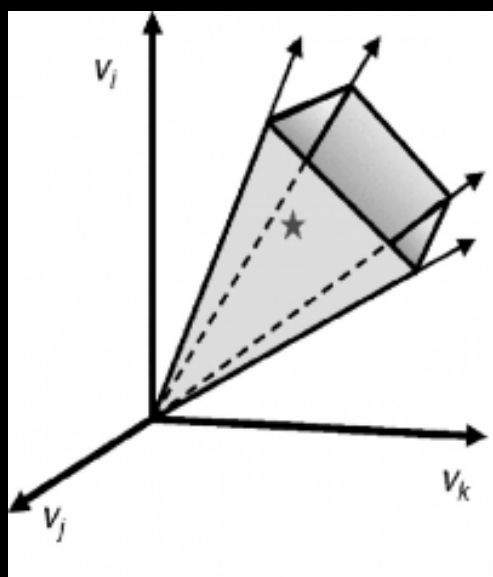
$$S(AC) + S(BC) - S(A) - S(B) \geq 0 \quad (WMO)$$

$\overline{\Sigma_n^*} \subseteq \Sigma_n$ by definition & known results

Equal? If so, above would
be all "laws of QIT"

2. The laws of info theory

$\Sigma_n :=$ polyhedral cone defined by the
Shannon-type inequalities



$$S(A) \geq 0 \quad (P)$$

~~$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$~~

redundant

$$I(A:C|B) \geq 0 \quad (SSA)$$

~~$$S(A) - S(B) + S(AB) \geq 0 \quad (\Delta \leq)$$~~

redundant

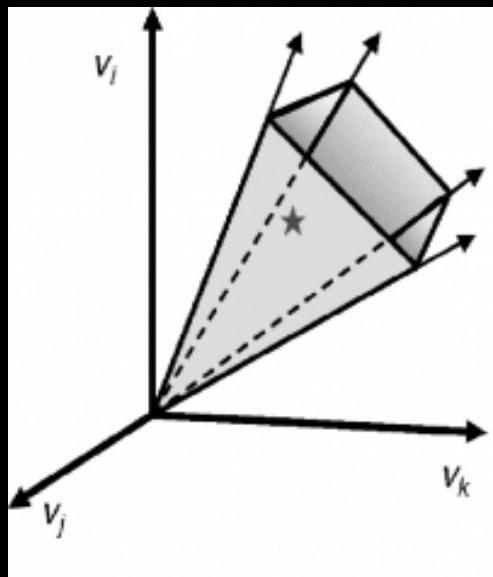
$$S(C|A) + S(C|B) \geq 0 \quad (WMO)$$

$\overline{\Sigma_n^*} \subseteq \Sigma_n$ by definition & known results

Equal? If so, above would
be all "laws of QIT"

2. The laws of info theory

$\Sigma_n :=$ polyhedral cone defined by the
Shannon-type inequalities



$$S(A) \geq 0 \quad (P)$$

$$I(A:C|B) \geq 0 \quad (SSA)$$

$$S(C|A) + S(C|B) \geq 0 \quad (WMO)$$

Equivalent to entropy cone of $(n+1)$ -party pure states: the purity implies $S(A_I) = S(A_{[n+1] \setminus I})$ for all $I \subseteq [n]$, and makes either SSA or WMO redundant.

2. The laws of info theory

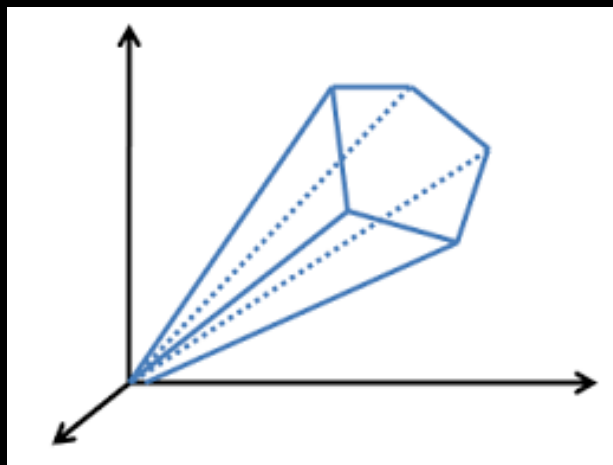
$\Gamma_n :=$ polyhedral cone defined by the
Shannon-type inequalities

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

$$S(AB) - S(A) \geq 0 \quad (MO)$$



2. The laws of info theory

$\Gamma_n :=$ polyhedral cone defined by the
Shannon-type inequalities

$$S(A) \geq 0 \quad (P)$$

$$S(A) + S(B) - S(AB) \geq 0 \quad (SA)$$

$$S(AB) + S(BC) - S(ABC) - S(B) \geq 0 \quad (SSA)$$

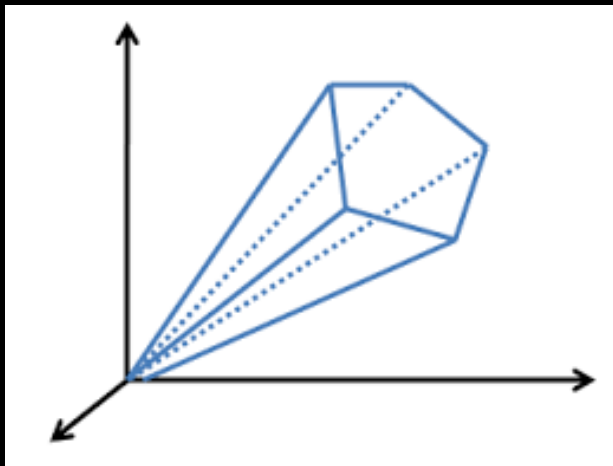
$$S(AB) - S(A) \geq 0 \quad (MO)$$

$\overline{\Gamma_n^*} \subseteq \overline{\Pi_n^*} \subseteq \Gamma_n$ by definition & known results

Equal? If so, above would
be all "laws of (Q)IT"

2. The laws of info theory

$\Gamma_n :=$ polyhedral cone defined by the
Shannon-type inequalities



$$\begin{aligned}
 & \cancel{S(A)} \geq 0 \quad (P) \\
 & \cancel{S(A) + S(B) - S(AB)} \geq 0 \quad (SA) \\
 & I(A:C|B) \geq 0 \quad (SSA) \\
 & S(B|A) \geq 0 \quad (MO)
 \end{aligned}$$

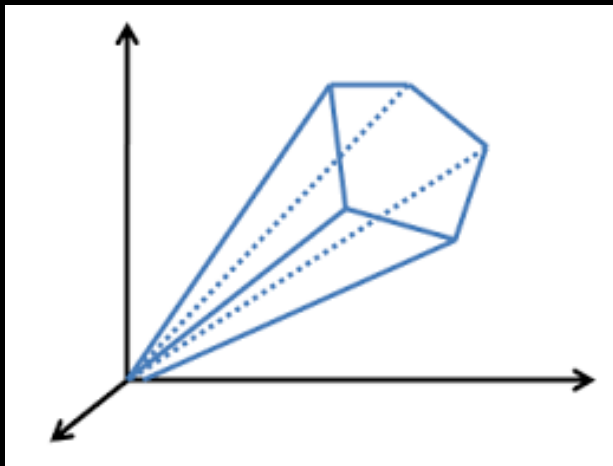
redundant

$\overline{\Gamma_n^*} \subseteq \overline{\Pi_n^*} \subseteq \Gamma_n$ by definition & known results

Equal? If so, above would
be all "laws of (Q)IT"

2. The laws of info theory

$\Gamma_n :=$ polyhedral cone defined by the
Shannon-type inequalities



$$\begin{aligned}
 & \cancel{S(A)} \geq 0 \quad (P) \\
 & \cancel{S(A) + S(B) - S(AB)} \geq 0 \quad (SA)
 \end{aligned}$$

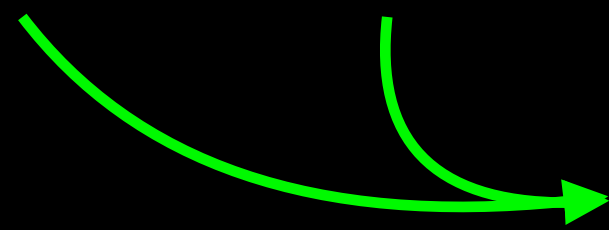
redundant

$$I(A:C|B) \geq 0 \quad (SSA)$$

$$S(B|A) \geq 0 \quad (MO)$$

"polymatroid" $\left\{ \right.$

$\overline{\Gamma_n^*} \subseteq \overline{\Pi_n^*} \subseteq \Gamma_n$ by definition & known results



Equal? If so, above would
be all "laws of (Q)IT"

2. The laws of info theory

For $n \leq 3$, we have all the inequalities, both classically and quantumly:

$$\overline{\Sigma_3^*} = \Sigma_3 \text{ and } \overline{\Gamma_3^*} = \overline{\Pi_3^*} = \Gamma_3.$$

Proof sketch (quantum case): Construct extremal rays of Σ_3 , as 4-party cone with the pure-state constraints

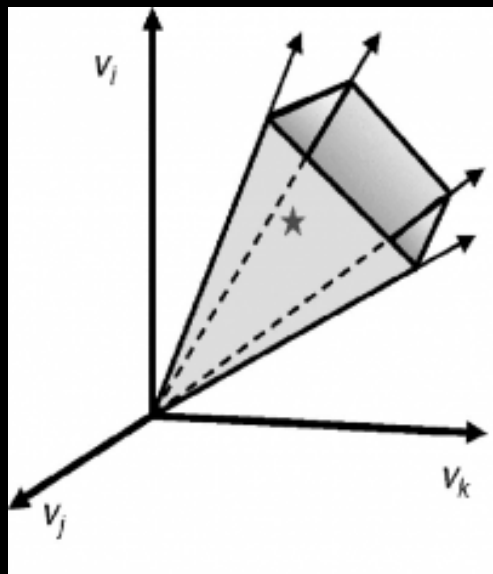
$S(A_I) = S(A_{[4] \setminus I})$, then for each of them find a state that realises it...

[R.W. Yeung, *IEEE-IT*, 43(6):1924-1934, 1997;
N. Pippenger, *IEEE-IT* 49(4):773-789, 2003]

2. The laws of info theory

$$\overline{\Sigma_3^*} = \Sigma_3 \text{ and } \overline{\Gamma_3^*} = \overline{\Pi_3^*} = \Gamma_3.$$

Proof sketch (quantum case): Extremal rays of Σ_3 , up to permutations of parties



A	B	C	ABC = D	AB = CD	AC = BD	BC = AD
1	1	0	0	0	1	1
1	1	1	1	1	1	1
1	1	1	1	2	2	2

2. The laws of info theory

$$\overline{\Sigma_3^*} = \Sigma_3 \text{ and } \overline{\Gamma_3^*} = \overline{\Pi_3^*} = \Gamma_3.$$

Proof sketch (quantum case): Extremal rays of Σ_3 , up to permutations

of parties

$|EPR\rangle_{AB}|00\rangle_{CD}$



$|GHZ\rangle_{ABCD}$



$|AME_4\rangle_{ABCD}$



A	B	C	ABC =D	AB =CD	AC =BD	BC =AD
1	1	0	0	0	1	1
1	1	1	1	1	1	1
1	1	1	1	2	2	2

3. New classical inequalities

For four RVs, there are information inequalities not implied by the Shannon-type inequalities, i.e. $\overline{\Gamma}_4^* \not\subseteq \Gamma_4$.

First by Zhang & Yeung:

$$I(C:D) \leq I(A:B) + I(C:D|A) + 2I(C:D|B) + I(B:C|D) + I(B:D|C) \quad (ZY)$$

Furthermore, this inequality is not a positive linear combination of Shannon-type inequalities.

[Z. Zhang, R.W. Yeung, IEEE-IT 44(4):1440-1452, 1998]

3. New classical inequalities

Latter part is proved by finding a vector satisfying all Shannon \leq 's, but not (ZY).

$$I(C:D) \leq I(A:B) + I(C:D|A) + 2I(C:D|B) + I(B:C|D) + I(B:D|C). \quad (ZY)$$

Inequality: RV B' s.t. $\mathbb{P}(BCD) = \mathbb{P}(B'CD)$, i.e. $B'CD$ has the same distribution as BCD , and $I(AB:B'|CD) = 0$, i.e. $AB-CD-B'$ is a Markov chain. Then use known inequalities...

3. New classical inequalities

Next by Dougherty, Freiling & Zeger:

$$I(C:D) \leq I(A:B) + I(C:D|A) + \frac{5}{2}I(C:D|B) + \frac{1}{2}I(B:C|D) + \frac{3}{2}I(B:D|C) \quad (DFZ)$$

This inequality, too, is not a positive linear combination of Shannon-type inequalities. Proved by more elaborate "copying" of RVs subject to conditional independence.

Both are part of an infinite family...

[R. Dougherty, C. Freiling, K. Zeger, arXiv:1104.3602, 2011]

3. New classical inequalities

Matúš, for any natural number s :

$$I(C:D) \leq I(A:B) + I(C:D|A) + \frac{s+3}{2} I(C:D|B) + \frac{1}{3} I(B:C|D) + \frac{s+1}{2} I(B:D|C) \quad (M_s)$$

3. New classical inequalities

Matúš, for any natural number s :

$$I(C:D) \leq I(A:B) + I(C:D|A) + \frac{s+3}{2} I(C:D|B) + \frac{1}{5} I(B:C|D) + \frac{s+1}{2} I(B:D|C) \quad (M_s)$$

These are independent non-Shannon-type inequalities, and infinitely many of them are necessary to delimit $\overline{\Gamma}_4^*$ (last point proved via a smooth curve of entropy vectors and its tangent at one point).

3. New classical inequalities

Digression: There are infinitely many information inequalities, but we don't know all of them (we don't even know if countably or uncountably many).

But they are all w.l.o.g. "balanced", meaning they are linear combinations of mutual informations; equivalently, their entropy expression vanishes on p.d.'s.

4. Same for von Neumann?

Start with Σ_4 , which we analyse as 5-party cone with the additional pure-state constraints $S(A_I) = S(A_{[5] \setminus I})$.

It has 76 extremal rays, falling into 8 classes under permutation of the parties.

The first three look familiar from $n=3$, but then it gets progressively wilder...

4. Same for von Neumann?

Up to permutation of the parties:

	A	B	C	D	E	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
1.	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0
2.	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
3.	1	1	1	1	0	2	2	2	1	2	2	1	2	1	1
4.	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5.	2	1	1	1	1	3	3	3	3	2	2	2	2	2	2
6.	1	1	2	2	2	2	3	3	3	3	3	3	2	2	2
7.	3	3	2	2	2	4	3	3	3	3	3	3	4	4	4
8.	3	3	3	3	2	4	4	4	5	4	4	5	6	5	5

4. Same for von Neumann?

#1, #2 and #3 are the same as for $n=3$:

$$(|00\rangle + |11\rangle)_{AB} \otimes |000\rangle_{CDE},$$

$$(|0000\rangle + |1111\rangle)_{ABCD} \otimes |0\rangle_E,$$

$$\sum_{i,j=0,1,2} |i\rangle_A |j\rangle_B |i+j\rangle_C |i+2j\rangle_D |0\rangle_E \pmod{3}.$$

#4 is realised by a 5-party GHZ state:

$$(|00000\rangle + |11111\rangle)_{ABCDE}.$$

#5 and #6, too, are realised by various stabilizer code states... But #7 and #8?

[N. Linden et al., unpublished; N. Linden, AW, CMP 259:129-138, 2005]

4. Same for von Neumann?

Note that #7 and #8, being extremal, have to saturate several Shannon inequalities with equality, among them $I(A:B|D)=0$, $I(A:C|B)=0$, $I(B:C|A)=0$.

4. Same for von Neumann?

Note that #7 and #8, being extremal, have to saturate several Shannon inequalities with equality, among them $I(A:B|D)=0$, $I(A:C|B)=0$, $I(B:C|A)=0$.

Thm. If ρ satisfies these constraints, then it follows $I(C:D) \geq I(C:AB)$.

But the latter is false on rays 7 & 8, so there are no states realising them.

4. Same for von Neumann?

Thm. If ρ s.t. $I(A:BD)=0$, $I(A:C|B)=0$,
 $I(B:C|A)=0$, then $I(C:D) \geq I(C:AB)$.

Proof rests on characterisation of equality in SSA [P. Hayden et al., CMP 246:359-374, 2004] that identifies a classical property Z in D , which can be measured without disturbing the state, and such that $I(A:B|Z)=0$, likewise for A and B ...

[N. Linden, AW, CMP 259:129-138, 2005]

Thm. If p s.t. $I(A:BD)=0$, $I(A:C|B)=0$,
 $I(B:C|A)=0$, then $I(C:D) \geq I(C:AB)$.

[N. Linden, AW, CMP 259:129-138, 2005]

Infinite family of such "constrained
information inequalities" in [J. Cadney, N.
Linden, AW, IEEE-IT 58(6):3657-3663, 2012], by the
same methodology.

Thm. If p s.t. $I(A:BD)=0$, $I(A:C|B)=0$,
 $I(B:C|A)=0$, then $I(C:D) \geq I(C:AB)$.

[N. Linden, AW, CMP 259:129-138, 2005]

Infinite family of such "constrained information inequalities" in [J. Cadney, N. Linden, AW, IEEE-IT 58(6):3657-3663, 2012], by the same methodology.

Unlike Zhang-Yeung, we are not able to pass to unconstrained inequalities, because the "copy lemma" is unavailable

5. Interlude: Rényi entropy

Consider the set of all α -Rényi entropy vectors, where $S_\alpha(\rho) = \frac{1}{1-\alpha} \log \text{Tr } \rho^\alpha$:

$$\Sigma_{n,\alpha}^* := \{ (S_\alpha(I) : \emptyset \neq I \subseteq [n]) \text{ for some } n\text{-party system and state} \}$$

5. Interlude: Rényi entropy

Consider the set of all α -Rényi entropy vectors, where $S_\alpha(\rho) = \frac{1}{1-\alpha} \log \text{Tr } \rho^\alpha$:

$\Sigma_{n,\alpha}^* := \{ (S_\alpha(I) : \emptyset \neq I \subseteq [n]) \text{ for some } n\text{-party system and state} \}$

Thm. For $0 < \alpha < 1$, $\overline{\Sigma_{n,\alpha}^*} = \mathbb{R}_{\geq 0}^{2^n - 1}$

Thm. For $\alpha > 1$, $\text{cone}(\overline{\Sigma_{n,\alpha}^*}) = \mathbb{R}_{\geq 0}^{2^n - 1}$

↳ Needed, as there are non-linear constraints...

5. Interlude: Rényi entropy

Thus, there are no nontrivial inequalities for the α -Rényi entropy when $0 < \alpha < 1$, & no nontrivial linear/convex inequalities when $\alpha > 1$.

At $\alpha=1$ is the von Neumann entropy, where we have plenty of inequalities, but there might be even more... (?)

5. Interlude: Rényi entropy

At $\alpha=0$, $S_0(\rho)=\log \text{rank } \rho$, has rich structure

For up to 3 parties, found:

$$S_0(A) \geq 0$$

$$S_0(A) + S_0(B) - S_0(AB) \geq 0$$

$$S_0(AB) + S_0(AC) - S_0(A) \geq 0$$

$$S_0(AB) + S_0(AC) + S_0(BC) - 2S_0(A) \geq 0$$

5. Interlude: Rényi entropy

At $\alpha=0$, $S_0(\rho)=\log \text{rank } \rho$, has rich structure

For up to 3 parties, found:

$$S_0(A) \geq 0$$

$$S_0(A)+S_0(B)-S_0(AB) \geq 0$$

$$S_0(AB)+S_0(AC)-S_0(A) \geq 0$$

$$S_0(AB)+S_0(AC)+S_0(BC)-2S_0(A) \geq 0$$

Conjecture: $S_0(AB)+S_0(AC)-S_0(BC) \geq 0$.

6. Quo vadis quantum?

(ZY), (DFZ) and a few others have been extensively checked numerically for quantum states of relatively small local dimension (< 5), and no violation found.

6. Quo vadis quantum?

(ZY), (DFZ) and a few others have been extensively checked numerically for quantum states of relatively small local dimension (< 5), and no violation found.

They also hold for pure 4-party states, in fact they reduce to Shannon-type inequalities (checked case by case).

Do they hold in general? How to prove it?

6. Quo vadis quantum?

Looking at the constructions for $n \leq 4$, one might think that extremal rays are always given by stabilizer states (of suitable dimension).

[D. Gross, M. Walter, JMP 54:082201, 2013;
N. Linden, F. Matúš, M.-B. Ruskai, AW, Proc. 8th TQC, 270-284, 2013]

6. Quo vadis quantum?

Looking at the constructions for $n \leq 4$, one might think that extremal rays are always given by stabilizer states (of suitable dimension).

But this is not true: in fact, stabilizer states obey the *Ingleton inequality*:

$$I(A:B) \leq I(C:D) + I(A:BC) + I(A:BD),$$

which however is false for Shannon and von Neumann entropy in general.

[D. Gross, M. Walter, JMP 54:082201, 2013;
N. Linden, F. Matúš, M.-B. Ruskai, AW, Proc. 8th TQC, 270-284, 2013]

6. Quo vadis quantum?

On the other hand, stabilizer states of n parties automatically obey all balanced information inequalities of the Shannon entropy, and these are all we need to worry about.

[D. Gross, M. Walter, JMP 54:082201, 2013;
N. Linden, F. Matúš, M.-B. Ruskai, AW, Proc. 8th TQC, 270-284, 2013]

6. Quo vadis quantum?

Question: Are all balanced inequalities of the Shannon entropy also quantum entropy inequalities?

6. Quo vadis quantum?

Question: Are all balanced inequalities of the Shannon entropy also quantum entropy inequalities?

Only possible approach seems to be, for state ρ on $A_{[n]}$, to look for σ_i on B_i , such that $\rho \otimes \sigma_1 \otimes \dots \otimes \sigma_n$ on $C_{[n]} = A_{[n]} B_{[n]}$, with entropies $S(C_I) = S(A_I) + \sum_{i \in I} S(\sigma_i)$, has classical entropy vector.

6. Quo vadis quantum?

Question: Are all balanced inequalities of the Shannon entropy also quantum entropy inequalities?

What we know is that for a state ρ on $A = A_{[n]}$, there exist RVs X_1, \dots, X_n correlated with A (i.e. a cq-state), such that

$$S(X_I | A) = S(A_I) + \sum_{i \in I} 2 \log |A_i|.$$

Kind of classical... but classical enough?

6. Quo vadis quantum?

What we know is that for a state ρ on $A \equiv A_{[n]}$, there exist RVs X_1, \dots, X_n correlated with A (i.e. a cq-state), such that

$$S(X_{\mathcal{I}}|A) = S(A_{\mathcal{I}}) + \sum_{i \in \mathcal{I}} 2 \log |A_i|.$$

Kind of classical... but classical enough?

$\overline{\Gamma}_n^*$ $\stackrel{?}{=} \overline{\Pi}_n^*$ might be a good starting point

