From log-determinant inequalities to Gaussian entanglement via recoverability theory

L. Lami, C. Hirche, G. Adesso, and A. Winter, IEEE 2017

arXiv:1703:06149

UAB Universitat Autònoma de Barcelona

giQ

QUANTUM CORRELATIONS GROUP

University of Nottingham UK | CHINA | MALAYSIA

Outline of the talk

- A bridge between probability theory, matrix analysis, and quantum optics.
- Summary of results.
- Properties of log-det conditional mutual information.
- Gaussian states in a nutshell.
- Main result: *the Rényi-2 Gaussian squashed entanglement coincides with the Rényi-2 Gaussian entanglement of formation for Gaussian states.*
- Conclusions & open problems.

Connecting probability theory and matrix analysis

- It has been known for a long time that one can turn information theoretical inequalities into determinantal inequalities by applying them to Gaussian random variables.[1]

$$\text{Gaussian:} \quad T \in_{\mathcal{R}} \mathbb{R}^N, \quad T \sim \mathcal{N}(0, V) \quad \longrightarrow \quad p_V(t) = \frac{e^{-\frac{1}{2} t^\intercal V^{-1} t}}{\sqrt{(2\pi)^N \det V}}$$

$$\begin{aligned} \text{Differential Rényi entropies:} \quad h_\alpha(T) &= \frac{1}{1-\alpha} \ln \int d^N t \, p_V(t)^\alpha \\ &= \frac{1}{2} \ln \det V + \frac{N}{2} \left(\ln 2\pi + \frac{1}{\alpha - 1} \ln \alpha \right), \end{aligned}$$

- All differential Rényi entropies reduce to 1/2 ln det (V) up to additive constants! Balanced entropy inequalities become inequalities between linear combinations of log determinants.

1. T.M. Cover and J.A. Thomas. Determinant inequalities via information theory. *SIAM J. Matrix Anal. Appl.* 9(3):384-392, 1988.

Example: strong subadditivity

- Strong subadditivity (SSA) is the most important "Shannon-type" entropy inequality. It tells us that any three random variables T_A, T_B, T_C satisfy

$$I(T_A : T_B|T_C) := H(T_A T_C) + H(T_B T_C) - H(T_C) - H(T_A T_B T_C) \geq 0$$

- When the three variables are jointly normal:

$$T = (T_A, T_B, T_C) \sim \mathcal{N}(V), \qquad V_{ABC} = \begin{pmatrix} V_A & X & Y \\ X^\intercal & V_B & Z \\ Y^\intercal & Z^\intercal & V_C \end{pmatrix} > 0$$

$$I(T_A : T_B|T_C) \;=\; \boxed{\frac{1}{2} \ln \frac{\det V_{AC} \det V_{BC}}{\det V_C \det V_{ABC}} =: I_M(A : B|C)_V}$$

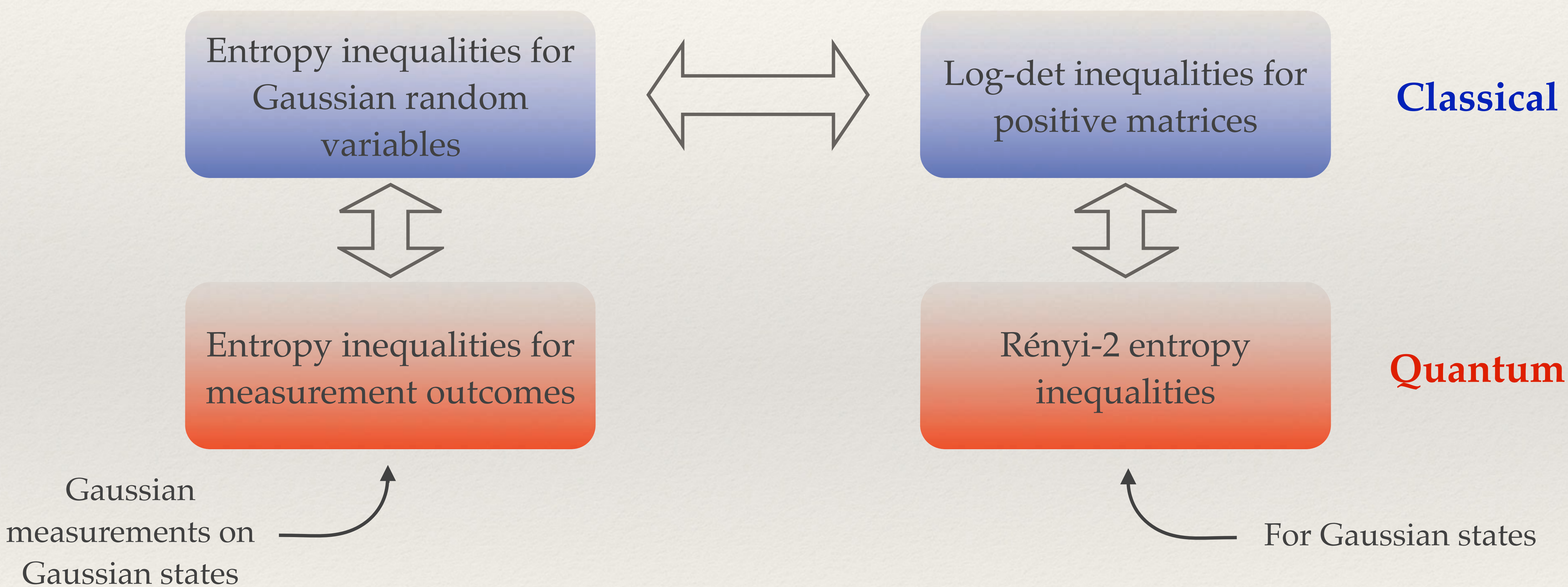
Log-det CMI

- I_M is the conditional mutual information (CMI) formed using the following **log-det entropy** defined on positive definite matrices:

$$M(V) := \frac{1}{2} \ln \det V$$

The grand plan

- Why is this relevant for quantum information?
  - In continuous variable systems, Gaussian random variables model the outcomes of Gaussian measurements performed on Gaussian states.
  - Rényi-2 entropies of Gaussian states are given by log-determinant expressions.



- This correspondences led to the introduction of operationally motivated Rényi-2 entropic quantifiers for Gaussian states.[2]

2. L. Mišta Jr. and R. Tatham. Gaussian intrinsic entanglement. *Phys. Rev. Lett.* 117:240505, 2016.

Our results in a nutshell

- We study general properties of the log-det conditional mutual information:
  - we analyse its behaviour under various matrix operations, most notably matrix inversion;
  - we show - among the other things - that the log-det mutual information is **convex on the geodesics of the "trace metric"**.

- We then establish **remainder terms** for the strong subadditivity inequality. This is done in two ways:
  - perturbing known bounds; and
  - exploiting new techniques based on **recoverability theory**.

- Our main result establishes the **equality** between two apparently very different **Gaussian entanglement measures**, when computed on Gaussian states:
  - Rényi-2 Gaussian squashed entanglement; and
  - Rényi-2 Gaussian entanglement of formation.

Schur complements

- **Definition.**

$$V_{AB} = \begin{pmatrix} \overbrace{V_A}^{A} & \overbrace{X}^{B} \\ X^T & V_B \end{pmatrix} \longrightarrow \textbf{Schur complement:} \quad V_{AB}/V_A := V_B - X^T V_A^{-1} X$$

- Schur complements answer a number of problems in matrix analysis & probability theory.[3]
  - Positivity of block matrices:

$$V_{AB} > 0 \iff V_A > 0 \text{ and } V_{AB}/V_A > 0$$

  - Determinant factorisation:

$$\det(V_{AB}) = \det(V_A)\det(V_{AB}/V_A)$$

  - Formula for block inverse:

$$V^{-1} = \begin{pmatrix} * & * \\ * & (V_{AB}/V_A)^{-1} \end{pmatrix}$$

  - Conditional distribution of normal variables:

$$T_{AB} \sim \mathcal{N}(V_{AB}) \implies T_B | (T_A = t) \sim \mathcal{N}(V_{AB}/V_A)$$

3. F. Zhang (ed.). *The Schur Complement and Its Applications*. Springer New York, 2005.

First properties of log-det CMI

- Log-det (conditional) mutual information:

$$I_M(A:B|C)_V = \frac{1}{2}\ln\frac{\det V_{AC}\det V_{BC}}{\det V_C \det V_{ABC}} \quad \cdots\cdots\cdots\rightarrow \quad I_M(A:B)_W = \frac{1}{2}\ln\frac{\det W_A \det W_B}{\det W_{AB}}$$

- **Theorem.** For all $V_{ABC} > 0$, one has

$$I_M(A:B|C)_V = I_M(A:B)_{V_{ABC}/V_C}$$
$$I_M(A:B|C)_V = I_M(A:B)_{V^{-1}}$$

- These are two ways to reduce a *conditional* mutual information to a *simple* mutual information. The second one, in particular, is somewhat surprising. It will come in handy later.

- *Sketch of proof*. For the first identity, observe that $T_{AB} \,|\, (T_C = t)$ is distributed normally, with covariance matrix V_{ABC}/V_C (which is independent from t). Then

$$I_M(A:B|C)_V = I(T_A:T_B|T_C) = \mathbb{E}_{T_C}(I(T_A:T_B)|T_C) = \mathbb{E}_{T_C}\big(I_M(A:B)_{V_{ABC}/V_C}\big) = I_M(A:B)_{V_{ABC}/V_C}$$

Second statement: block inversion formulae + determinant factorisation rule:

$$(V^{-1})_{AB} = (V_{ABC}/V_C)^{-1}, \quad (V^{-1})_A = (V_{ABC}/V_{BC})^{-1}, \quad (V^{-1})_B = (V_{ABC}/V_{AC})^{-1}$$

$$\begin{aligned}
I_M(A:B)_{V^{-1}} &= \frac{1}{2}\ln\frac{\det(V^{-1})_A \det(V^{-1})_B}{\det(V^{-1})_{AB}} \\
&= \frac{1}{2}\ln\frac{\det(V_{ABC}/V_{BC})^{-1}\det(V_{ABC}/V_{AC})^{-1}}{\det(V_{ABC}/V_C)^{-1}} \\
&= \frac{1}{2}\ln\frac{\det(V_{ABC}/V_C)}{\det(V_{ABC}/V_{BC})\det(V_{ABC}/V_{AC})} \\
&= \frac{1}{2}\ln\frac{(\det V_{ABC})(\det V_C)^{-1}}{(\det V_{ABC})(\det V_{BC})^{-1}(\det V_{ABC})(\det V_{AC})^{-1}} \\
&= \frac{1}{2}\ln\frac{\det V_{AC}\det V_{BC}}{\det V_{ABC}\det V_C} \\
&= I_M(A:B|C)_V
\end{aligned}$$

■

Application: lower bounds on log-det CMI

- Strong subadditivity is saturated iff the variables form a Markov chain. In other words,

$$I(T_A : T_B|T_C) = 0 \quad \Longleftrightarrow \quad T_A - T_C - T_B$$

- Problem: in the case of $T = (T_A, T_B, T_C)$ being Gaussian, how can we read this from the covariance matrix? The question was answered by Ando & Petz[4], but here we can give a one-line proof.

$$0 = I(T_A : T_B|T_C) = I_M(A:B|C)_V = I_M(A:B)_{V^{-1}}\,, \qquad V_{ABC} = \begin{pmatrix} V_A & X & Y \\ X^\intercal & V_B & Z \\ Y^\intercal & Z^\intercal & V_C \end{pmatrix}$$

Note that $I_M(A{:}B)_{V^{-1}} = 0$ is possible iff the off-diagonal blocks of $(V^{-1})_{AB}$ vanish. Introducing the projectors $\mathbf{\Pi}_A$ and $\mathbf{\Pi}_B$ onto the A and B subspaces, this can be rephrased as

$$0 = \Pi_A (V_{ABC})^{-1} \Pi_B^\intercal = -(V_{ABC}/V_{BC})^{-1}\big(X - Y V_C^{-1} Z^\intercal\big)(V_{BC}/V_C)^{-1}$$

- Saturation condition (= Markov chain condition): $\qquad X - Y V_C^{-1} Z^\intercal = 0$

4. T. Ando and D. Petz. *Acta Sci. Math. (Szeged)* 75:265-281, 2009.

- The advantage of this approach over the traditional one is that by working a bit harder you can perturb this saturation condition and get a **remainder term**:

$$I_M(A:B|C)_V \geq \frac{1}{2}\left\|V_A^{-1/2}(X - YV_C^{-1}Z^\intercal)V_B^{-1/2}\right\|_2^2$$

- Other remainder terms can be obtained by transforming the log-det CMI into a relative entropy and then applying any lower bound to the latter (e.g. negative log fidelity):

$$I(T_A:T_B|T_C) = D(T\|T')\,, \qquad p_{T'}(t_A,t_B,t_C) = p_{T_AT_C}(t_A,t_C)\,p_{T_B|T_C}(t_B|t_C)$$

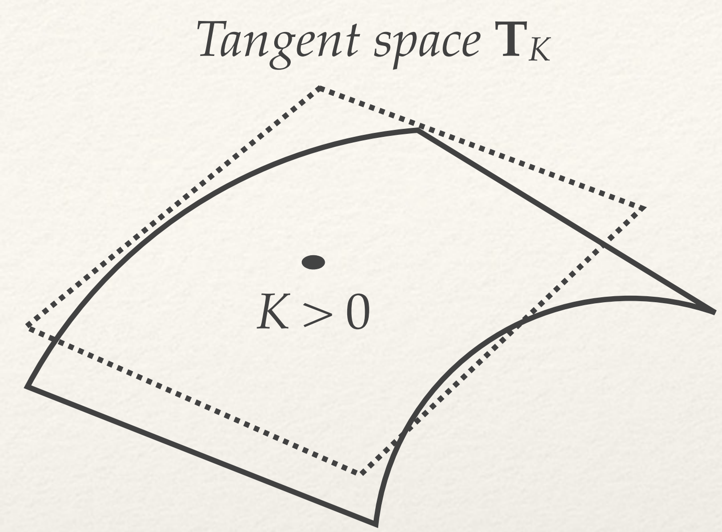
- A necessary condition for this strategy to succeed is that we work out the distribution of T': this new variable can be thought of as an "attempt" to reconstruct the original T once T_B has been lost, assuming that $T_A - T_C - T_B$ is a Markov chain.

  Also T' is distributed normally:

$$T' \sim \mathcal{N}(V')\,, \qquad V'_{ABC} := \begin{pmatrix} V_A & YV_C^{-1}Z^\intercal & Y \\ ZV_C^{-1}Y^\intercal & V_B & Z \\ Y^\intercal & Z^\intercal & V_C \end{pmatrix}$$

Matrix geometric mean

- The set $\mathbb{P}_N$ of positive definite matrices is a differentiable manifold.



- All tangent spaces $\mathbf{T}_K$ are isomorphic to $\mathbf{T}_{\mathbb{1}}$ (and hence to each other):

$$\mathbf{T}_K \ni X \mapsto K^{-1/2} X K^{-1/2} \in \mathbf{T}_{\mathbb{1}}$$

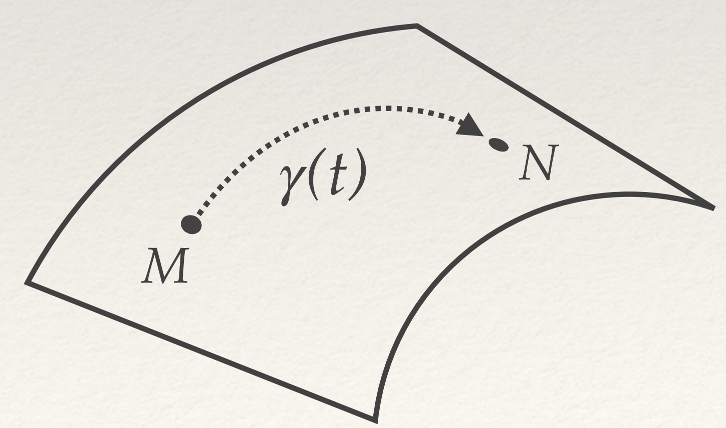
- $\mathbf{T}_{\mathbb{1}}$ (≃ Hermitian matrices) has a natural metric that comes from the Hilbert-Schmidt norm. This induces a metric, called the **trace metric**, on the whole manifold:

$$ds := \|K^{-1/2} dK K^{-1/2}\|_2 = \left(\mathrm{Tr}\left[(K^{-1} dK)^2 \right] \right)^{1/2}$$

- Then $\mathbb{P}_N$ becomes a Riemaniann manifold. How are its geodesics shaped?
  As one it turn out, can give an analytical expression[5] of the geodesic connecting M and N:

$$\gamma_{M \to N}(t) = \boxed{M^{1/2} \left(M^{-1/2} N M^{-1/2} \right)^t M^{1/2} =: M \#_t N}$$

Weighted geometric mean



5. M. Moakher. *SIAM J. Matrix Anal. & Appl.* 26(3):735-747, 2005.

- The weighted geometric mean enjoys a wealth of useful properties:[6]
  - Determinant factorisation:

$$\det(M\#_t N) = (\det M)^{1-t}(\det N)^t$$

  - Monotonicity under positive maps:

$$\Phi(M\#_t N) \leq \Phi(M)\#_t\Phi(N)$$

- Consider bipartite block matrices V_{AB}, W_{AB}. Applying this monotonicity property to the map that projects onto the subspace A we get

$$(V\#_t W)_A = \Pi_A(V\#_t W)\Pi_A^\intercal \leq (\Pi_A V \Pi_A^\intercal)\#_t(\Pi_A W \Pi_A^\intercal) = V_A\#_t W_A$$

Taking the determinant:

$$\det\left(V\#_t W\right)_A \leq \det\left(V_A\#_t W_A\right) = (\det V_A)^{1-t}(\det W_A)^t$$

6. T. Ando. *Linear Algebra Appl.* 26:203-241, 1979.

An important property of log-det MI

- **Theorem.** The log-det mutual information is convex on the geodesics of the trace metric, i.e.

$$I_M(A:B)_{V\#_t W} \leq (1-t)I_M(A:B)_V + tI_M(A:B)_W$$

- This is surprising, given that in general the log-det mutual information is *not* convex in the covariance matrix! It is also useful, as we shall see.

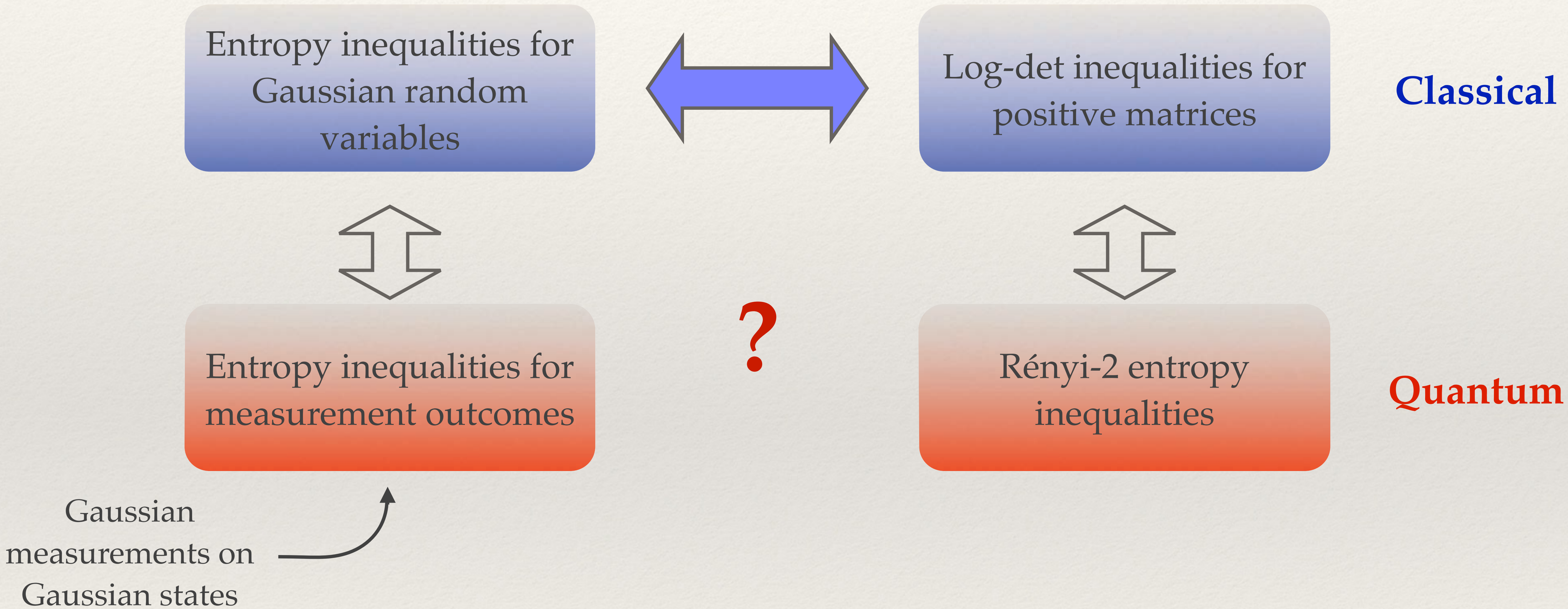
- *Proof*. Applying the determinantal inequality we have just found:

$$\begin{aligned}
I_M(A:B)_{V\#_t W} &= \frac{1}{2}\ln\frac{(\det(V\#_t W)_A)\,(\det(V\#_t W)_B)}{\det(V\#_t W)_{AB}} \\
&\leq \frac{1}{2}\ln\frac{(\det V_A)^{1-t}(\det W_A)^t(\det V_B)^{1-t}(\det W_B)^t}{(\det V_{AB})^{1-t}(\det W_{AB})^t} \\
&= \frac{1-t}{2}\ln\frac{\det V_A \det V_B}{\det V_{AB}} + \frac{t}{2}\ln\frac{\det W_A \det W_B}{\det W_{AB}} \\
&= (1-t)I_M(A:B)_V + tI_M(A:B)_W
\end{aligned}$$

∎

Where's the quantum?

- Until now we have explored the connections between classical probability theory and matrix analysis. Why is this relevant for quantum information?



- First we need to introduce the basic formalism of quantum optics: Gaussian states, quantum covariance matrices etc.

Quantum Gaussian states

- **Quantum optics** ~ quantum mechanics applied to a finite number of harmonic oscillators.

$$[\hat{x}_j, \hat{p}_k] = i\delta_{jk} \quad \longrightarrow \quad \hat{r} := (\hat{x}_1, \ldots, \hat{x}_n, \hat{p}_1, \ldots, \hat{p}_n)^T \;, \quad [\hat{r}, \hat{r}^T] = i\Omega = i \begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{pmatrix}$$

- Thermal states of quadratic Hamiltonians, also called **Gaussian states**, form a privileged class of experimentally relevant quantum states.

- As their classical relatives, they are parametrised by a mean vector w and a covariance matrix V.

- Covariance matrices of n-mode quantum states are exactly those $2n \times 2n$ real matrices such that

$$\boxed{V \geq i\Omega} \quad \longrightarrow \text{ Heisenberg uncertainty principle!}$$

  Real symmetric matrices satisfying the above condition are called **quantum covariance matrices** (QCMs).

- Pure states are represented by *minimal* QCMs, or equivalently by QCMs with determinant 1.

$$\hat{\rho}_G(V, w) \text{ pure} \quad \Longleftrightarrow \quad V \geq i\Omega \text{ and } \det V = 1$$

- Experimentally, **Gaussian measurements** are easily accessible. These can be described by POVMs parametrised by another QCM, called **seed**.

- When one makes a Gaussian measurement described by a seed γ on a Gaussian state with covariance matrix V, the outcome T is again distributed normally:

$$T \sim \mathcal{N}\left(\frac{1}{2}(V+\gamma)\right)$$

- Hence, its differential entropy becomes:

$$h(T) = \frac{1}{2}\ln\det\left(\frac{1}{2}(V+\gamma)\right) + n(\ln 2\pi + 1)$$

The *quantum* entropy of the Gaussian state itself is significantly more complicated…

- ***Moral: log-determinant entropies are the right thing to look at if what you care about are measured correlations.***

- To recover log-determinant expressions from the quantum state directly one has to work with Rényi-2 entropies:

$$S_2(\hat{\rho}_G(V,w)) := -\ln \mathrm{Tr}\left[\hat{\rho}(V,w)^2\right] = \frac{1}{2}\ln\det V$$

Gaussian entanglement measures

- Consider a bipartite Gaussian state. How to quantify its entanglement? An important measure is the **Rényi-α entanglement of formation**, aka the convex roof of the Rényi-α entanglement entropy.

- Since we are dealing with Gaussian states, it makes sense to restrict to Gaussian decompositions in the convex roof, and to look at $\alpha = 2$. In this way one obtains the **Rényi-2 Gaussian entanglement of formation**.[7]

- The choice of α makes the expression extremely simple at the level of covariance matrices:

$$E^G_{F,2}(A:B)_V = \inf \frac{1}{2} I_M(A:B)_\gamma$$

$$\text{s.t. } \gamma_{AB} \text{ pure QCM and } \gamma_{AB} \leq V_{AB}$$

← It has been conjectured to be linked to the secret key distillation rate in the Gaussian setting [Mišta & Tatham, PRL 2016].

7. Wolf et al., *Phys. Rev. A* 69:052320, 2003 — Adesso et al., *Phys. Rev. Lett.* 109:190502, 2012.

Main result

- **Theorem.** For any quantum covariance matrix V_{ABC}, twice the Rényi-2 Gaussian entanglement of formation between A and B is a lower bound on the log-det CMI:

$$\frac{1}{2} I_M(A:B|C)_V \geq E^G_{F,2}(A:B)_V$$

Furthermore, the r.h.s can be recovered by taking the infimum of the l.h.s over all (legal) extensions V_{ABC} of V_{AB}:

$$\boxed{\inf_{V_{ABC} \geq i\Omega_{ABC}} \frac{1}{2} I_M(A:B|C)_V = E^G_{F,2}(A:B)_V}$$

- *Sketch of proof (first inequality).* Start by defining[8]

$$\gamma_{AB} := (V_{ABC}/V_C) \#_{1/2} \left(\Omega_{AB} (V_{ABC}/V_C)^{-1} \Omega_{AB}^T \right)$$

Even if it is not obvious at first glance, this is always a QCM, and moreover $\gamma_{AB} \leq V_{AB}$. Now, compute its determinant:

$$\det \gamma_{AB} = \left(\det(V_{ABC}/V_C) \det\left(\Omega_{AB} (V_{ABC}/V_C)^{-1} \Omega_{AB}^T \right) \right)^{1/2} = \left(\det(V_{ABC}/V_C) \det(V_{ABC}/V_C)^{-1} \right)^{1/2} = 1$$

Hence, this γ_{AB} is a *pure* QCM. This means that we can use it as an ansatz in the inf that defines the Rényi-2 Gaussian entanglement of formation!

8. LL, C. Hirche, G. Adesso, and A. Winter. *Phys. Rev. Lett.* 117:220502, 2016.

Doing so yields:

$$E^{\mathrm{G}}_{F,2}(A:B)_V = \inf_{\tau_{AB} \le V_{AB},\ \tau_{AB}\ \text{pure}} \frac{1}{2} I_M(A:B)_\tau$$

$$\le \frac{1}{2} I_M(A:B)_{(V_{ABC}/V_C)\#_{1/2}(\Omega(V_{ABC}/V_C)^{-1}\Omega^\intercal)}$$

Convexity of log-det MI on the geodesics of the trace metric ⟶

$$\le \frac{1}{4} I_M(A:B)_{V_{ABC}/V_C} + \frac{1}{4} I_M(A:B)_{\Omega(V_{ABC}/V_C)^{-1}\Omega^\intercal}$$

Getting rid of Ω (orthogonal matrix) ⟶

$$= \frac{1}{4} I_M(A:B)_{V_{ABC}/V_C} + \frac{1}{4} I_M(A:B)_{(V_{ABC}/V_C)^{-1}}$$

Properties of log-det CMI ⟶

$I_M(A:B|C)_V = I_M(A:B)_{V_{ABC}/V_C}$

$I_M(A:B|C)_V = I_M(A:B)_{V^{-1}}$

$$= \frac{1}{4} I_M(A:B|C)_V + \frac{1}{4} I_M(A:B|C)_V$$

$$= \frac{1}{2} I_M(A:B|C)_V$$

In the second part of the proof we had to construct suitable extensions that can saturate the above bound (a bit more cumbersome).

■

Consequences

$$\inf_{V_{ABC}\geq i\Omega_{ABC}} \frac{1}{2} I_M(A:B|C)_V = E_{F,2}^G(A:B)_V$$

- The theorem reduces the inf on the l.h.s., which is in principle over extensions of unbounded dimension, to an optimisation over a compact set of matrices of fixed dimension.

- The optimised mutual information is reminiscent of the squashed entanglement:[10]

$$E_{\mathrm{sq}}(A:B)_\rho := \inf_{\rho_{ABC}} \frac{1}{2} I(A:B|C)_\rho$$

  In fact, it is a "Rényi-2 Gaussian" version of the squashed entanglement.

- For comparison, remember that a simple expression for the von Neumann squashed entanglement remains out of reach, even for very simple states.

- Our results may be useful to tackle a conjecture in [Mišta & Tatham, PRL 2016]: *the Rényi-2 Gaussian entanglement of formation coincides with the* ***Gaussian intrinsic entanglement****, i.e. the intrinsic information of the measured correlations, when all the parties are assumed to employ only Gaussian processing.*

9. R.R. Tucci, arXiv:quant-ph/9909041. — M. Christandl and A. Winter, *J. Math. Phys.* 45(3):829-840, 2004.

Conclusions

- Log-determinant expressions appear:
  - in the entropies of normal variables;
  - in the entropies of the outcomes of Gaussian measurements on Gaussian states;
  - in the Rényi-2 entropies of Gaussian states.
- The log-determinant mutual information enjoys lots of useful properties: for instance, it is convex on the geodesics of the trace metric.
- These properties can be used to show that the Rényi-2 Gaussian squashed entanglement coincides with the Rényi-2 Gaussian entanglement of formation.
- This may shed light on the connections between these quantifiers and the cryptographically motivated Gaussian intrinsic entanglement.

Thank you!