Comment

https://doi.org/10.1038/s41567-023-02289-9

The tangled state of quantum hypothesis testing

Mario Berta, Fernando G. S. L. Brandão, Gilad Gour, Ludovico Lami, Martin B. Plenio, Bartosz Regula & Marco Tomamichel

Quantum hypothesis testing—the task of distinguishing quantum states—enjoys surprisingly deep connections with the theory of entanglement. Recent findings have reopened the biggest questions in hypothesis testing and reversible entanglement manipulation.

Most physicists are introduced to entropy through thermodynamics. Entropy is the fundamental and unique quantity that governs the transformations under adiabatic processes: a transformation between two compatible states of a closed system can be realized if and only if the entropy does not decrease[1]. However, it also has a crucial role in the more abstract field of information theory. In particular, a generalization known as the relative entropy provides a way to measure the distinguishability between probability distributions.

Extending the concept to quantum states was challenging because the non-commutative character of quantum states means that there are many possible ways to define such an extension. A unique and unambiguous solution came from the study of quantum hypothesis testing—a task in which we are given multiple copies of one of two quantum states, ρ or σ, and the goal is to distinguish between the two states. The probability of mistaking ρ for σ decays exponentially with the number of copies, and the corresponding exponent is given exactly by a quantum variant of the relative entropy

$$D(\rho\|\sigma) = \mathrm{Tr}\,\rho\left(\log_2\rho - \log_2\sigma\right). \quad (1)$$

Its role in quantum hypothesis testing gives quantum relative entropy an operational meaning and a solid physical justification, identifying it as the correct extension of the classical relative entropy to the quantum case.

The uniqueness of the entropic measure of distinguishability of quantum states is consistent with the special role that thermodynamic entropy plays in determining the transformations of physical systems. However, it is not the only link between quantum information theory and thermodynamics. At their core, both theories deal with resources that can be extracted from physical systems: in the case of thermodynamics, this sought-after resource is work, while in quantum information it is entanglement, which fuels quantum communication and computation tasks. Drawing an analogy with thermodynamics, the notion of an entropy of entanglement rose to prominence as a quantity that might completely characterize all entanglement transformations[2]. It was, however, unclear whether an exact correspondence between entanglement and thermodynamics could be established. Once again, the key to conclusively resolving this question was quantum hypothesis testing—or so it seemed.

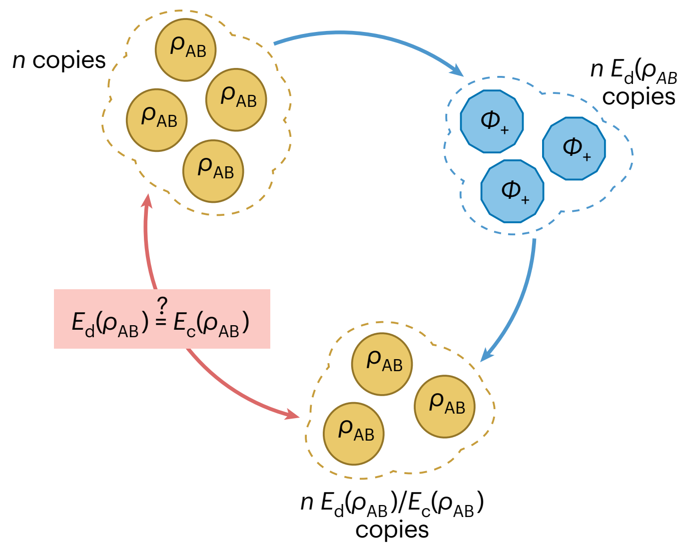

Fig. 1 | (Ir)reversibility in asymptotic state conversion. From each copy of a bipartite state ρ_{AB}, one can approximately extract $E_d(\rho_{AB})$ copies of a maximally entangled two-qubit state Φ_+. Conversely, from each copy of the maximally entangled state Φ_+, one can approximately prepare $1/E_c(\rho_{AB})$ copies of the state ρ_{AB}, with the approximation becoming perfect when there is access to an asymptotically large number of copies. The problem of reversibility is then the question of whether $E_d(\rho_{AB}) = E_c(\rho_{AB})$, so that the rate at which entanglement can be extracted from ρ_{AB} equals the rate at which entanglement is needed to generate ρ_{AB}, making the overall process asymptotically cyclic and identifying the rate as the unique asymptotic measure of entanglement. It is known that equality holds whenever ρ_{AB} is a pure state, but this is not necessarily the case in general. If $E_d(\rho_{AB}) < E_c(\rho_{AB})$ for some state ρ_{AB}, then the state cannot be reversibly manipulated.

Entropy of entanglement

Initial evidence for the existence of a unique entropy of entanglement was very promising. Many parallels between entanglement theory and thermodynamics were discovered, most strikingly the reversibility of the manipulation of pure, noiseless quantum states.

Consider a situation where two separate parties, Alice and Bob, share many copies of a bipartite quantum state with density matrix ρ_{AB}. The state may be entangled, which could be quantified by establishing how many maximally entangled two-qubit states can be extracted—or distilled—from the shared state. Alternatively, one could consider how

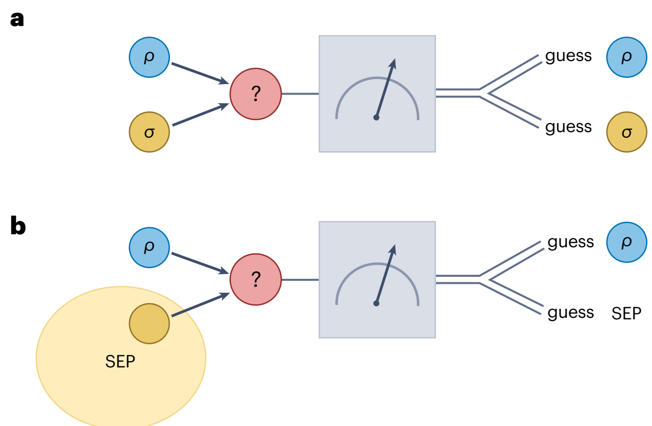

Fig. 2 | Two types of quantum hypothesis testing. In the setting of hypothesis testing, we are given an unknown quantum state which is promised to be either a fixed state ρ or another fixed state σ (panel **a**), or either a fixed state ρ or a state belonging to some set of quantum states, for example all unentangled, separable states SEP (panel **b**). The task is then to guess correctly which of the two we have been given by measuring multiple copies of the system and deciding based on the measurement outcomes. The variant shown in panel **b** is known as composite hypothesis testing, and we refer to the particular case discussed here—where the alternative hypothesis comprises all unentangled states in SEP—as entanglement testing.

much entanglement it costs to synthesize ρ_{AB}. These two questions led to the notions of distillable entanglement $E_d(\rho_{AB})$ and entanglement cost $E_c(\rho_{AB})$, respectively. Remarkably, for any pure state $\psi_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, it holds that[3]

$$E_d(\psi_{AB}) = E_c(\psi_{AB}) = S(\psi_A) \tag{2}$$

where $S(\rho) = -\mathrm{Tr}\rho\log_2\rho$ is the von Neumann entropy, and ψ_A is the reduced state on one of the two parties.

This equality means that any pure state costs exactly as much entanglement as can be distilled from it. If we consider the asymptotic limit, in which we can manipulate more and more copies of the given quantum state, nothing is lost in the process (see Fig. 1). This resembles reversible cycles in thermodynamics, and indeed it allows us to conclude that a strong 'second law of entanglement' holds: the entropy $S(\psi_A)$ can be identified as the unique measure of pure-state entanglement in the context of entanglement transformations.

However, it has been shown that for some noisy, mixed quantum states these transformations are irreversible[4], calling into question the precise relation between thermodynamics and entanglement. A ray of hope appeared shortly thereafter thanks to relaxing some of the restrictions to which entanglement manipulation was subjected[5].

Entanglement manipulation is typically studied in the framework of local operations and classical communication[3], in the sense that Alice and Bob are free to perform any local operations and exchange information classically, but quantum communication may not be used freely, because doing so would allow them to distribute additional entanglement. This framework can be extended to give the two parties access to some additional, restricted resources. For instance, allowing so-called positive partial transpose operations makes it possible to reversibly transform some mixed states that are irreversible under the framework of local operations and classical communication[5].

This raised the question of what additional resources might be needed so that $E_d(\rho_{AB}) = E_c(\rho_{AB})$ holds for all mixed quantum states ρ_{AB}, making the theory fully reversible[6]. Some of us, Brandão and Plenio, tackled this problem with an axiomatic approach[7,8]. Rather than specifying what Alice and Bob are allowed to do, the aim was to define the problem in terms of what they cannot do.

One natural restriction is simply to impose that they may not generate entanglement for free, as this would trivialize the whole framework. Relaxing this assumption slightly yields the set of 'asymptotically non-entangling operations'. These may create some small amounts of entanglement, but this supplemented amount must become vanishingly small as more and more copies of states are manipulated. Under such permitted operations, the entanglement cost $E_c(\rho_{AB})$ of any mixed state equals the so-called regularized relative entropy of entanglement E_R^∞ (ref. 8):

$$E_c(\rho_{AB}) = E_R^\infty(\rho_{AB}) = \lim_{n\to\infty}\frac{1}{n}\left(\min_{\sigma_{A^nB^n}\in\mathrm{SEP}} D(\rho_{AB}^{\otimes n}\,\|\,\sigma_{A^nB^n})\right) \tag{3}$$

where the quantum relative entropy is minimized over the set of all separable (unentangled) states SEP, and the limit $n \to \infty$ represents the asymptotic character of the entanglement transformations. E_R^∞ thus gives a quantitative measure of how far ρ_{AB} is from being an unentangled state. The discovery that it equals the entanglement cost under asymptotically non-entangling operations directly generalized part of the earlier pure-state result in Eq. (2) and identified a promising candidate for a reversible framework of entanglement for all quantum states.

To complete the extension of Eq. (2), Brandão and Plenio needed to show that the distillable entanglement E_d also equals the regularized relative entropy. In an attempt to do so, they revealed a connection between the distillation of entanglement and a special kind of quantum hypothesis testing.

The role of quantum hypothesis testing

When identifying whether a given quantum state is one of two possibilities, ρ or σ, there are two types of error that can be made. One can either mistake ρ for σ (conventionally called a type I error), or σ for ρ (type II error). These two mistakes are often not equally consequential, just as false-positive and false-negative results are not necessarily equally undesirable in clinical testing.

To understand the relation between the two errors, one defines the optimized type II error $\beta_\varepsilon(\rho\,\|\,\sigma)$ as the least probability of type II error such that the probability of type I error is at most ε. We can then consider how this error probability scales as we use more and more copies of the unknown state. A result known as the quantum Stein's lemma[9] tells us that in the asymptotic limit the relative entropy determines this scaling precisely, thus capturing how difficult it is to distinguish any two states:

$$\beta_\varepsilon\left(\rho^{\otimes n}\|\sigma^{\otimes n}\right) \sim 2^{-nD(\rho\|\sigma)} \qquad (n\to\infty). \tag{4}$$

The coefficient associated with the exponential decay in n of the left-hand side is therefore exactly given by the relative entropy.

But we may wish to consider a different task, where we are not just distinguishing between ρ and a single state σ, but between ρ and a whole family of states. For example, if we wish to test whether a certain quantum device produces entanglement, we may want to test ρ_{AB} against all separable states (see Fig. 2). Intuitively, this can be used to gauge how entangled a given state is, since the distinguishability error quantifies how easy it is to mistake some unentangled state for ρ_{AB}. We refer to this composite hypothesis testing as entanglement testing. It is a very difficult problem to characterize, especially in the many-copy setting, as we need to understand the worst-case distinguishability error $\beta_\varepsilon(\rho_{AB}^{\otimes n} \,\|\, \sigma_{A^nB^n})$ optimized over all possible separable states $\sigma_{A^nB^n}$.

Brandão and Plenio's work[7,8] showed that the error exponent of entanglement testing is determined by the rate of distillation under asymptotically non-entangling operations

$$\sup_{\sigma_{A^nB^n}\in \mathrm{SEP}} \beta_\varepsilon\left(\rho_{AB}^{\otimes n} \| \sigma_{A^nB^n}\right) \sim 2^{-nE_d(\rho_{AB})} \qquad (n\to\infty;\varepsilon\to 0^+) \tag{5}$$

where the equivalence holds exactly in the limit as the number of copies n grows to infinity and the type I error probability $\varepsilon > 0$ becomes vanishingly small (with the latter limit taken after the former one).

This result connected two very different tasks, entanglement distillation on the one hand and entanglement testing on the other. Taking cues from the original Stein's lemma in Eq. (4), it is natural to expect this quantity to be equivalent to some type of relative entropy. Indeed, ref. 7,8 claimed to prove a generalization of the quantum Stein's lemma, showing that the error exponent equals the regularized relative entropy of entanglement,

$$E_\mathrm{d}(\rho_{AB}) = E_\mathrm{R}^\infty(\rho_{AB}). \tag{6}$$

This would have established an exact expression quantifying the ultimate effectiveness of entanglement testing. Importantly, combining Eq. (6) with Eq. (3) would also complete the search for a reversible framework for entanglement theory by establishing that $E_\mathrm{d}(\rho_{AB}) = E_\mathrm{R}^\infty(\rho_{AB}) = E_\mathrm{c}(\rho_{AB})$ under asymptotically non-entangling operations. This result would thus single out E_R^∞ as the sole measure that is compatible with asymptotically non-entangling transformations, identifying it as the unique generalization of the entropy of entanglement to mixed states in this framework. However, the situation turned out to be much more complicated.

Reversibility, or the lack thereof

Over 12 years after the publication of the generalized quantum Stein's lemma[7], which underlies Eq. (6), a gap was discovered in its original proof[10]. This brings the whole claim, and hence one of the most important developments in quantum hypothesis testing since the original quantum Stein's lemma[9], into question.

What is an even more far-reaching consequence, this means that the first—and so far only—reversible framework for entanglement manipulation cannot be considered valid, reopening the question of whether it is possible to construct one at all.

We stress that the gap does not immediately disprove the reversibility conjectured in ref. 7,8, since no counterexample has been found either. It also does not contradict the conceptual parallels between entanglement testing and entanglement distillation that we discussed above, as those results are independent of the generalized quantum Stein's lemma. Although the error is seemingly just a technical oversight, it is unclear whether any of the known approaches[10] can be used to re-establish the result.

To add to the confusion, although previous evidence generally seemed to support the hypothesis that reversibility of entanglement can be expected in some form, more recent results may suggest otherwise. Some of us showed[11] that the theory of entanglement remains irreversible under all protocols which do not generate entanglement. This result effectively established Brandão and Plenio's class of asymptotically non-entangling operations as the smallest one that could become reversible, ruling out less permissive ways to restore reversibility. What is more, according to some measures of entanglement, the amount of entanglement created in Brandão and Plenio's approach was found not to be vanishingly small but rather asymptotically large[11], casting doubt on whether such a framework can be considered truly 'asymptotically non-entangling'.

On the more positive side, there are also reasons to believe that the original claims of ref. 7,8 are indeed true. Perhaps one of the most compelling for us is the fact that a slightly tweaked version of Eq. (5), in which we replace the limit $\varepsilon \to 0$ with $\varepsilon \to 1$, can be proved to converge to the limit $E_\mathrm{R}^\infty(\rho_{AB})$ (ref. 10). Such a modification corresponds to asking about the optimal type II error exponent when we do not require the type I error probability to be small, but rather we content ourselves with it not being too large, that is, too close to 1. In information theory, this is known as the 'strong converse' regime. Crucially, the transition to the strong converse regime is known not to change the asymptotic rates of important quantum information processing tasks, including standard quantum hypothesis testing between two states. If this were true also for entanglement testing, it would recover $E_\mathrm{R}^\infty(\rho_{AB})$ as the optimal error exponent of entanglement testing and restore the reversibility of entanglement. However, this property remains to be proved.

The gap in the proof of ref. 7,8 also affects other follow-up results. The generality of Brandão and Plenio's approach allowed it to be applied beyond entanglement theory, suggesting that essentially all phenomena that find use in quantum information can be manipulated reversibly[12]. Such a strong property may be lost unless a proof of the generalized quantum Stein's lemma can be recovered. Additionally, several important proofs in quantum information theory become incomplete without the generalized quantum Stein's lemma[10].

Some other quantum resources, such as quantum coherence, can be shown to be reversible using different methods. Although this may suggest that reversibility is a generic property shared by different theories of quantum resource manipulation, we already know that the reversibility of entanglement—if it is at all possible—cannot be obtained under the same setting and assumptions[11]. This makes it difficult to draw any strong conclusions from the other reversible quantum resource theories. Similarly, several extensions of quantum Stein's lemma can be established in certain settings, but none of them are quite strong enough to recover the original statement of Eq. (6) (ref. 10).

Altogether, Brandão and Plenio's axiomatic framework certainly did unveil deep connections between quantum hypothesis testing and asymptotic transformations of quantum resources. However, the most important application of these connections—the establishment of a reversible theory of quantum entanglement, together with a unique entropic measure of entanglement—can only be considered a conjecture at this point.

Although the discovery of the gap in the proof of ref. 7,8 has shaken up the foundations of modern quantum information, it has also reinvigorated interest in some of the cornerstone problems of the theories of entanglement and quantum state discrimination, and we can only hope that this will lead to exciting new research in the future. What we certainly know now is that quantum entanglement hides an even richer and more complicated structure than we had given it credit for, and understanding some of its most fundamental properties may be even more difficult than it seemed.

Mario Berta[1,2], Fernando G. S. L. Brandão[3,4], Gilad Gour[5], Ludovico Lami[6,7,8] ✉, Martin B. Plenio[9], Bartosz Regula[10] ✉ & Marco Tomamichel[11,12]

[1]Institute for Quantum Information, RWTH Aachen University, Aachen, Germany. [2]Department of Computing, Imperial College London, London, UK. [3]Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA. [4]AWS Center for Quantum Computing, Pasadena, CA, USA. [5]Department of Mathematics and Statistics, Institute for Quantum Science and Technology, University of Calgary, Calgary, Alberta, Canada. [6]QuSoft, Amsterdam, The Netherlands. [7]Korteweg–de Vries Institute for Mathematics, University of Amsterdam, Amsterdam, The Netherlands. [8]Institute for Theoretical Physics, University of Amsterdam, Amsterdam, The Netherlands. [9]Institut für Theoretische Physik und IQST, Universität Ulm, Ulm, Germany. [10]Mathematical Quantum Information RIKEN Hakubi Research Team, RIKEN Cluster for Pioneering Research (CPR) and RIKEN Center for Quantum Computing (RQC), Wako, Japan. [11]Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore. [12]Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore.

✉e-mail: ludovico.lami@gmail.com; bartosz.regula@gmail.com

Published online: 22 December 2023

References

1. Lieb, E. H. & Yngvason, J. *Phys. Rep.* **310**, 1–96 (1999).
2. Horodecki, M., Oppenheim, J. & Horodecki, R. *Phys. Rev. Lett.* **89**, 240403 (2002).
3. Bennett, C. H., Bernstein, H. J., Popescu, S. & Schumacher, B. *Phys. Rev. A* **53**, 2046 (1996).
4. Vidal, G. & Cirac, J. I. *Phys. Rev. Lett.* **86**, 5803 (2001).
5. Audenaert, K., Plenio, M. B. & Eisert, J. *Phys. Rev. Lett.* **90**, 027901 (2003).
6. Plenio, M. B. Problem 20. In preprint at http://arxiv.org/abs/quant-ph/0504166 (eds Krueger, O. & Werner, R. F.) (2005).
7. Brandão, F. G. S. L. & Plenio, M. B. *Commun. Math. Phys.* **295**, 791–828 (2010).
8. Brandão, F. G. S. L. & Plenio, M. B. *Commun. Math. Phys.* **295**, 829–851 (2010).
9. Hiai, F. & Petz, D. *Commun. Math. Phys.* **143**, 99–114 (1991).
10. Berta, M. et al. *Quantum* **7**, 1103 (2023).
11. Lami, L. & Regula, B. *Nat. Phys.* **19**, 184–189 (2023).
12. Brandão, F. G. S. L. & Gour, G. *Phys. Rev. Lett.* **115**, 070503 (2015).

Competing interests

The authors declare no competing interests.