

Faithful Squashed Entanglement

with applications to separability testing and quantum Merlin-Arthur games

Fernando G.S.L. Brandão, Matthias Christandl and Jon Yard

Summary. Squashed entanglement is a measure for the entanglement of bipartite quantum states. In [1] we present a lower bound for squashed entanglement in terms of the LOCC distance to the set of separable states. This, in turn, has a number of consequences to quantum information theory and quantum complexity theory. In particular, we find

- squashed entanglement to be a *faithful* entanglement measure, meaning that it is nonzero on every entangled state;
- a new de Finetti-type theorem that gives conditions for the existence of data-hiding states;
- a subexponential-time algorithm solving the weak membership problem for the set of separable states in LOCC norm;
- multiple provers not to be more powerful than a single prover when the verifier is restricted to LOCC operations. This answers a question posed by Aaronson *et al.* [2] and provides a new characterization of the complexity class QMA.

We derive the lower bound on squashed entanglement from a lower bound on the quantum conditional mutual information, which corresponds to the amount by which strong subadditivity of von Neumann entropy fails to be saturated. Our result therefore sheds light on the structure of states that *almost* satisfy strong subadditivity with equality. The proof of the lower bound is based on two recent results from quantum information theory: the operational interpretation of the quantum mutual information as the optimal rate for state redistribution [3] and the interpretation of the regularised relative entropy of entanglement as an error exponent in hypothesis testing [4].

Main result. The quantum conditional mutual information of a tripartite quantum state ρ_{ABE} measures the correlations between A and B relative to E and is defined as

$$I(A; B|E)_\rho = H(AE)_\rho + H(BE)_\rho - H(ABE)_\rho - H(E)_\rho.$$

Here, $H(A)_\rho$ is the von Neumann entropy of the reduced state $\rho_A = \text{Tr}_{BE} \rho_{ABE}$. This measure is always non-negative by strong subadditivity and in [5] a characterisation of states with $I(A; B|E) = 0$ was given. In particular, it was found that for such states, the reduced density matrix ρ_{AB} must be *separable*, i.e. of the form $\sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$. Our main result is an *approximate* version of this fact, which we will now discuss.

By analogy with the trace distance, which relates to the optimal probability of distinguishing two quantum states, the LOCC-norm distance $\|\rho - \sigma\|_{\text{LOCC}}$ of two bipartite states measures how well ρ and σ can be distinguished with local operations and classical communication (LOCC) only. Formally [6], $\|X\|_{\text{LOCC}} = \max_{A \in \text{LOCC}} |\text{tr}(AX)|$, where LOCC is the set of POVM elements which can be implemented by LOCC. We similarly define $\|*\|_{\text{LOCC} \rightarrow}$ as the LOCC norm restricted to one-way communication from A to B . Our main result is that for every tripartite quantum state ρ_{ABE} ,

$$I(A; B|E)_\rho \geq \frac{1}{2 \ln 2} \left(\min_{\sigma_{A:B} \in \mathcal{S}} \|\rho_{A:B} - \sigma_{A:B}\|_{\text{LOCC} \rightarrow} \right)^2, \quad (1)$$

where \mathcal{S} is the set of separable states on $A : B$. We note that (1) is known to be false for the trace norm since the ratio of the two sides might be as large as $\Omega(|A|)$, where $|A|$ denotes the dimension of A [7]. This shows the need for considering restricted norms in order to get a *dimension-independent* relation, something that is crucial for our applications. We will now use our main result (1) in order to find a lower bound on squashed entanglement.

The entanglement measure *squashed entanglement* is defined as [8]

$$E_{sq}(\rho_{A:B}) = \inf \left\{ \frac{1}{2} I(A; B|E) : \rho_{ABE} \text{ satisfies } \text{Tr}_E \rho_{ABE} = \rho_{AB} \right\}.$$

A central open question, posed already in [8], is whether squashed entanglement is faithful, i.e. strictly positive on every entangled state. An affirmative answer to this question follows from the following lower bound, which is a consequence of (1) and the monotonicity of E_{sq} under LOCC:

$$E_{sq}(\rho_{A:B}) \geq \frac{1}{4 \ln 2} \left(\min_{\sigma_{A:B} \in \mathcal{S}} \|\rho_{A:B} - \sigma_{A:B}\|_{\text{LOCC}} \right)^2. \quad (2)$$

As we will show in the following, the combination of (2) and the monogamy of squashed entanglement [9] has a number of interesting consequences outside entanglement theory.

Application 1: Quantum de Finetti theorem and data hiding. A state $\rho_{A:B}$ is k -extendible if there is a state $\rho_{A:B_1, \dots, B_k}$ that is permutation-symmetric in the B systems with $\rho_{A:B} = \rho_{A:B_1}$. Quantum versions of the de Finetti theorem [10, 11] show that any k -extendible state is $\frac{4|B|^2}{k}$ -close to a separable state in trace norm. A corollary of (2) is an exponentially improved bound for the LOCC norm: for every k -extendible $\rho_{A:B}$

$$\min_{\sigma_{A:B} \in \mathcal{S}} \|\rho_{A:B} - \sigma_{A:B}\|_{\text{LOCC}} \leq \left(\frac{4 \ln 2 \log |A|}{k} \right)^{\frac{1}{2}}. \quad (3)$$

Among other things, this shows that highly extendible states that are far away in trace norm from the set of separable states are *data hiding states* [12], which means that they can be used to globally store information that is not accessible by LOCC operations alone.

Application 2: A subexponential-time algorithm for deciding separability. In the weak-membership problem for separability one should decide if a given bipartite state $\rho_{A:B}$ is in the ϵ -interior of the set of separable states or ϵ -away from any separable state (in trace norm). The best known algorithms for the problem have worst case complexity $2^{\text{poly}(|A|, |B|) \log(1/\epsilon)}$, and the problem is NP-hard for $\epsilon = 1/\text{poly}(n)$ [13, 14]. Assuming that there is no subexponential-time algorithm for 3-SAT, even subexponential-time algorithms for separability of complexity up to $2^{O(\log^{1-\nu} |A| \log^{1-\mu} |B|)}$ for *constant* ϵ and any $\nu + \mu > 0$ can be ruled out [15].

Our de Finetti bound (3) implies an exponential improvement for the LOCC-norm version of this problem: There is a subexponential-time algorithm for deciding the weak membership problem for separability in the LOCC norm, running in time $2^{O(\epsilon^{-2} \log |A| \log |B|)}$. In fact, the algorithm is based on a well-known sequence of separability tests [16] and consists of searching for a $O(\log |A| \epsilon^{-2})$ -extension of $\rho_{A:B}$ with semidefinite programming.

Application 3: Quantum Merlin-Arthur games with multiple Merlins. The class QMA is a quantum analogue of NP and is formed by all languages that can be decided in polynomial-time by a quantum verifier who is given a quantum system of polynomially many qubits as a proof. It is natural to ask how robust this definition is and a few results are known in this direction [17–19].

Our de Finetti bound (3) gives a new characterisation of QMA, which at first sight might appear to be strictly more powerful: We show that QMA is the class of languages decidable in polynomial-time by a quantum verifier who is given k unentangled proofs and can measure them using any

polynomial-time implementable LOCC protocol (among the k proofs). This answers a question posed by Aaronson *et al.* [2].

Outline of the proof. We will give an outline of the proof of the main result (1). The described applications follow relatively straightforward from this result. Details can be found in [1].

Inequality (1) follows by chaining together three inequalities, each of which is a new result in entanglement theory and may be of independent interest:

$$I(A; B|E) \geq E_R^\infty(\rho_{A:BE}) - E_R^\infty(\rho_{A:E}) \geq D_{\text{LOCC}^+}(\rho_{A:B}) \geq \frac{1}{2 \ln 2} \left(\min_{\sigma \in \mathcal{S}} \|\rho_{A:B} - \sigma\|_{\text{LOCC}^+} \right)^2.$$

Here, $E_R^\infty(\rho_{A:B})$ is the regularised relative entropy of entanglement (see e.g. [4]), and $D_{\text{LOCC}^+}(\rho_{AB})$ is the optimal error exponent for distinguishing $\rho_{A:B}$ from separable states using one-way LOCC measurements in asymmetric hypothesis testing [4].

The first inequality strengthens the *non-lockability* relation for E_R [20], a key property of this entanglement measure. It also connects, in an unexpected way, E_{sq} and E_R^∞ . No relation between these two quantities was known before. The inequality is obtained by using the optimal protocol for state redistribution from [3] in order to trace subsystem B in a more efficient way.

The second inequality is a monogamy-like relation for E_R^∞ , the only one known to date. It is proven by exploring the result from [4] that $E_R^\infty = D_{\text{ALL}}$, with D_{ALL} defined in analogy with D_{LOCC^+} , but with no restrictions on the measurements available. Using the optimal measurements for $\rho_{A:E}$ and $\rho_{A:B}$ achieving $D_{\text{ALL}}(\rho_{A:E})$ and $D_{\text{LOCC}^+}(\rho_{A:B})$ we construct a measurement for $\rho_{A:BE}$ distinguishing it from separable states at a rate $D_{\text{ALL}}(\rho_{A:E}) + D_{\text{LOCC}^+}(\rho_{A:B})$, which is always smaller than $D_{\text{ALL}}(\rho_{A:BE})$ by the definition of the optimal rate. The inequality then follows from the relation $E_R^\infty = D_{\text{ALL}}$ [4].

Finally, the third inequality is an analogue of Pinsker's inequality for $D_{\text{LOCC}^+}(\rho_{A:B})$. Its proof is based on von Neumann's minimax theorem and a martingale property that separable states satisfy when they are subject to local measurements.

-
- [1] F.G.S.L. Brandão, M. Christandl and J. Yard, arXiv:1010.1750.
 - [2] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. Shor. *Theory of Computing* **5**, 1 (2009).
 - [3] J. Yard and I. Devetak. *IEEE Trans. Inf. Theory*, **55**, 11, p. 5339 (2009).
 - [4] F.G.S.L. Brandão and M.B. Plenio. *Comm. Math. Phys.* **295**, 791 (2010).
 - [5] P. Hayden, R. Jozsa, D. Petz and A. Winter. *Comm. Math. Phys.* **246**, 359 (2004).
 - [6] W. Matthews, S. Wehner and A. Winter. *Comm. Math. Phys.* **291**, 813 (2009).
 - [7] B. Ibinson, N. Linden and A. Winter. *Comm. Math. Phys.* **277**, 289 (2008).
 - [8] M. Christandl and A. Winter. *J. Math. Phys.* **45**, 829 (2004).
 - [9] M. Koashi and A. Winter. *Phys. Rev. A* **69**, 022309 (2004).
 - [10] R. Koenig and R. Renner. *J. Math. Phys.* **46**, 122108 (2005).
 - [11] M. Christandl, R. Koenig, G. Mitchison and R. Renner. *Comm. Math. Phys.* **273**, 473 (2007).
 - [12] D.P. DiVincenzo, D.W. Leung and B.M. Terhal. *IEEE Trans. Inf. Theory*, **48**, 580 (2002).
 - [13] L. Gurvits. *Proceedings of STOC '03*, p.10 (2003).
 - [14] S. Gharibian. *Quant. Inf. Comp.* **10**, 343 (2010).
 - [15] A. Harrow and A. Montanaro. arXiv:1001.0017.
 - [16] A.C. Doherty, P.A. Parrilo and F.M. Spedalieri. *Phys. Rev. A* **69**, 022308 (2004).
 - [17] C. Marriott and J. Watrous. *Computational Complexity* **14**, 122 (2005).
 - [18] S. Beigi, P.W. Shor and J. Watrous. arXiv:1004.0411.
 - [19] H. Kobayashi, K. Matsumoto and T. Yamakami. *Lect. Notes Comp. Sci.*, pg. 188 (2003).
 - [20] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. *Phys. Rev. Lett.* **94**, 200501 (2005).