PAPER • OPEN ACCESS

Quantumness of correlations, quantumness of ensembles and quantum data hiding

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

Quantumness of correlations, quantumness of ensembles and quantum data hiding

M Piani[1,2], V Narasimhachar[3] and J Calsamiglia[4]

[1] Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo ON N2L 3G1, Canada
[2] Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK
[3] Department of Physics and Astronomy and Institute for Quantum Science and Technology, University of Calgary, Calgary AB T2N 1N4, Canada
[4] Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
E-mail: mpiani@uwaterloo.ca, vnarasim@ucalgary.ca and john.calsamiglia@uab.cat

Received 13 May 2014, revised 25 August 2014
Accepted for publication 16 September 2014
Published 31 October 2014

New Journal of Physics **16** (2014) 113001

doi:10.1088/1367-2630/16/11/113001

Abstract

We study the quantumness of correlations for ensembles of bi- and multi-partite systems and relate it to the task of quantum data hiding. Quantumness is here intended in the sense of minimum average disturbance under local measurements. We consider a very general framework, but focus on local complete von Neumann measurements as the cause of the disturbance, and, later on, on the trace-distance as a quantifier of the disturbance. We discuss connections with entanglement and previously defined notions of quantumness of correlations. We prove that a large class of quantifiers of the quantumness of correlations are entanglement monotones for pure bipartite states. In particular, we define an entanglement of disturbance for pure states, for which we give an analytical expression. Such a measure coincides with negativity and concurrence for the case of two qubits. We compute general bounds on disturbance for both single states and ensembles, and consider several examples, including the uniform Haar ensemble of pure states, and pairs of qubit states. Finally, we show that the notion of ensemble quantumness of correlations is most relevant in quantum data hiding. Indeed, while it is known that entanglement is not necessary for a good

quantum data-hiding scheme, we prove that ensemble quantumness of correlations is necessary.

Keywords: quantumness, discord, entanglement, disturbance, data hiding, ensemble

1. Introduction

Although quantum entanglement (Horodecki *et al* 2009) constitutes one of the most counterintuitive aspects of quantum mechanics and is a key ingredient of quantum information processing (Nielsen and Chuang 2000), in recent years other, more general, quantum features of correlations have attracted much interest. The role of such general quantumness of correlations has been investigated in areas that go from the foundations of quantum mechanics, to thermodynamics, to quantum computation, to quantum information, to entanglement theory (Modi *et al* 2012).

Discord (Ollivier and Zurek 2001, Henderson and Vedral 2001), as well as a number of other related quantifiers (Modi *et al* 2012), were introduced to measure such general quantumness. Two fruitful and conceptually interesting approaches to measuring the quantumness of correlations are in terms of disturbance and extraction of correlations. The first approach, disturbance-based, identifies a distributed state as classical if local maximally informative measurements (that is, rank-one projections) exist that do not perturb the state (Luo 2008b). The second approach, based on the extraction of correlations, identifies a state as classical if local measurements exist that transfer all the correlations present between the quantum subsystems to classical variables/systems (Ollivier and Zurek 2001, Piani *et al* 2008). The two approaches are very tightly related, and the two classes of classical states they pin down—those that are not perturbed by local measurements and those whose correlations can be made classical, respectively—coincide (Modi *et al* 2012).

In this paper, we mostly focus on the quantumness of correlations as understood in terms of measurement-induced disturbance. In most of the recent literature on the quantumness of correlations, a single state distributed among many parties is typically considered. On the other hand, the study of the quantumness of ensembles of states has a long history [see, e.g., (Fuchs and Sasaki 2003, Horodecki *et al* 2005, 2006)]. Recently, the two concepts—the quantumness of correlations and the quantumness of ensembles—have been connected both conceptually and quantitatively. In particular, in (Luo *et al* 2010, 2011, Yao *et al* 2013), an approach was put forward where the quantumness of the ensembles is quantified in terms of the quantumness of correlations of a properly defined bipartite state.

In this paper, on one hand we take a step further and consider the quantumness of correlations of ensembles of distributed states. In particular, we point out how several quantumness measures—either of single-system ensembles, or of the correlations of a single state of a multipartite system, or of the correlations of an ensemble of states of a multipartite system—can be understood in the same formally unified approach.

On the other hand, we consider the role of the quantumness of correlations in quantum data hiding (Terhal *et al* 2001, DiVincenzo *et al* 2002). In its simplest instance, quantum data hiding consists of encoding a classical bit in a quantum state shared by distant parties—i.e., in letting these parties share one out of two possible quantum states—so that, while such a bit can be recovered perfectly or almost perfectly through a global—i.e., unrestricted—measurement that

discriminates between the two states, the bit is almost perfectly hidden from parties that are limited to act via local operations and classical communication (LOCC). It is known that quantum data hiding is possible using pairs of unentangled quantum states (Eggeling and Werner 2002). Nonetheless, it is easy to see that some quantumness of correlations must be at play. In the following we prove that, while there are hiding schemes where one of the two hiding states does not display any quantumness of correlations, on one hand (i) the lack of quantumness of correlations in one of the hiding states imposes limits on the hiding scheme and, on the other hand, (ii) the ensemble composed of the two states in a general hiding scheme must necessarily display a large quantumness of correlations, as quantified by one of the ensemble measures we introduce.

The paper is organized as follows. In section 2, we look at a general framework to quantify the quantumness of ensembles and the quantumness of correlations of ensembles. We further discuss relations with notions and measures of quantumness of ensembles and correlations already present in the literature, including entanglement. In section 3, we focus on the particular disturbance induced by complete projective measurements and quantified by the trace distance. We show that this kind of disturbance measure induces a natural entanglement measure on pure bipartite states, for which we provide an analytical expression. We also compute bounds on general disturbance measures and focus on some concrete examples. In section 4, we consider the role of the quantumness of correlations in quantum data hiding. We show how the disturbance-based measures of correlations we introduced and studied in the preceding sections provide natural bounds on the quality of quantum data-hiding schemes. We present concluding remarks in section 5.

2. Measures of ensemble-quantumness

As indicated in the introduction, we focus on the quantumness of ensembles of states as revealed in terms of the (average) disturbance necessarily induced by operations—in particular, measurements—in some restricted class.

2.1. Definitions

We adopt the following general definition for disturbance:

Definition 2.1. Given a measure $D[\,\cdot\,,\,\cdot\,]$ of distance between quantum states, and a set $\mathcal{L}$ of measurement strategies, we define the quantumness of an ensemble $\mathcal{E} := \{(p_i, \rho^{(i)})\}_{i=1}^{n}$ under $\mathcal{L}$ as measured by D, or simply the $(D, \mathcal{L})$-quantumness of $\mathcal{E}$, as

$$Q_{D,\mathcal{L}}[\mathcal{E}] := \inf_{\Lambda\in\mathcal{L}} \sum_{i=1}^{n} p_i D\left[\rho^{(i)}, \Lambda\left[\rho^{(i)}\right]\right], \tag{1}$$

where $\Lambda[\rho]$ denotes the resulting state—typically with classical features (see definition 2.3 below)—when ρ is subjected to Λ. Such a notion of quantumness is well-defined only when the operations Λ are such that the distance measure $D\left[\rho^{(i)}, \Lambda[\rho^{(i)}]\right]$ is well-defined.

Two meaningful distance measures to consider are the trace distance, $D_1[\sigma, \tau] = 1/2\,\|\sigma - \tau\|_1$, with $\|X\|_1 = \mathrm{Tr}\sqrt{X^\dagger X}$, and the relative entropy[5],

[5] Here we take the notion of distance in a loose sense, since the relative entropy is not a distance, as it is neither symmetric, nor satisfies the triangle inequality.

$S[\sigma \| \tau] = \mathrm{Tr}\,(\sigma(\log_2\sigma - \log_2\tau))$, because they have well-understood operational meanings in terms of state distinguishability (Nielsen and Chuang 2000). For the sake of simplicity, we will use the notation $Q_{D_1,\mathcal{L}}$ and $Q_{S,\mathcal{L}}$, respectively. Another sensible choice would be the Bures distance $\sqrt{1 - F(\sigma, \tau)}$ (or its square), with the fidelity $F(\sigma, \tau) = \mathrm{Tr}\sqrt{\sqrt{\sigma}\tau\sqrt{\sigma}}$ (Uhlmann 1976, Jozsa 1994), and we do use it in section 4, but we will mostly focus on the trace distance and the relative entropy.

As for $\mathcal{L}$, in order for our definition of ensemble quantumness to make sense, we must restrict it to sets of operations that admit a meaningful 'post-measurement state' from whence the distance measure is rendered meaningful. In principle, if the states in the ensemble are density matrices acting on a Hilbert space $\mathcal{X}$, any subset of the set of channels $C(\mathcal{X}) := \{\Lambda\colon L(\mathcal{X}) \to L(\mathcal{X}), \Lambda\}$ completely positive and trace preserving, where $L(\mathcal{X})$ is the set of operators from $\mathcal{X}$ to $\mathcal{X}$, would be a potential mathematically sound choice. Nonetheless, we aim here at capturing the idea of 'informative' measurement, either constrained or unconstrained, that necessarily leads to some disturbance for most states (see, e.g., (D'Ariano 2003, Kretschmann *et al* 2008, Luo 2008b) and references therein). Furthermore, we have in mind the following notions of classicality, for ensembles and for correlations, respectively (Fuchs and Sasaki 2003, Horodecki *et al* 2005, 2006, Groisman *et al* 2007, Piani *et al* 2008):

Definition 2.2. A set of states $\{\rho^{(i)}\}$ is *classical* if all the states in the set commute, i.e. $[\rho^{(i)}, \rho^{(j)}] = 0$ for all i, j, so that the states can be diagonalized simultaneously.

Definition 2.3. An n-partite state $\rho_{A_1A_2\ldots A_n}$ is classical on A_k if $\rho_{A_1A_2\ldots A_n} = \sum_i p_i\, |i\rangle\langle i|_{A_k} \otimes \langle i|_{A_k}\rho_{A_1A_2\ldots A_n}|i\rangle_{A_k}$ for some orthonormal basis $\{|i\rangle\}$ of A_k. In particular, a bipartite state ρ_{AB} is called *classical-quantum* if it is classical on A and *classical-classical* (or *fully classical*) if it is classical on both A and B.It is worth remarking that there are distributed states that are unentangled (or separable)—i.e., of the form $\sum_i p_i\rho_A^{(i)} \otimes \rho_B^{(i)}$—but not classical[6].

For these reasons, we mostly focus on complete projective measurements $\Pi := \{P^{(k)}\}_k$ acting as $\Pi[\sigma] = \sum_k P^{(k)}\sigma P^{(k)}$, and on complete local projective measurements $\Pi_A := \{P_A^{(j)}\}_j$ (on subsystem A; similarly for subsystem B) or complete bilocal ones $\Pi_A \otimes \Pi_B$ (and generalizations thereof for multipartite systems) when we want to focus on the quantumness of correlations. Of course, one could consider other generalizations, for example, to incomplete measurements, or to channels whose Kraus operators have some specified rank (Luo and Fu 2013, Gharibian 2012, Brodutch 2013), but for the sake of concreteness, we will limit ourselves to the explicit cases above.

For the sake of concreteness, we explicitly list the quantifiers of ensemble quantumness corresponding to the set of operations $\{\Pi\}$, $\{\Pi_A\}$ and $\{\Pi_A \otimes \Pi_B\}$, and to the two distance measures mentioned above:

[6] Notice that almost all multipartite states are not classical in the sense above (Ferraro *et al* 2010). This is an additional motivation to study general quantumness quantitatively, rather than qualitatively.

- ensemble quantumness for single systems:

$$Q_{D_1,\{\Pi\}}[\mathcal{E}] := \min_{\Pi} \sum_{i=1}^{n} p_i \frac{1}{2} \left\| \rho^{(i)} - \Pi\left[\rho^{(i)}\right] \right\|_1, \tag{2}$$

$$Q_{S,\{\Pi\}}[\mathcal{E}] := \min_{\Pi} \sum_{i=1}^{n} p_i S\left[\rho^{(i)} \middle\| \Pi\left[\rho^{(i)}\right]\right] = \min_{\Pi} \sum_{i=1}^{n} p_i \left[S\left(\Pi\left[\rho^{(i)}\right]\right) - S\left(\rho^{(i)}\right)\right]; \tag{3}$$

- ensemble quantumness of correlations:

- one-sided:

$$Q_{D_1,\{\Pi_A\}}[\mathcal{E}] := \min_{\Pi_A} \sum_{i=1}^{n} p_i \frac{1}{2} \left\| \rho^{(i)} - \Pi_A\left[\rho^{(i)}\right] \right\|_1, \tag{4}$$

$$Q_{S,\{\Pi_A\}}[\mathcal{E}] := \min_{\Pi_A} \sum_{i=1}^{n} p_i S\left[\rho^{(i)} \middle\| \Pi_A\left[\rho^{(i)}\right]\right] \tag{5}$$

$$= \min_{\Pi_A} \sum_{i=1}^{n} p_i \left[S\left(\Pi\left[\rho^{(i)}\right]\right) - S\left(\Pi_A\left[\rho^{(i)}\right]\right)\right]; \tag{6}$$

- two-sided:

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}[\mathcal{E}] := \min_{\Pi_A\otimes\Pi_B} \sum_{i=1}^{n} p_i \frac{1}{2} \left\| \rho^{(i)} - \left(\Pi_A \otimes \Pi_B\right)\left[\rho^{(i)}\right] \right\|_1. \tag{7}$$

$$Q_{S,\{\Pi_A\otimes\Pi_B\}}[\mathcal{E}] := \min_{\Pi_A\otimes\Pi_B} \sum_{i=1}^{n} p_i S\left[\rho^{(i)} \middle\| \left(\Pi_A \otimes \Pi_B\right)\left[\rho^{(i)}\right]\right] \tag{8}$$

$$= \min_{\Pi_A\otimes\Pi_B} \sum_{i=1}^{n} p_i \left[S\left(\Pi\left[\rho^{(i)}\right]\right) - S\left(\Pi_A \otimes \Pi_B\left[\rho^{(i)}\right]\right)\right]. \tag{9}$$

Note that we have used the fact that for projective measurements the infimum in (1) is in fact a minimum. In addition, for the measures based on relative entropy, we made use of the relation $S(\rho \,\|\, \Pi[\rho]) = S(\Pi[\rho]) - S(\rho)$, valid for any (not necessarily complete) projective measurement Π, with $S(\sigma) := -\mathrm{Tr}\,(\sigma \log_2 \sigma)$ the von Neumann entropy (Nielsen and Chuang 2000).

2.2. Some basic observations

We first remark that the use of one specific distance measure, rather than another one in general, strongly depends on the context and, potentially, on the convenience of calculation. For example, in the following, we will often focus on the quantity $Q_{D_1,\{\Pi_A\}}$ because of its natural connection with the task of discriminating distributed states via LOCC. On the other hand, it is natural to expect $Q_{S,\mathcal{L}}$ to be more relevant from an information-theoretical point of view (see section 2.3). Also, the quantumness measures $Q_{D_1,\mathcal{L}}$ are always bounded above by unity, and could be considered to be not so helpful in providing insight on the role of quantumness with increasing dimensions of the systems under scrutiny. We do not believe this to be a strong

contraindication to the adoption of measures in the class $Q_{D_1,\mathcal{L}}$; furthermore, one can always reinstate a scaling with dimensions via the composition with the logarithm function. For example, in section 3 we will find less trivial upper bounds for $Q_{D_1,\{\Pi_A\}}$, and show that, for fixed local dimension d, Q_{D_1,Π_A} is maximized by maximally entangled states—even in the case of the trivial ensemble made of only one state—assuming in such a case the value $1 - 1/d$. This suggests to define a logarithmic version of disturbance as

$$LQ_{D_1,\Pi_A} := -\log\left(1 - Q_{D_1,\Pi_A}\right).$$

Such a quantity varies between 0 for ensembles of states classical on A, to $\log d$ for (ensembles of) maximally entangled states (in dimension d).

In general, the properties of the measure $Q_{D,\mathcal{L}}[\mathcal{E}]$ will strongly depend on the properties of the distance D and of the class of operations $\mathcal{L}$. Some basic properties like invariance under unitaries or local unitaries are easily assessed for relevant choices of D and $\mathcal{L}$. Interestingly, if we suppose that D is jointly convex, as it happens for any norm-based distance—like the trace distance—and for the relative entropy, then $Q_{D,\mathcal{L}}[\mathcal{E}]$ is a monotone under coarse graining, independently of the choice of $\mathcal{L}$. More precisely, if $\mathcal{E}' = \{(p'_i, \rho'^{(i)})\}$ is such that $p'_i\rho'^{(i)} = \sum_{k\in I_i} p_k\rho^{(k)}$ for some starting ensemble $\mathcal{E} = \{(p_j, \rho^{(j)})\}_{j=1}^n$ and some partition $\left\{I_i\colon \cup_i\ I_i = \{1, 2, \ldots, n\}, I_i \cap I_j = \varnothing\ \ \forall\ i \neq j\right\}$, then

$$Q_{D,\mathcal{L}}[\mathcal{E}'] \leqslant Q_{D,\mathcal{L}}[\mathcal{E}].$$

A final remark is that through Pinsker's inequality (Hiai *et al* 1981, Schumacher and Westmoreland 2002), $\|\rho - \sigma\|_1^2 \leqslant (\ln 4) S[\rho\,\|\,\sigma]$, one easily derives the relation

$$Q_{D_1,\mathcal{L}}[\mathcal{E}] \leqslant \sqrt{\frac{\ln 2}{2}}\sqrt{Q_{S,\mathcal{L}}[\mathcal{E}]} \qquad \forall\ \mathcal{L}, \mathcal{E}. \tag{10}$$

2.3. Relations with other measures of quantumness and entanglement

In this section, we relate the family of quantities introduced in section 2 with quantifiers of quantumness already present in the existing literature.

2.3.1. Quantumness of correlations of a single state. In the case in which the ensemble $\mathcal{E}$ is trivial and contains only one state, i.e., $\mathcal{E} = \{(1, \rho)\}$, the ensemble measures become single-state measures, and we write $Q_{D,\mathcal{L}}[\rho]$ for $Q_{D,\mathcal{L}}(\{(1, \rho)\})$. In particular, the quantities introduced above trivially vanish in the case in which we consider single systems and 'global' complete von Neumann measurements, i.e.,

$$Q_{D_1,\{\Pi\}}[\rho] = Q_{S,\{\Pi\}}[\rho] = 0,$$

because one can always consider projective measurements in the eigenbasis of ρ. On the other hand, for a distributed state $\rho = \rho_{AB}$, all the following are non-trivial measures of the quantumness of correlations of ρ_{AB}:

$$Q_{D_1,\{\Pi_A\}}[\rho_{AB}] = \min_{\Pi_A}\frac{1}{2}\,\|\rho_{AB} - \Pi_A[\rho_{AB}]\|_1, \tag{11}$$

$$Q_{S,\{\Pi_A\}}[\rho_{AB}] = \min_{\Pi_A} S\Big[\rho_{AB}\Big\|\Pi_A[\rho_{AB}]\Big] = \min_{\Pi_A} S\Big(\Pi_A[\rho_{AB}]\Big) - S(\rho_{AB}), \tag{12}$$

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}[\rho_{AB}] = \min_{\Pi_A\otimes\Pi_B} \frac{1}{2}\,\|\rho_{AB} - (\Pi_A\otimes\Pi_B)[\rho_{AB}]\|_1, \tag{13}$$

$$Q_{S,\{\Pi_A\otimes\Pi_B\}}[\rho_{AB}] = \min_{\Pi_A\otimes\Pi_B} S\Big[\rho_{AB}\Big\|(\Pi_A\otimes\Pi_B)[\rho_{AB}]\Big] \tag{14}$$

$$= \min_{\Pi_A\otimes\Pi_B} S\Big((\Pi_A\otimes\Pi_B)[\rho_{AB}]\Big) - S(\rho_{AB}). \tag{15}$$

These four quantifiers correspond to the measurement-induced disturbance (Luo 2008b) due to one-sided or two-sided measurement, measured either entropically or by means of the trace-distance. The latter case, corresponding to a 'trace-norm discord', has been defined and studied in (Debarba *et al* 2012, Rana and Parashar 2013, Paula *et al* 2013, Nakano *et al* 2013); the entropic measures were instead introduced first as quantum deficits (Horodecki *et al* 2005). Such measures also correspond, either in general (in the entropic case) (Modi *et al* 2010) or at least in relevant special cases (for the trace-norm) (Paula *et al* 2013, Nakano *et al* 2013), to the distance of the given state from the set of classical–quantum or classical–classical states. Another interpretation worth mentioning of such measures, again valid either in general or in special cases, is that in terms of entanglement generated in a quantum measurement (Streltsov *et al* 2011, Piani *et al* 2011, Gharibian *et al* 2011, Piani and Adesso 2012, Adesso *et al* 2014). We refer to (Nakano *et al* 2013) for a recent and more extensive summary of the relevant properties and relations between these measures.

2.3.2. Quantumness of single-system ensembles as quantumness of correlations. Given a generic ensemble $\mathcal{E} = \{(p_i, \rho_S^{(i)})\}_{i=1}^n$ for a system S, one can associate with it a bipartite state $\rho_{SX}(\mathcal{E}) = \sum_i p_i\rho_S^{(i)} \otimes |i\rangle\langle i|_X$. Using the fact that for relative entropy (Nielsen and Chuang 2000, Cover and Thomas 2012, Piani 2009)

$$S\left[\sum_i p_i\rho_S^{(i)} \otimes |i\rangle\langle i|_X \,\middle\|\, \sum_i p_i\sigma_S^{(i)} \otimes |i\rangle\langle i|_X\right] = \sum_i p_i S\Big[\rho_S^{(i)}\Big\|\sigma_S^{(i)}\Big], \tag{16}$$

and that the trace norm of a block diagonal matrix is equal to the sum of the trace norms of the blocks, i.e., $\big\|\oplus_i M_i\big\|_1 = \sum_i \big\|M_i\big\|_1$ (Bhatia 1997), so that

$$\left\|\sum_i p_i\rho_S^{(i)} \otimes |i\rangle\langle i|_X - \sum_i p_i\sigma_S^{(i)} \otimes |i\rangle\langle i|_X\right\|_1 = \sum_i p_i\,\|\rho_S^{(i)} - \sigma_S^{(i)}\|_1, \tag{17}$$

we have the identities

$$Q_{D_1,\{\Pi_S\}}\Big[\rho_{SX}(\mathcal{E})\Big] = Q_{D_1,\{\Pi\}}(\mathcal{E}) = Q_{D_1,\{\Pi_S\otimes\Pi_X\}}\Big[\rho_{SX}(\mathcal{E})\Big], \tag{18}$$

$$Q_{S,\{\Pi_S\}}\Big[\rho_{SX}(\mathcal{E})\Big] = Q_{S,\{\Pi\}}(\mathcal{E}) = Q_{S,\{\Pi_S\otimes\Pi_X\}}\Big[\rho_{SX}(\mathcal{E})\Big], \tag{19}$$

where the last equality in each of the above equations is due to the fact that Π_X can be chosen to project in the basis $\{|i\rangle_X\}$. On the other hand, the first equality in each equation holds independently of the class of operations $\mathcal{L}$ considered, that is, for example,

$$Q_{D_1,\mathcal{L}_S}\left[\rho_{SX}(\mathcal{E})\right] = Q_{D_1,\mathcal{L}}(\mathcal{E}), \quad \forall\ \mathcal{L}.$$

The approach consisting of using tools originally introduced to quantify the quantumness of correlations to instead quantify the quantumness of ensembles was already put forward in, e.g., (Luo *et al* 2010, 2011, Yao *et al* 2013), in particular making use of the relative entropy. Here, we emphasize that this is a general fact that actually applies to any distance measure that respects a 'direct sum' rule such as (16) and (17), and fits in a general paradigm as the one we laid out in section 2. For example, in the case where S is a composite system itself, that is, $S = AB$, one can have similar relations for the (bipartite) quantumness of correlations of an ensemble of states $\{(p_i, \rho_{AB}^{(i)})\}$ of AB and the (tripartite) quantumness of correlations of a tripartite state $\rho_{ABX}(\mathcal{E}) = \sum_i p_i \rho_{AB}^{(i)} \otimes |i\rangle\langle i|_X$, like

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}\left[\rho_{ABX}(\mathcal{E})\right] = Q_{D_1,\{\Pi_A\otimes\Pi_B\otimes\Pi_X\}}\left[\rho_{ABX}(\mathcal{E})\right] = Q_{D_1,\{\Pi_A\otimes\Pi_B\}}\left[\left\{\left(p_i, \rho_{AB}^{(i)}\right)\right\}\right].$$

2.3.3. Quantumness of ensembles for a single mixed state and convex-roof constructions. In section 2.3.1, we have seen how our general ensemble quantifiers can reduce to quantifiers for a single state in the case of a trivial ensemble. There are other, less trivial ways to use our ensemble measures when we deal with a single state.

One possibility is that of considering ensemble realizations of that state. For example, we can consider an arbitrary pure-state ensemble $\mathcal{E}(\rho) = \left\{(p_i, |\psi^{(i)}\rangle\langle\psi^{(i)}|)\right\}$ such that $\rho = \sum_i p_i\ |\psi^{(i)}\rangle\langle\psi^{(i)}|$. The idea, then, is that of defining a single-state quantifier of quantum correlations based on a minimization over such a decomposition, i.e.,

$$Q^{\mathrm{ens}}_{D,\mathcal{L}}(\rho) := \min_{\mathcal{E}(\rho)} Q_{D,\mathcal{L}}(\mathcal{E}(\rho)).$$

As discussed in section 2.2, if D is jointly convex, then $Q_{D,\mathcal{L}}(\mathcal{E})$ is monotonic under coarse-graining of $\mathcal{E}$, and one has the relation

$$Q^{\mathrm{ens}}_{D,\mathcal{L}}(\rho) \geqslant Q_{D,\mathcal{L}}(\rho).$$

We notice that a state that is classical on, let us say, A will admit pure-state ensemble decompositions, where all the pure states in the ensemble are classical in the same basis. So, for example, $Q_{D_1,\{\Pi_A\}}(\rho_{AB}) = 0$ implies $Q^{\mathrm{ens}}_{D_1,\{\Pi_A\}}(\rho_{AB}) = 0$.

On the other hand, given a mixed state, one can again use pure-state ensemble realizations of that state, but consider the so-called convex-roof construction

$$Q^{\mathrm{cr}}_{D,\mathcal{L}}(\rho) := \min_{\mathcal{E}(\rho)} \sum_i p_i Q_{D,\mathcal{L}}\left(\left|\psi^{(i)}\right\rangle\left\langle\psi^{(i)}\right|\right). \tag{20}$$

This construction is the standard one used to extend many entanglement measures from bi- and multi-partite pure states to mixed states (Horodecki *et al* 2009), and indeed $Q^{\mathrm{cr}}_{D,\mathcal{L}}(\rho)$ is an entanglement measure if $Q_{D,\mathcal{L}}(|\psi\rangle\langle\psi|)$ is an entanglement monotone on pure states $|\psi\rangle$ (Vidal 2000, Horodecki 2001). Note that in the following, we often use the shorthand notation $\psi = |\psi\rangle\langle\psi|$, hence writing $Q_{D,\mathcal{L}}(\psi)$.

Notice that the difference between $Q^{\mathrm{cr}}_{D,\mathcal{L}}(\rho)$ and $Q^{\mathrm{ens}}_{D,\mathcal{L}}(\rho)$, both defined for a single state ρ, is that the infimum entering in definition (1) is or is not, respectively, adapted to each element of the pure-state ensemble of ρ. This automatically implies

$$Q^{\mathrm{ens}}_{D,\mathcal{L}}(\rho) \geqslant Q^{\mathrm{cr}}_{D,\mathcal{L}}(\rho), \tag{21}$$

independently of the convexity properties of D.

2.3.4. Quantumness and entanglement. When we say that we are interested in a quantumness of correlations that is more general than entanglement, we have in mind a hierarchy that, above all, is qualitative, but may also be cast in quantitative terms, depending on the choice of quantifiers for entanglement and general quantumness. What we expect is that the general quantumness of correlations will be larger than entanglement also quantitatively. A generic approach that leads to a consistent quantitative hierarchy, i.e., a hierarchy in which the quantumness of correlations is always greater than entanglement, is the one based on the mapping of said quantumness into entanglement itself through a measurement interaction (Streltsov *et al* 2011, Piani *et al* 2011, Gharibian *et al* 2011, Piani and Adesso 2012, Coles 2012, Nakano *et al* 2013, Adesso *et al* 2014). Another such hierarchy is the one that naturally arises by considering distance measures from various sets that form a hierarchy themselves (Modi *et al* 2010).

In the latter spirit, if one considers the relative entropy of entanglement (Vedral *et al* 1997, Vedral and Plenio 1998)

$$E_R\left[\rho_{AB}\right] := \min_{\sigma_{AB}\ \text{separable}} S\left[\rho_{AB}\,\|\,\sigma_{AB}\right],$$

it is easy to see that $Q_{S,\{\Pi_A\}}(\rho_{AB}) \geqslant E_R[\rho_{AB}]$, since $\Pi_A[\rho_{AB}]$ is necessarily separable for Π_A a complete von Neumann measurement. On the other hand, $Q_{S,\{\Pi_A\}}$ and the entanglement of formation (Bennett *et al* 1996)

$$E_F\left[\rho_{AB}\right] := \min_{\mathcal{E}(\rho_{AB})} \sum_i p_i S\left(\mathrm{Tr}_A\left(\left|\psi^{(i)}_{AB}\right\rangle\left\langle\psi^{(i)}_{AB}\right|\right)\right)$$

do not respect a hierarchy (Luo 2008a), i.e., there exist states ρ_{AB} and σ_{AB} such that

$$Q_S,\left\{\Pi_A\right\}(\rho_{AB}) < E_F(\rho_{AB}) \quad \text{and} \quad Q_{S,\{\Pi_A\}}(\sigma_{AB}) > E_F(\sigma_{AB}).$$

We observe here that instead

$$Q^{\mathrm{ens}}_{S,\{\Pi_A\}}(\rho_{AB}) \geqslant E_F[\rho_{AB}].$$

Indeed, for a pure state, $Q_{S,\{\Pi_A\}}(|\psi_{AB}\rangle\langle\psi_{AB}|) = S\left(\mathrm{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)\right) = E_F(|\psi_{AB}\rangle\langle\psi_{AB}|)$ (Luo 2008b), so that $Q^{\mathrm{cr}}_{S,\{\Pi_A\}}(\rho_{AB}) = E_F[\rho_{AB}]$, and we can invoke the general relation (21).

2.4. Entanglement monotones based on disturbance

Here, we prove that a large class of measures $Q_{D,\mathcal{L}_A}$, including $Q_{S,\{\Pi_A\}}$ and $Q_{D,\{\Pi_A\}}$, when restricted to single bipartite pure states (see section 2.3.1), are entanglement monotones. By this, we mean that said quantifiers do not increase *on average* under stochastic LOCC (SLOCC) (Vidal 2000).

Theorem 2.4. *For any distance measure D that*

(i) is invariant under unitaries,

(ii) is monotonic under general quantum operations (this condition actually comprises (i)),

(iii) respects the 'flags' condition[7] $D(\sum_i p_i\rho_i \otimes |i\rangle\langle i|, \sum_i p_i\sigma_i \otimes |i\rangle\langle i|) = \sum_i p_i D(\rho_i, \sigma_i)$*, for* $\{p_i\}$ *a probability distribution,* $\{\rho_i\}$*,* $\{\sigma_i\}$ *states, and* $\{|i\rangle\}$ *orthogonal flags,*

and for any class $\mathcal{L}_A$ *of local operations* Λ_A *that is closed under conjugation by unitaries, i.e., if* Λ_A *is in* $\mathcal{L}_A$ *then also* $U_A^\dagger\Lambda_A[U_A\cdot U_A^\dagger]U_A$ *is in* $\mathcal{L}_A$ *for all* U_A*, one has that* $Q_{D,\mathcal{L}_A}(\psi_{AB})$ *is an entanglement monotone on average, i.e.*

$$Q_{D,\mathcal{L}_A}(\psi_{AB}) \geqslant \sum_i p_i Q_{D,\mathcal{L}_A}\left(\phi_{AB}^i\right),$$

where $\{p_i, \phi_{AB}^i\}$ *is a pure-state ensemble obtained from* ψ_{AB} *by local operations and classical communication.*

Proof. We first note that $Q_{D,\mathcal{L}_A}(\psi_{AB})$ depends only on the Schmidt coefficients $\{p_i\}$ of $|\psi_{AB}\rangle = U_A\otimes U_B|\phi_{AB}\rangle$ with $|\phi_{AB}\rangle = \sum\sqrt{p_i}|ii\rangle_{AB}$. This follows from the unitary invariance of D and from $U_A^\dagger\Lambda_A[U_A\cdot U_A^\dagger]U_A = \Lambda'_A[\,\cdot\,]\in\mathcal{L}_A$:

$$\begin{aligned} Q_{D,\mathcal{L}_A}(\psi_{AB}) &= \min_{\Lambda_A\in\mathcal{L}_A} D\left(U_A^\dagger\otimes U_B^\dagger\psi_{AB}U_A\otimes U_B,\, U_A^\dagger\otimes U_B^\dagger\Lambda_A[\psi_{AB}]U_A\otimes U_B\right) \\ &= \min_{\Lambda'_A\in\mathcal{L}_A} D\left(\phi_{AB}, \Lambda'_A\left[\phi_{AB}\right]\right)\Big) = f(\{p_i\}). \end{aligned}$$

Given the symmetry of the state $|\phi_{AB}\rangle$ if is clear that

$$Q_{D,\mathcal{L}_A}(\psi_{AB}) = \min_{\Lambda_A\in\mathcal{L}_A} D\left(\psi_{AB}, \Lambda_A[\psi_{AB}]\right) = \min_{\Lambda_B\in\mathcal{L}_B} D\left(\psi_{AB}, \Lambda_B[\psi_{AB}]\right) = Q_{D,\mathcal{L}_B}(\psi_{AB}), \tag{22}$$

i.e., we can consider indifferently a minimization over projections on Alice's or Bob's side. In order to prove monotonicity *on average*, it is sufficient to prove monotonicity under unilocal transformations, i.e., stochastic operations defined through

$$\left|\phi_{AB}^i\right\rangle = C_A^i|\psi\rangle_{AB}\Big/\sqrt{p_i} \qquad p_i = \mathrm{Tr}\left(C_A^i\,|\psi\rangle\langle\psi|\,C_A^{i\dagger}\right), \tag{23}$$

where the C_A^i's are the Kraus operators of a generic quantum operation on Alice's side. If monotonicity holds under such operations, and the same holds for operations on Bob's side, then monotonicity *on average* under general LOCC follows, because an LOCC protocol is just a sequence of adaptive unilocal operations (Vidal 2000). To this end,

$$\begin{aligned} Q_{D,\mathcal{L}_B}(\psi_{AB}) &= \min_{\Lambda_B\in\mathcal{L}_B} D\left(\psi_{AB}, \Lambda_B[\psi_{AB}]\right) \\ &\geqslant \min_{\Lambda_B\in\mathcal{L}_B} D\left(\sum_i C_A^i\psi_{AB}C_A^{i\dagger}\otimes|i\rangle\langle i|_{A'}, \sum_i C_A^i\Lambda_B[\psi_{AB}]C_A^{i\dagger}\otimes|i\rangle\langle i|_{A'}\right) \\ &= \min_{\Lambda_B\in\mathcal{L}_B} D\left(\sum_i p_i\phi_i\otimes|i\rangle\langle i|_{A'}, \sum_i p_i\Lambda_B\left[\phi_i\right]\otimes|i\rangle\langle i|_{A'}\right) \end{aligned}$$

[7] See (Horodecki 2005) for the use of the 'flags' condition in entanglement theory.

$$
\begin{aligned}
&= \min_{\Lambda_B \in \mathcal{L}_B} \sum_i p_i D\left(\phi_i, \Lambda_B\left[\phi_i\right]\right)\Bigg) \\
&\geqslant \sum_i p_i \min_{\Lambda_B \in \mathcal{L}_B} D\left(\phi_i, \Lambda_B\left[\phi_i\right]\right) \\
&= \sum_i p_i Q_{D,\mathcal{L}_B}\left(\phi_i\right).
\end{aligned}
$$

The first inequality is due to monotonicity of the distance D under quantum operations, in this case the application of local Kraus operators, with the 'which-operator' information stored in a classical local flag. Notice that the quantum operation on Alice and the projection on Bob commute. Simply moving the measuring operation to Alice's side thanks to (22), similar steps can be taken in the case of a unilocal operation on Bob's side. □

It will be important in this work to establish bounds on the quantumness of states and ensembles. For this purpose, it is useful to note that *maximal quantumness corresponds to maximal entanglement*.

Corollary 2.5. *For a given fixed dimension of A, d_A, maximally entangled states are maximally quantum-correlated with respect to any measure $Q_{D,\mathcal{L}_A}(\rho_{AB})$ that respects the conditions of theorem 2.4.*

Proof. In (Streltsov *et al* 2012) it was already proven that a measure of correlations Q that does not increase under operations on at least one side must be maximal on pure states. It is easy to verify that monotonicity under operations of D implies monotonicity under operations on B for any $Q_{D,\mathcal{L}_A}$. Furthermore, any pure state of A and B can be obtained via LOCC—in particular, with one-way communication from Bob to Alice—from a maximally entangled state of Schmidt rank d_A. □

3. Trace-norm disturbance: analysis and bounds

Our main goal here is that of finding non-trivial bounds on $Q_{D,\mathcal{L}}(\mathcal{E})$, focusing on measures like $Q_{D_1,\{\Pi_A\}}$ and $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}$. The latter have the interpretation of quantifiers of the quantumness of correlations in terms of measurement-induced disturbance, where the change is quantified by means of a distance with an operational meaning—the trace distance. This will make such measures key in the connection between ensemble quantumness and quantum data hiding that we will establish in section 4.

To find bounds on ensemble quantumness, we notice that, in general, if D is jointly convex

$$
\begin{aligned}
Q_{D,\mathcal{L}}[\mathcal{E}] &= \min_{\Lambda \in \mathcal{L}} \sum_{i=1}^{n} p_i D\left[\rho^{(i)}, \Lambda\left[\rho^{(i)}\right]\right] \\
&\leqslant \min_{\Lambda \in \mathcal{L}} \max_{|\psi\rangle} D\left[|\psi\rangle\langle\psi|, \Lambda\left[|\psi\rangle\langle\psi|\right]\right].
\end{aligned} \tag{24}
$$

For example, we want to calculate

$$\min_{\Pi}\max_{|\psi\rangle}\frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \Pi\,[|\psi\rangle\langle\psi|]\,\|_1 = \max_{|\psi\rangle}\frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \bar{\Pi}\,[|\psi\rangle\langle\psi|]\,\|_1$$

for the sake of bounding $Q_{D_1,\{\Pi\}}$. Here we got rid of the minimization over the projector, since any change of basis for the projection is irrelevant once we consider the maximization over pure states. Similarly, for the sake of bounding $Q_{D_1,\{\Pi_A\}}$, it will be enough to calculate $\max_{|\psi_{AB}\rangle}\frac{1}{2}\,\|\,|\psi_{AB}\rangle\langle\psi_{AB}| - \bar{\Pi}_A\,[|\psi_{AB}\rangle\langle\psi_{AB}|]\,\|_1$.

To begin, it is worth considering with more attention the single-state measures $Q_{D_1,\{\Pi_A\}}$ of equation (11) and $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}$ of equation (13), evaluated on pure states. On one hand, consideration of such measures is interesting in itself; on the other hand, we will see that the tools that we will develop will be useful also to bound ensemble quantumness.

3.1. Trace-norm disturbance for pure states: Entanglement of disturbance

The following lemma will be the key in the study of the maximum disturbances induced by a complete projective measurement on system A, for the case of a bipartite pure state.

Lemma 3.1. *In the case of a bipartite pure state $|\psi\rangle_{AB}$, the disturbance caused by a one-sided complete projective measurement Π_A on A, as measured by the trace distance, is given by the positive c such that*

$$\sum_i \frac{p_i}{c + p_i} = 1, \tag{25}$$

for $p_i = \langle i|\,\rho_A\,|i\rangle$, with $\rho_A = \mathrm{Tr}_B\,|\psi\rangle\langle\psi|$, the probability of obtaining outcome i by measuring in the local orthonormal basis $\{|i\rangle\}$.

Proof. Let $|\psi\rangle = \sum_i |i\rangle_A|w_i\rangle_B$, with the vectors $|w_i\rangle$ not necessarily orthogonal and satisfying $\langle w_i|w_i\rangle = p_i$. Then $\Pi_A\,[|\psi\rangle\langle\psi|] = \sum_i |i\rangle\langle i| \otimes |w_i\rangle\langle w_i|$. We observe that for any vector $|v\rangle$ and any positive-semidefinite A, the positive-definite part of $|v\rangle\langle v| - A$ can have a rank of at most 1, and consequently, if $|v\rangle\langle v| - A$ is traceless, then $\|\,|v\rangle\langle v| - A\,\|_1 = 2\,\|\,|v\rangle\langle v| - A\,\|_\infty$. In our case then,

$$\frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \Pi_A\,[|\psi\rangle\langle\psi|]\,\|_1 = \|\,|\psi\rangle\langle\psi| - \Pi_A\,[|\psi\rangle\langle\psi|]\,\|_\infty .$$

To further simplify things, let us consider a generic normalized vector $|\phi\rangle = \sum_i |i\rangle|z_i\rangle$, where, similarly as before, the vectors $|z_i\rangle$ are not necessarily orthogonal and satisfy $\langle z_i|z_i\rangle = q_i$, with q_i the probability of the outcome i when measuring A in the basis $\{|i\rangle\}$. One has

$$\begin{aligned}
\|\,|\psi\rangle\langle\psi| - \Pi_A\,[|\psi\rangle\langle\psi|]\,\|_\infty &= \max_{|\phi\rangle}\langle\phi|\big(|\psi\rangle\langle\psi| - \Pi_A\,[|\psi\rangle\langle\psi|]\big)|\phi\rangle \\
&= \max_{|\phi\rangle}\left|\sum_i \big\langle z_i\big|w_i\big\rangle\right|^2 - \sum_i \big|\big\langle z_i\big|w_i\big\rangle\big|^2 \\
&= \max_{|\phi\rangle}\sum_{i>j}\Big(\big\langle z_i\big|w_i\big\rangle\big\langle w_j\big|z_j\big\rangle + \big\langle z_j\big|w_j\big\rangle\big\langle w_i\big|z_i\big\rangle\Big)
\end{aligned}$$

$$
\begin{aligned}
&= 2 \max_{|\phi\rangle} \sum_{i>j} \Re\Big(\big\langle z_i \big| w_i \big\rangle \big\langle w_j \big| z_j \big\rangle \Big) \\
&= 2 \max_{|q\rangle} \sum_{i>j} \sqrt{q_i p_i q_j p_j} \\
&= \max_{|q\rangle} \left(\sum_i \sqrt{q_i p_i} \right)^2 - \sum_i q_i p_i \\
&= \max_{|q\rangle} \langle q | \left(|p\rangle\langle p| - \sum_i p_i \, |i\rangle\langle i| \right) |q\rangle,
\end{aligned}
$$

where we have introduced the notation $|p\rangle = \sum_i \sqrt{p_i}\, |i\rangle$ (similarly for $|q\rangle$), and used that $\Re(\langle z_i|w_i\rangle\langle w_j|z_j\rangle) \leqslant \sqrt{q_i p_i q_j p_j}$, with equality achieved for $|z_i\rangle = (\sqrt{q_i}/\sqrt{p_i})|w_i\rangle$. Thus, it is sufficient to find the largest (positive) eigenvalue of the operator $|p\rangle\langle p| - \sum_i p_i \, |i\rangle\langle i|$, which we know will be achieved by $|q\rangle$ of the form $|q\rangle = \sum_i \sqrt{q_i}\, |i\rangle$. With this ansatz, we set

$$
\left(|p\rangle\langle p| - \sum_i p_i \, |i\rangle\langle i| \right) |q\rangle = c \, |q\rangle,
$$

from which we find the scalar relations

$$
\langle p|q\rangle \sqrt{p_i} - p_i \sqrt{q_i} = c \sqrt{q_i},
$$

i.e.,

$$
\sqrt{q_i} = \langle p|q\rangle \frac{\sqrt{p_i}}{c + p_i}.
$$

Imposing consistency for $\sum_i \sqrt{p_i q_i} = \langle p|q\rangle$, i.e., imposing

$$
\sum_i \sqrt{p_i q_i} = \sum_i \sqrt{p_i} \left(\langle p|q\rangle \frac{\sqrt{p_i}}{c + p_i} \right) = \langle p|q\rangle \sum_i \frac{p_i}{c + p_i} \equiv \langle p|q\rangle,
$$

and noticing that (25) is monotonically decreasing (and hence invertible) for $c \geqslant 0$, we arrive at the condition of the statement. □

We now make another preliminary observation.

Lemma 3.2. *Let* $\{p_i\}$ *indicate a probability distribution. Then*

$$
f_c(\{p_i\}) := \sum_i \frac{p_i}{c + p_i}
$$

is Schur-concave in $\{p_i\}$ *for fixed* $c \geqslant 0$. *It is also monotonically decreasing for fixed* $\{p_i\}$ *and for increasing positive* c. *Define also the function*

$$
c(\{p_i\}) := \text{ the unique } c \geqslant 0 \text{ such that } f_c(\{p_i\}) = \sum_i \frac{p_i}{c + p_i} = 1
$$

on probability vectors. The function $c(\{p_i\})$ *is Schur-concave in* $\{p_i\}$.

Proof. The Schur-concavity of f_c is a simple consequence of the concavity of $x/(c+x)$ in $x \geqslant 0$ for $c \geqslant 0$, and of the symmetry of f_c in the p_i's. Monotonicity in c is evident.

Consider now a probability distribution $p_i' = \sum_j B_{ij} p_j$ obtained from the probability distribution p_{i_i} by multiplication by a bistochastic matrix B_{ij}. Because of the Schur concavity of $f_c(\{p_i\})$ in $\{p_i\}$ for fixed c, we have

$$\begin{aligned} 1 &= f_{c(\{p_i\})}(\{p_i\}) \\ &= \sum_j \frac{p_j}{c(\{p_i\}) + p_j} \\ &\leqslant \sum_i \frac{p_i'}{c(\{p_i\}) + p_i'} \\ &= f_{c(\{p_i\})}\left(\left\{p_i'\right\}\right). \end{aligned}$$

Because of the monotonicity of $f_c(\{p_i\})$ in c for fixed $\{p_i\}$, we conclude that $c(\{p_i'\}) \geqslant c(\{p_i\})$. This proves that $c(\{p_i\})$ is a Schur-concave function of $\{p_i\}$. □

Thus we arrive at:

Theorem 3.3. *The one-sided trace-norm disturbance*

$$Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|) = \min_{\Pi_A} \frac{1}{2} \| |\psi\rangle\langle\psi| - \Pi_A[|\psi\rangle\langle\psi|] \|_1$$

is a bona fide entanglement monotone for the bipartite pure state $|\psi\rangle = \sum_i \sqrt{p_i}\, |i\rangle|i\rangle$*, here expressed in its Schmidt decomposition. The minimum disturbance is obtained by measuring in the local Schmidt basis and is equal to the positive c such that*

$$\sum_i \frac{p_i}{c + p_i} = 1. \tag{26}$$

The same holds for the two-sided trace-norm disturbance

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(|\psi\rangle\langle\psi|) = \min_{\Pi_A\otimes\Pi_B} \frac{1}{2} \| |\psi\rangle\langle\psi| - (\Pi_A \otimes \Pi_B)[|\psi\rangle\langle\psi|] \|_1,$$

so that we have $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(|\psi\rangle\langle\psi|) = Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|)$ *for all* $|\psi\rangle_{AB}$.

Proof. From lemma 3.1, we have that $\frac{1}{2} \| |\psi\rangle\langle\psi| - \Pi_A[|\psi\rangle\langle\psi|] \|_1$ is equal to $c(\{q_i\})$ where q_i is the probability of outcome i in the local projective measurement. Let the latter take place in the local Schmidt basis of $|\psi\rangle = \sum_i \sqrt{p_i}\, |i\rangle|i\rangle$, so that $q_i = p_i$. Let $\{|u_j\rangle\}$ be any other orthonormal basis. The probability of the outcome j in such an alternative basis is

$$\begin{aligned} p'_j &= \left\langle u_j \right| \rho_A \left| u_j \right\rangle \\ &= \left\langle u_j \right| \left(\sum_i p_i \left| i \right\rangle\!\left\langle i \right| \right) \left| u_j \right\rangle \\ &= \sum_i p_i \left| \left\langle u_j \middle| i \right\rangle \right|^2. \end{aligned}$$

Since the coefficients $B_{ij} = |\langle u_j|i\rangle|^2$ form the entries of a bistochastic matrix, the Schur concavity of $c(\{q_i\})$ (lemma 3.2) lets us conclude that measurement in the Schmidt basis is optimal for the sake of disturbance.

Note that, similarly, the Schur concavity of $c(\{q_i\})$ in $\{q_i\}$ ensures that $Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|) = c(\{p_i\})$, for $\{\sqrt{p_i}\}$ the Schmidt coefficients of $|\psi\rangle$, is a *bona fide* entanglement measure on pure states (Nielsen 1999, Vidal 2000) for deterministic LOCC transformations. Recall that theorem 2.4 already shows that a wide class of disturbance measures, including $Q_{D_1,\{\Pi_A\}}$, are entanglement monotones on pure states, i.e., they are non-increasing *on average* under (non-deterministic) LOCC. Hence, it provides a proof for a stronger form of monotonicity.

Finally, to see that $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(|\psi\rangle\langle\psi|) = Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|)$, realize that it again holds

$$\frac{1}{2}\left\| |\psi\rangle\langle\psi| - \left(\Pi_A \otimes \Pi_B\right)[|\psi\rangle\langle\psi|] \right\|_1 = \max_{|\phi\rangle} \langle\phi| \left(|\psi\rangle\langle\psi| - \left(\Pi_A \otimes \Pi_B\right)[|\psi\rangle\langle\psi|] \right) |\phi\rangle.$$

Consider Π_A projecting in the local Schmidt basis and $|\phi\rangle = \sum_i \sqrt{q_i}\,|i\rangle|i\rangle$ optimal choices for the sake of achieving $\max_{|\phi\rangle} \langle\phi| \left(|\psi\rangle\langle\psi| - \Pi_A[|\psi\rangle\langle\psi|] \right) |\phi\rangle = Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|) = |\sum_i \sqrt{p_i q_i}|^2 - \sum_i p_i q_i$ (see the proof lemma 3.1), in the case of the one-sided measurement. Then, coming back to two-sided projective measurements,

$$\begin{aligned} &\max_{|\phi\rangle} \langle\phi| \left(|\psi\rangle\langle\psi| - \left(\Pi_A \otimes \Pi_B\right)[|\psi\rangle\langle\psi|] \right) |\phi\rangle \\ &\quad \geqslant \langle\phi| \left(|\psi\rangle\langle\psi| - \left(\Pi_A \otimes \Pi_B\right)[|\psi\rangle\langle\psi|] \right) |\phi\rangle \\ &\quad \geqslant \left| \sum_i \sqrt{p_i q_i} \right|^2 - \sum_i p_i q_i \operatorname{Tr}\left(\Pi_B[|i\rangle\langle i|]\Pi_B[|i\rangle\langle i|]\right). \end{aligned}$$

Since $\operatorname{Tr}(\Pi_B[|i\rangle\langle i|]\Pi_B[|i\rangle\langle i|]) \leqslant 1$ for all choices of Π_B, and since Π_A was optimal for $Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|)$, we have proven $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(|\psi\rangle\langle\psi|) \geqslant Q_{D_1,\{\Pi_A\}}(|\psi\rangle\langle\psi|)$. The last inequality can be saturated for Π_B, a projection in the local Schmidt basis of B. □

We will call $Q_{D_1,\{\Pi_A\}}$ the *entanglement of disturbance* when considering it on pure states, and denote it as $E^{\text{disturbance}}(\psi_{AB})$. Since it is an entanglement monotone *on average*, it can be naturally extended to an entanglement measure on mixed states by a convex-roof construction[8]:

$$E^{\text{disturbance}}(\rho_{AB}) := Q^{\text{cr}}_{D_1,\{\Pi_A\}}(\rho_{AB}) = \min_{\mathcal{E}(\rho)} \sum_i p_i E^{\text{disturbance}}\left(\left|\psi^{(i)}\right\rangle\!\left\langle\psi^{(i)}\right| \right). \quad (27)$$

[8] This would not necessarily be true if only deterministic monotonicity were proven.

We remark that Bravyi (Bravyi 2003) also studied and quantified entanglement of pure states as a property that implies non-vanishing disturbance under local measurements, but chose entropy —equivalently, relative entropy—as a disturbance quantifier.

It is instructive to consider some simple cases to get a flavor of the new measure of entanglement, in particular to see how the formula (26) plays out. Obviously, in the case of a factorized state $|\alpha\rangle|\beta\rangle$, we have only one non-zero p_i, which is equal to 1. So, condition (26) becomes $1/(c+1)=1$, which is satisfied by $c=0$, as expected. In the case of a maximally entangled state of two qudits, one has $p_i = 1/d$ for $i = 1,...,d$. So, (26) becomes $d\frac{1/d}{c+1/d}=1$, which is solved by $c = 1 - 1/d$; this is the maximal value of minimal disturbance due to local projective measurements on pure states of two qudits. For a pure state of two qubits, the probability distribution reads $\{p_i\} = \{p, 1-p\}$, and (26) becomes

$$\frac{p}{c+p}+\frac{1-p}{c+1-p}=1,$$

which is satisfied by $c=\sqrt{p(1-p)}$. The latter is the same as the negativity of entanglement (Vidal and Werner 2001) [and, up to a constant factor, concurrence (Wootters 1998)], as to be expected from (Nakano *et al* 2013, Ciccarello *et al* 2014).

We conclude this section by providing some explicit upper and lower bounds for $E = E^{\text{disturbance}}$. We recall that the main result of theorem 3.3 can be restated as the fact that the entanglement of disturbance of $|\psi_{AB}\rangle$ is the positive number E such that

$$\sum_i \frac{p_i}{E+p_i}=1,$$

where the p_i's are the Schmidt coefficients of $|\psi_{AB}\rangle$. This is an analytic expression for E, as E can simply be considered the inverse of the function $y=f(x)=\sum_i \frac{p_i}{x+p_i}$—with the Schmidt coefficients considered as parameters—evaluated at $y=1$. Nonetheless, we provide here some bounds in terms of more standard functions.

In order to find an upper bound to E, we can consider the following steps:

$$\begin{aligned}
1 &= \sum_i \frac{p_i}{E+p_i} \\
&= \frac{p_1}{E+p_1}+(R-1)\sum_{i=2}^{R}\frac{1}{R-1}\left(\frac{p_i}{E+p_i}\right) \\
&\leqslant \frac{p_1}{E+p_1}+(R-1)\frac{\sum_{i=2}^{R}\frac{1}{R-1}p_i}{E+\sum_{i=2}^{R}\frac{1}{R-1}p_i} \\
&= \frac{p_1}{E+p_1}+\frac{1-p_1}{E+\frac{1-p_1}{R-1}},
\end{aligned}$$

where the inequality is due to the concavity of $x/(1+x)$, p_1 is the largest probability, and R is the rank (the number of non-vanishing p_i's). From this, we find the bound

$$E \leqslant \frac{-2 + 2p_1 + R - p_1 R + \sqrt{4 - 4p_1 - 4R + 4p_1^2 R + R^2 + 2p_1 R^2 - 3p_1^2 R^2}}{2(-1+R)}$$
$$\leqslant \frac{1}{2}\left(1 - p_1 + \sqrt{-3p_1^2 + 1 + 2p_1}\right), \tag{28}$$

where the second bound is obtained from the first in the limit $R \to \infty$ (see figure 1). On the other hand, to find a lower bound, we can consider

$$\begin{aligned} 1 &= \sum_i \frac{p_i}{E + p_i} \\ &= \frac{p_1}{E + p_1} + \sum_{i=2}^{R} \frac{p_i}{E + p_i} \\ &\geqslant \frac{p_1}{E + p_1} + \sum_{i=2}^{R} \frac{p_i}{E + p_2} \\ &= \frac{p_1}{E + p_1} + \frac{1 - p_1}{E + p_2}. \end{aligned} \tag{29}$$

Here p_2 is the second largest probability, hence the inequality. From this, we can find

$$E \geqslant \frac{1}{2}\left(1 - p_1 - p_2 + \sqrt{-3p_1^2 + \left(-1 + p_2\right)^2 + 2p_1\left(1 + p_2\right)}\right) \geqslant 1 - p_1,$$

where the rightmost bound is obtained by setting $p_2 \equiv p_1$, i.e., loosening the inequality in (29).

Both the upper and the lower bound can be checked to be good, in that they converge to the actual value of $E^{\text{disturbance}}$ in both the limit of an unentangled state and a maximally entangled one.

3.2. Bounds on disturbance

We would like to remark on the difference between calculating (bounds for) the maximal disturbance on *one* distributed state, and on an *ensemble* of distributed states. This is because the measurement in the first case can be tailored to the particular state. More concretely, while

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(\psi) \leqslant \max_{|\phi_{AB}\rangle} \min_{\{\Pi_A\otimes\Pi_B\}} \frac{1}{2} \left\| |\phi\rangle\langle\phi|_{AB} - \left(\Pi_A \otimes \Pi_B\right)\left[|\phi\rangle\langle\phi|_{AB}\right] \right\|_1,$$

we have (see equation (24))

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(\mathcal{E}) \leqslant \min_{\{\Pi_A\otimes\Pi_B\}} \max_{|\phi_{AB}\rangle} \frac{1}{2} \left\| |\phi\rangle\langle\phi|_{AB} - \left(\Pi_A \otimes \Pi_B\right)\left[|\phi\rangle\langle\phi|_{AB}\right] \right\|_1.$$

In particular, theorem 3.3 implies

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(\psi) \leqslant 1 - 1/d_A, \tag{30}$$

to be compared with the ensemble bound (35) of corollary 3.6 below, here reported for the convenience of the reader:

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(\mathcal{E}) \leqslant 1 - 1/(d_A d_B).$$

Nonetheless, as anticipated, in our quest for bounds for the quantumness of ensembles, we will be able to take advantage of the results and techniques developed in section 3.1.

To begin, we remark how in the proof of lemma 3.1 we used a decomposition $|\psi\rangle = \sum_i |i\rangle|w_i\rangle$; this was to analyze projective measurements of the first system in the basis $\{|i\rangle\}$, with the $|w_i\rangle$'s neither orthonormal nor normalized. It is easy to convince oneself that all the calculations we did remain valid in the case of a single system, as long as we interpret the $|w_i\rangle$'s as complex numbers. Therefore, we find

Theorem 3.4. *In the case of a single-system pure state ψ, the disturbance caused by a complete projective measurement Π in the orthonormal basis $\{|i\rangle\}$, as measured by the trace distance is given by the positive c such that*

$$\sum_i \frac{p_i}{c + p_i} = 1. \tag{31}$$

for $p_i = |\langle i|\psi\rangle|^2$.

We are thus able to find a bound on the quantumness of ensembles, based on the maximum disturbance caused by a fixed projective measurement.

Corollary 3.5. *The maximum disturbance of one state under a von Neumann measurement in dimension d, minimized over all measurements and maximized over all states, is given by:*

$$\begin{aligned}\min_{\{|i\rangle\}_{i=1}^d} \max_\rho \frac{1}{2} \left\| \rho - \sum_{i=1}^d (|i\rangle\langle i|\,\rho\,|i\rangle\langle i|) \right\|_1 \\ = \max_\rho \frac{1}{2} \left\| \rho - \sum_{i=1}^d (|i\rangle\langle i|\,\rho\,|i\rangle\langle i|) \right\|_1 = 1 - \frac{1}{d},\end{aligned} \tag{32}$$

where $\{|i\rangle\}_{i=1}^d$ denotes a general orthonormal basis spanning the space. Thus,

$$Q_{D_1,\{\Pi\}}(\mathcal{E}) \leqslant 1 - \frac{1}{d}. \tag{33}$$

Proof. The maximum is attained by a pure state because of the convexity of the trace-norm. From theorem 3.4 and the Schur concavity of c as a function of the probabilities $\{p_i\}$ (lemma 3.2), it is clear that the maximum is attained for the flat probability distribution $p_i = 1/d$, which can be obtained by measuring the state $(\sum_{i=1}^d |i\rangle)/\sqrt{d}$ in the basis $\{|i\rangle\}$. □

Thus, as one may expect, the worst disturbance is obtained by considering a pure state and a projective measurement in a basis that is unbiased with respect to that state, so that $\|\psi\rangle\langle\psi| - \Pi[|\Psi\rangle\langle\Psi|]\|_1 = \|\psi\rangle\langle\psi| - \mathbb{1}/d\|_1 = 2(1 - 1/d)$.

In the bipartite case, the upper bound can be achieved even without entanglement, by local projective measurements acting on appropriately 'skewed' local pure states. We thus have

Corollary 3.6. *The maximum disturbance of one bipartite state under local complete von Neumann measurements in local dimensions d_A and d_B is given by:*

$$\min_{\{|i\rangle_A\}_{i=1}^{d_A},\{|j\rangle_B\}_{i=1}^{d_B}} \max_{\rho_{AB}} \frac{1}{2} \left\| \rho - \sum_{i=1}^{d_A}\sum_{j=1}^{d_B} \left(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_B\right)\rho_{AB}\left(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_B\right) \right\|_1$$
$$= 1 - \frac{1}{d_A d_B}. \tag{34}$$

Thus,

$$Q_{D_1,\{\Pi_A\otimes\Pi_B\}}(\mathcal{E}) \leqslant 1 - \frac{1}{d_A d_B}. \tag{35}$$

These results can be generalized to the multipartite case, and one can cast the bound on disturbance in the following general way.

Theorem 3.7. *Consider a composite system $A_1A_2\ldots A_n$, with local dimensions $d_1, d_2, \ldots, d_n$. The maximum disturbance under complete projective measurements on $A_{k_1}A_{k_2}\ldots A_{k_m}$, with $\{k_1, k_2, \ldots, k_m\} \subseteq \{1, 2, \ldots, n\}$ is given by:*

$$\min_{\Pi_{Ak1Ak2\ldots Akm}} \max_{\rho_{A1A2\ldots An}} \frac{1}{2} \left\| \rho_{A_1A_2\ldots A_n} - \Pi_{A_{k1}A_{k2}\ldots A_{km}}\left[\rho_{A_1A_2\ldots A_n}\right] \right\|_1 = 1 - \frac{1}{d_{A_{k1}} d_{A_{k2}} \cdots d_{A_{km}}}, \tag{36}$$

independently of whether the minimization is over arbitrary complete projective measurements on $A_{k_1}A_{k_2}\ldots A_{k_m}$ or over local—with respect to an arbitrary grouping of $A_{k_1}A_{k_2}\ldots A_{k_m}$—ones. Thus,

$$Q_{D_1,\left\{\Pi_{Ak1Ak2\ldots Akm}\right\}}(\mathcal{E}) \leqslant 1 - \frac{1}{d_{A_{k1}} d_{A_{k2}} \cdots d_{A_{km}}}. \tag{37}$$

We notice that it is possible to tighten all the above bounds on disturbance if one takes also into account the probabilities of the various states in the ensemble. In particular, using a consideration similar to the one used to bound the relative entropy of quantumness of classical-quantum states in (Gharibian *et al* 2011), one can derive the following.

Theorem 3.8. *Consider a composite system $A_1A_2\ldots A_n$, with local dimensions $d_1, d_2, \ldots, d_n$. Suppose $\mathcal{E}$ is an ensemble comprising, with probability q, a state $\rho = \rho_{A_1A_2\ldots A_n}$ which is classical on the individual systems $A_{k_1}A_{k_2}\ldots A_{k_m}$; then*

$$Q_{D_1,\Pi_{Ak1Ak2\ldots Akm}}(\mathcal{E}) \leqslant (1-q)\left(1 - \frac{1}{d_{A_{k1}} d_{A_{k2}} \cdots d_{A_{km}}}\right),$$

independently of whether the minimization is over arbitrary complete projective measurements or over local ones. In particular, if there are n states in the ensemble and they all are classical on the individual systems $A_{k_1}A_{k_2}\ldots A_{k_m}$, then

$$Q_{D_1,\Pi_{A_{k1}A_{k2}\ldots A_{km}}}(\mathcal{E}) \leqslant \left(1-\frac{1}{n}\right)\left(1-\frac{1}{d_{A_{k1}}d_{A_{k2}}\cdots d_{A_{km}}}\right).$$

Proof. Consider a projection $\bar{\Pi} = \bar{\Pi}_{A_{k1}A_{k2}\ldots A_{km}}$ that leaves ρ invariant. Without loss of generality, assume ρ is the first state listed in the ensemble. Then

$$\begin{aligned} Q_{D_1,\left\{\Pi_{A_{k1}A_{k2}\ldots A_{km}}\right\}}(\mathcal{E}) &= \min_{\left\{\Pi=\Pi_{A_{k1}A_{k2}\ldots A_{km}}\right\}} \sum_{i=1}^{n} p_i D_1\left(\rho_i, \Pi\left[\rho_i\right]\right) \\ &\leqslant q D_1\left(\rho, \bar{\Pi}\left[\rho\right]\right) + \sum_{i=2}^{n} p_i D_1\left(\rho, \bar{\Pi}\left[\rho\right]\right) \\ &\leqslant \sum_{i=2}^{n} p_i \left(1-\frac{1}{d_{A_{k1}}d_{A_{k2}}\cdots d_{A_{km}}}\right) \\ &= (1-q)\left(1-\frac{1}{d_{A_{k1}}d_{A_{k2}}\cdots d_{A_{km}}}\right). \end{aligned} \tag{38}$$

The first inequality is due to the choice of a particular projection $\bar{\Pi}$. The second inequality comes from the fact that $\bar{\Pi}$ is such that $\bar{\Pi}[\rho] = \rho$, so that $D_1(\rho, \bar{\Pi}[\rho]) = 0$, and from the general bound (36), applied to all the other states in the ensemble.

For the second claim, it suffices to notice that if all n states in the ensemble are classical on the individual systems $A_{k_1}A_{k_2}\ldots A_{k_m}$ (possibly in different local orthonormal bases), then at least one of them has the associated probability $q \geqslant 1/n$, because probabilities must sum up to 1. □

It is worth recalling that, if one considers a single system, every given state is classical in its eigenbasis. So, as an application of theorem 3.8 we find the following improvement over equation (33):

$$Q_{D_1,\{\Pi\}}(\mathcal{E}) \leqslant \left(1-p_{\max}\right)\left(1-\frac{1}{d}\right) \leqslant \left(1-\frac{1}{n}\right)\left(1-\frac{1}{d}\right), \tag{39}$$

where d is the dimension of the system, $p_{\max}$ is the largest among all probabilities with which each state appears in the ensemble, and n is the number of elements in the ensemble. Notice that, because of the identity (18), these bounds on the disturbance of ensembles of a single system can be immediately used to bound the disturbance of correlations of $d \times n$ quantum-classical states ρ_{SX}.

3.3. Examples

In this section, we compute, or provide bounds for, the quantumness of ensembles, both for single systems and for correlations, for some interesting examples. These include qubit ensembles and uniform ensembles of pure states. As we will see, both kinds of examples seem to indicate that the general bound we found are quite good.

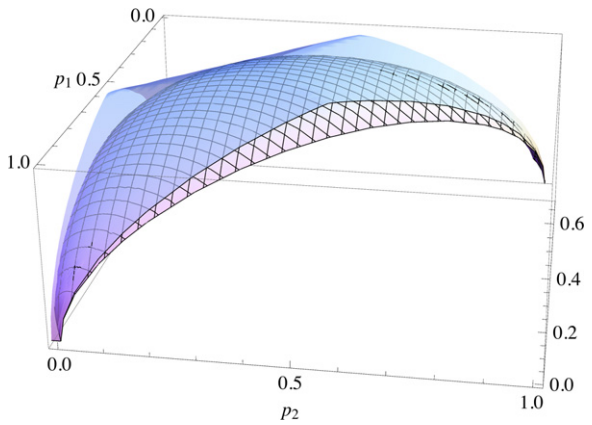

Figure 1. Comparison of $E^{\text{disturbance}}$ (lower graph) and the upper bound of equation (28) (upper, semitransparent graph) in the case $d = 3$ (d is the local dimension). The upper bound is closer to the exact value for highly entangled states corresponding to $p_1, p_2 \approx 1/3$ (for which also $p_3 = 1 - p_1 - p_2 \approx 1/3$).

3.3.1. Qubits. We start by providing a general formula for the single-system ensemble quantumness of ensembles of qubit states.

Theorem 3.9. *The* $(D_1, \{\Pi\})$*-quantumness of an ensemble* $\mathcal{E} := \left\{ (p_i, \rho^{(i)}) \right\}_{i=1}^{n}$ *of qubit states is given by*

$$Q_{D_1,\{\Pi\}}[\mathcal{E}] = \frac{1}{2} \min_{\hat{v}\in S^2} \sum_{i=1}^{n} p_i \, \|\vec{r}_i\| \left| \sin\left[\angle(\hat{v}, \vec{r}_i) \right] \right|, \tag{40}$$

where the minimization is performed over all vectors $\hat{v}$ *on the Bloch sphere,* $\vec{r}_i$ *is the Bloch vector corresponding to* $\rho^{(i)}$, $\|\cdot\| \equiv \|\cdot\|_2$ *is the Euclidean norm on* $\mathbb{R}^3$, $\angle(\hat{v}, \vec{r}_i)$ *is the angle between the two vectors named.*

Proof. For some qubit state $\rho = \frac{1}{2}\left(\mathbb{1} + \vec{r}\cdot\vec{\sigma}\right)$, if Π is the projective measurement along a basis corresponding to the unit vector $\hat{v}$, then

$$\begin{aligned}\Pi[\rho] &= \tfrac{1}{2^3}\left(\mathbb{1} + \hat{v}\cdot\vec{\sigma}\right)\left(\mathbb{1} + \vec{r}\cdot\vec{\sigma}\right)\left(\mathbb{1} + \hat{v}\cdot\vec{\sigma}\right) + \tfrac{1}{2^3}\left(\mathbb{1} - \hat{v}\cdot\vec{\sigma}\right)\left(\mathbb{1} + \vec{r}\cdot\vec{\sigma}\right)\left(\mathbb{1} - \hat{v}\cdot\vec{\sigma}\right) \\ &= \tfrac{1}{2}\left(\mathbb{1} + \left(\hat{v}\cdot\vec{r}\right)\hat{v}\cdot\vec{\sigma}\right).\end{aligned} \tag{41}$$

Therefore,

$$\begin{aligned}\|\rho - \Pi[\rho]\|_1 &= \left\| \tfrac{1}{2}\left(\mathbb{1} + \vec{r}\cdot\vec{\sigma} - \mathbb{1} - \left(\hat{v}\cdot\vec{r}\right)\hat{v}\cdot\vec{\sigma}\right) \right\|_1 \\ &= \tfrac{1}{2}\left\| \left(\vec{r} - \left(\hat{v}\cdot\vec{r}\right)\hat{v}\right)\cdot\vec{\sigma} \right\|_1 \\ &= \left\| \vec{r} - \left(\hat{v}\cdot\vec{r}\right)\hat{v} \right\| \\ &= \|\vec{r}\| \left| \sin\left[\left(\hat{v}, \vec{r}\right) \right] \right|.\end{aligned} \tag{42}$$

The result follows by the definition of $Q_{D_1,\{\Pi\}}$. □

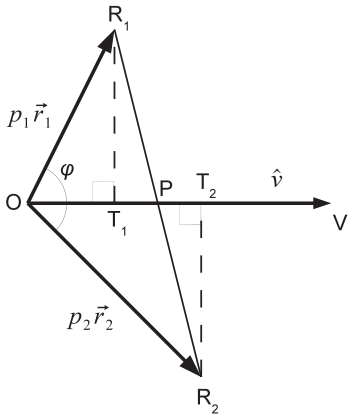

Figure 2. Calculation of optimal projective measurement for the least disturbance for an ensemble of two qubit states. $\hat{v}$ indicates the direction of the projective measurement; $p_i\vec{r}_i$, $i = 1, 2$, are the rescaled (by the probability in the ensemble) Bloch vectors of the two states. φ is the angle between such rescaled Bloch vectors. The optimal $\hat{v}$ can always be chosen in the plane defined by the two Bloch vectors, so the problem is a two-dimensional one. The point O corresponds to the centre of the Bloch sphere, and the point P is the point of intersection of $\hat{v}$ and the segment R_1R_2 connecting the endpoints of the two rescaled Bloch vectors.

In the case where the qubit ensemble contains two elements, we are able to provide an explicit analytical formula.

Corollary 3.10. *In the case of an ensemble consisting of two one-qubit states (the case $n = 2$ in theorem 3.9), the minimum comes out to be*

$$Q_{D_1,\{\Pi\}}\left[\left\{\left(p,\rho^{(1)}\right),\left(1-p,\rho^{(2)}\right)\right\}\right]=\frac{1}{2}\left|\sin\left[\angle\left(\vec{r}_1,\vec{r}_2\right)\right]\right|\min\left[p\,\|\vec{r}_1\|,(1-p)\,\|\vec{r}_2\|\right]. \quad (43)$$

Proof. It is clear that we should choose $\hat{v}$ to lie in the plane defined by $\vec{r}_1$ and $\vec{r}_2$. This is because, for a fixed angle between $\hat{v}$ and $\vec{r}_1$, the smallest angle between $\hat{v}$ and $\vec{r}_2$ is achieved for $\hat{v}$ lying in such a plane. Having reduced the problem to a two-dimensional one, we can prove the claim by simply considering figure 2.

In terms of the geometric elements present in figure 2, our objective function can be recast as

$$\begin{aligned}Q_{D_1,\{\Pi\}}\left[\left\{\left(p,\rho^{(1)}\right),\left(1-p,\rho^{(2)}\right)\right\}\right]&=\frac{1}{2}\min_{\hat{v}\in S^2}\Big(p_1\,\|\vec{r}_1\|\,\left|\sin\left[\angle\left(\hat{v},\vec{r}_1\right)\right]\right|\\&\quad+p_2\,\|\vec{r}_2\|\,\left|\sin\left[\angle\left(\hat{v},\vec{r}_1\right)\right]\right|\Big)\\&=\min_{\hat{v}\in S^2}\frac{1}{2}\Big(d\left(R_1,T_1\right)+d\left(R_2,T_2\right)\Big),\end{aligned}$$

where we have used the notation $d(X, Y)$ to denote the Euclidean distance between two points X and Y. We now notice that $\frac{1}{2}d(R_1, T_1)d(O, P)$ is the area of the triangle OPR_1. Similarly,

$\frac{1}{2}d(R_2, T_2)d(O, P)$ is the area of the triangle OPR_2. The sum of the two areas gives the area of the triangle OR_1R_2, independently of the position of P, i.e., independently of the choice of $\vec{v}$ in the plane. So

$$\frac{1}{2}d\big(R_1, T_1\big)d(O, P) + \frac{1}{2}d\big(R_2, T_2\big)d(O, P) = \frac{1}{2}\Big(d\big(R_1, T_1\big) + d\big(R_2, T_2\big)\Big)d(O, P) = \text{const.}$$

Thus, it is clear that $\hat{v}$ should be chosen to maximize $d(O, P)$. This can be done by choosing the measurement axis $\hat{v}$ parallel to the longest $p_i\vec{r}_i$. In such a case $\frac{1}{2}(d(R_1, T_1) + d(R_2, T_2)) = \frac{1}{2}\left|\sin\left[\angle(\vec{r}_1, \vec{r}_2)\right]\right|\min\left[p\,\|\vec{r}_1\|, (1-p)\,\|\vec{r}_2\|\right]$. □

Via the relations (18), which equate the quantumness of correlations of a classical-quantum system to the quantumness of a single-system ensemble, we conclude that the classical-quantum state of two qubits that exhibits the largest one-sided quantumness of correlations, as measured by trace-distance disturbance, is, up to local unitaries, the state

$$\frac{1}{2}\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}\,|+\rangle\langle +| \otimes |1\rangle\langle 1|, \tag{44}$$

for which $Q_{D_1,\Pi_A} = 1/4$. It is worth remarking that this quantumness matches the upper bound (39). The same state (44) is the classical-quantum state exhibiting the largest quantumness of correlations also according to the entropic disturbance (Gharibian *et al* 2011).

3.3.2. Uniform ensembles. In this section, we will consider uniform ensembles of pure states, that is, ensembles $\mathcal{E}_{\text{Haar}}$ of pure states distributed according to the Haar measure (Bengtsson and Życzkowski 1996). We will begin with the calculation of the trace-distance single-system ensemble quantumness, $Q_{D_1,\{\Pi\}}$, and move later to the trace-distance ensemble quantumness of correlations, both one-sided, $Q_{D_1,\{\Pi_A\}}$, and two-sided, $Q_{D_1,\{\Pi_A\otimes\Pi_B\}}$.

By symmetry considerations[9], it is clear that the choice of basis for the measurement is irrelevant: the average disturbance is going to be the same in all local bases. So

$$Q_{D_1,\{\Pi\}}\left(\mathcal{E}_{\text{Haar}}\right) = \min_{\Pi}\int \mathrm{d}\psi \frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \Pi\left[|\psi\rangle\langle\psi|\right]\|_1 = \int \mathrm{d}\psi \frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \Pi\left[|\psi\rangle\langle\psi|\right]\|_1,$$

where the projection on the rightmost-hand side is fixed arbitrarily. We find

$$\begin{aligned}\int \mathrm{d}\psi \frac{1}{2}\,\|\,|\psi\rangle\langle\psi| - \Pi\left[|\psi\rangle\langle\psi|\right]\|_1 &\geqslant \int \mathrm{d}\psi\left(1 - \langle\psi|\,\Pi\left[|\psi\rangle\langle\psi|\right]|\psi\rangle\right)\Big) \\ &= 1 - \int \mathrm{d}\psi\ \mathrm{Tr}\left(\Pi\left[|\psi\rangle\langle\psi|\right]^2\right) \\ &= 1 - \int \mathrm{d}\psi\ \mathrm{Tr}((\Pi\left[|\psi\rangle\langle\psi|\right] \otimes \Pi\left[|\psi\rangle\langle\psi|\right])W)\end{aligned}$$

[9] Alternatively, it can be checked.

$$
\begin{aligned}
&= 1 - \int \mathrm{d}\psi \ \mathrm{Tr}((|\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|)((\Pi \otimes \Pi)[V])) \\
&= 1 - \mathrm{Tr}\left(\left(\int \mathrm{d}\psi \, |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|\right)(\Pi \otimes \Pi)[W]\right) \\
&= 1 - \mathrm{Tr}\left(\frac{\mathbb{1} + W}{d(d+1)}(\Pi \otimes \Pi)[W]\right) \\
&= 1 - \mathrm{Tr}\left(\frac{\mathbb{1} + W}{d(d+1)} \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i|\right) \\
&= 1 - \frac{2d}{d(d+1)} \\
&= 1 - \frac{2}{d+1}.
\end{aligned}
$$

In the above, we have introduced the swap operator W acting on two copies of the Hilbert space according to $W|\alpha\rangle|\beta\rangle = |\beta\rangle|\alpha\rangle$. For any arbitrary choice of orthonormal basis $\{|i\rangle\}$, W admits the decomposition $W = \sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i|$. We used two useful standard identities involving W: $\mathrm{Tr}_{1,2}((X_1 \otimes Y_2)W_{1,2}) = \mathrm{Tr}\,(XY)$ and $\int \mathrm{d}\psi \, |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| = \frac{\mathbb{1}+W}{d(d+1)}$[10]. On the other hand,

$$
\begin{aligned}
Q_{D_1,\{\Pi\}}\left(\mathcal{E}_{\mathrm{Haar}}\right) &\leqslant \int \mathrm{d}\psi \sqrt{1 - \langle\psi|\,\Pi\,[|\psi\rangle\langle\psi|]|\psi\rangle} \\
&\leqslant \sqrt{1 - \int \mathrm{d}\psi \, \langle\psi|\,\Pi\,[|\psi\rangle\langle\psi|]|\psi\rangle} \\
&= \sqrt{1 - \frac{2}{d+1}} \\
&= 1 - \frac{1}{d+1} + O\left(d^{-2}\right)
\end{aligned}
$$

In corollary 3.5, we had found that the greatest trace-distance disturbance, maximized over states, is equal to $1 - 1/d$ in dimension d, and used the same value to bound the (single-system) ensemble disturbance. From the calculations above we see that the ensemble disturbance over the Haar ensemble is essentially the maximal one.

We move now to the one-sided trace-distance quantumness of correlations, $Q_{D_1,\{\Pi_A\}}$. We can actually follow several of the steps above to arrive to

$$
\begin{aligned}
Q_{D_1,\{\Pi_A\}}\left(\mathcal{E}_{\mathrm{Haar}}\right) \quad &\geqslant 1 - \mathrm{Tr}\left(\frac{\mathbb{1}_{A_1A_2B_1B_2} + W_{A_1B_1:A_2B_2}}{d_{AB}(d_{AB}+1)}\left(\Pi_{A_1} \otimes \Pi_{A_2}\right)\left[W_{A_1B_1:A_2B_2}\right]\right) \\
&= 1 - \mathrm{Tr}\left(\frac{\mathbb{1}_{A_1A_2B_1B_2} + W_{A_1:A_2} \otimes W_{B_1:B_2}}{d_{AB}(d_{AB}+1)}\left(\Pi_{A_1} \otimes \Pi_{A_2}\right)\left[W_{A_1:A_2} \otimes W_{B_1:B_2}\right]\right)
\end{aligned}
$$

[10] The first identity can be checked by direct inspection; the second identity can be proved by invoking Schur's lemma in representation theory.

$$= 1 - \mathrm{Tr}\left(\frac{\mathbb{1}_{A_1A_2B_1B_2} + W_{A_1:A_2} \otimes W_{B_1:B_2}}{d_{AB}(d_{AB}+1)} \left(\sum_i |i\rangle\langle i|_{A_1} \otimes |i\rangle\langle i|_{A_2} \right) \otimes W_{B_1:B_2} \right)$$

$$= 1 - \frac{d_A d_B + d_A d_B^2}{d_{AB}(d_{AB}+1)}$$

$$= 1 - \frac{d_B + 1}{d_A d_B + 1}.$$

In the derivation, we have used $d_{AB} = d_A d_B$ and that the swap operator between two copies A_1B_1 and A_2B_2 of AB can be written as the product of the swaps of the copies of the subsystems, i.e., $W_{A_1B_1:A_2B_2} = W_{A_1:A_2} \otimes W_{B_1:B_2}$. Similarly as before, we also find the upper bound

$$Q_{D_1,\{\Pi_A\}}\left(\mathcal{E}_{\mathrm{Haar}}\right) \leqslant \sqrt{1 - \frac{d_B + 1}{d_A d_B + 1}}$$

Notice also that in this case the average disturbance is comparable with the maximal disturbance for local projective measurements that we computed, $1 - 1/d_A$.

Finally, it should be clear from the steps in the proof above that, when we consider the two-sided ensemble quantumness of correlations, we go back to the bounds that we obtained for a single system, just with the dimension equal to the total dimension, $d = d_{AB} = d_A d_B$, obtaining

$$1 - \frac{2}{d_A d_B + 1} \leqslant Q_{D_1,\{\Pi_A \otimes \Pi_B\}}\left(\mathcal{E}_{\mathrm{Haar}}\right) \leqslant \sqrt{1 - \frac{2}{d_A d_B + 1}}.$$

Notice that this proves that a bound like (30) cannot hold in the case of ensembles, even if it does for single states, and that the dependence on the total dimension of the ensemble bound (35) is optimal up to constant factors, at least asymptotically, i.e., for large dimensions.

4. Quantum data hiding and ensemble quantumness of correlations

We concern ourselves with hiding classical bits using pairs of quantum states. An (ϵ, δ)-hiding pair of bipartite states (ρ_{AB}, σ_{AB}) has the properties

$$\frac{1}{2} \left\| \rho_{AB} - \sigma_{AB} \right\|_1 = 1 - \epsilon,$$

$$\frac{1}{2} \left\| \rho_{AB} - \sigma_{AB} \right\|_{\mathrm{LOCC}} = \delta,$$

where LOCC is meant under the partition $A\colon B$. Both the trace distance and the LOCC distance are related to the optimal probability of success in identifying correctly the state, assuming each state is prepared with equal probability, either by global measurements or LOCC measurements (Matthews *et al* 2009):

$$p_{\text{global}}^{\text{success}} = \frac{1}{2}\left(1 + \frac{1}{2}\,\|\rho_{AB} - \sigma_{AB}\|_1\right)$$
$$p_{\text{LOCC}}^{\text{success}} = \frac{1}{2}\left(1 + \frac{1}{2}\,\|\rho_{AB} - \sigma_{AB}\|_{\text{LOCC}}\right).$$

The $\|\cdot\|_{\text{LOCC}}$ norm is defined on bipartite Hermitian operators as (Matthews *et al* 2009)

$$\|X\|_{\text{LOCC}} = \max_{\{M_i\}} \sum_i \left|\text{Tr}\left(M_i X\right)\right|,$$

where the maximum is taken over all POVMs $\{M_i\}$ that can be realized by LOCC. In the following, we will need that

$$\begin{aligned}\tfrac{1}{2}\left\|\rho_{AB} - \sigma_{AB}\right\|_{\text{LOCC}} &= \max_{\mathcal{M}_{\text{LOCC}}} \|\mathcal{M}_{\text{LOCC}}[\rho_{AB} - \sigma_{AB}]\|_1 \\ &\geqslant \max_{\mathcal{M}_{1-\text{LOCC}}} \|\mathcal{M}_{1-\text{LOCC}}[\rho_{AB} - \sigma_{AB}]\|_1 \\ &\geqslant \max_{\Pi_A} \|\Pi_A[\rho_{AB} - \sigma_{AB}]\|_1 . \end{aligned} \tag{45}$$

Here, $\mathcal{M}_{\text{LOCC}}[\tau_{AB}] = \sum_i \text{Tr}\,(M_i X)|i\rangle\langle i|$ is any LOCC-measurement map (Matthews *et al* 2009, Piani 2009), which comprises LOCC measurements realized by one-way classical communication (1-LOCC), which in turn include measurement schemes where Alice performs a complete projective measurement and communicates the result to Bob. In the latter case, the fact that Bob performs an optimal measurement that depends on the outcome of Alice's projective measurement is automatically taken into account by the definition of the trace norm used in the last line of (45).

A 'good' quantum data hiding scheme seeks a pair of states such that both ϵ and δ are small positive numbers. The point is that we want to consider a pair of bipartite states that are (almost) perfectly distinguishable by global operations but almost indistinguishable by LOCC. We can define a single parameter for the quality of the hiding scheme in the following way.

Definition 4.1. The *hiding capability* of a pair (ρ_{AB}, σ_{AB}) of states is given by

$$\Delta_{\text{H}}[\rho_{AB}, \sigma_{AB}] := \frac{1}{2}\left(\left\|\rho_{AB} - \sigma_{AB}\right\|_1 - \left\|\rho_{AB} - \sigma_{AB}\right\|_{\text{LOCC}}\right) = 1 - \delta - \epsilon. \tag{46}$$

It is clear that $\delta, \epsilon \ll 1$ if and only if $\Delta_{\text{H}}[\rho_{AB}, \sigma_{AB}] \approx 1$.

It is known that there are good hiding schemes—i.e., with $\Delta_{\text{H}} \approx 1$—that do not make use of entanglement (Eggeling and Werner 2002). In the following we will see that, even if entanglement is not strictly needed, some form of quantumness of correlations (in particular, ensemble quantumness) must be present for a hiding scheme to be good. Before getting to such a result, we present evidence that even using one classical state in the pair of hiding states makes the task of quantum data hiding somewhat harder, although not impossible, as the existing constructions present in the literature show.

4.1. On hiding with classical states

Here, we prove a theorem on the limitations of hiding using classical states. For this, we make use of the following observation.

Lemma 4.2. *For any two normalized density operators ρ and σ on some Hilbert space $\mathcal{H}$,*

$$\frac{1}{\min\{R(\rho), R(\sigma)\}} F^2(\rho, \sigma) \leqslant \mathrm{Tr}\,(\rho\sigma) \leqslant F^2(\rho, \sigma), \tag{47}$$

where $F(\rho, \sigma) := \mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$ is the fidelity of the two states and $R(\rho)$ and $R(\sigma)$ are the ranks of ρ and σ, respectively.

Proof. We will use the fact that for any matrix X it holds

$$\|X\|_2 \leqslant \|X\|_1 \leqslant \sqrt{R(X)}\ \|X\|_2\,, \tag{48}$$

with $\|X\|_1 = \mathrm{Tr}\sqrt{X^\dagger X}$ the 1-norm (also known as trace norm) of X and $\|X\|_2 = \sqrt{\mathrm{Tr}\,(X^\dagger X)}$ the 2-norm (also known as Hilbert–Schmidt norm) of X. Then the lemma is proved by simply considering $X = \sqrt{\rho}\,\sqrt{\sigma}$, since $F(\rho, \sigma) = \|\sqrt{\rho}\,\sqrt{\sigma}\|_1$ and $\mathrm{Tr}\,(\rho\sigma) = \|\sqrt{\rho}\,\sqrt{\sigma}\|_2^2$, and by noting that $R(YZ) \leqslant \min\{R(Y), R(Z)\}$, while $R(\sqrt{\rho}) = R(\rho)$ (similarly for σ). □

We are now ready to prove the theorem.

Theorem 4.3. *If a classical-quantum (w.r.t. the partition $A\colon B$) bipartite state $\rho_{AB} = \sum_i p_i\,|i\rangle\langle i| \otimes \rho_i$ is ϵ-distinguishable from another bipartite state σ_{AB} under global operations, i.e.,*

$$\frac{1}{2}\,\|\rho_{AB} - \sigma_{AB}\|_1 \geqslant 1 - \epsilon, \tag{49}$$

and $R = \min\{R(\rho), R(\tilde{\sigma})\} \leqslant R(\rho)$ is the lesser of the ranks of ρ and $\tilde{\sigma}$, with $\tilde{\sigma} = \sum_i |i\rangle\langle i|_A\,\sigma\,|i\rangle\langle i|_A$, then ρ is at least $\sqrt{2R\epsilon}$-distinguishable from σ_{AB} under LOCC *w.r.t. $A\colon B$, i.e.,*

$$\frac{1}{2}\,\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \geqslant 1 - \sqrt{2R\epsilon}\,.$$

Proof. Besides lemma 4.2, we will make use of the well-known relation (Nielsen and Chuang 2000)

$$1 - F(\rho, \sigma) \leqslant D(\rho, \sigma) \leqslant \sqrt{1 - F(\rho, \sigma)^2}\,. \tag{50}$$

The claim can be proved through the following steps:

$$\begin{aligned}
\tfrac{1}{2}\,\|\rho - \sigma\|_{\mathrm{LOCC}} &\overset{(i)}{\geqslant} \tfrac{1}{2}\,\|\rho - \tilde{\sigma}\|_1 \\
&\overset{(ii)}{\geqslant} 1 - F(\rho, \tilde{\sigma}) \\
&\overset{(iii)}{\geqslant} 1 - \sqrt{R}\sqrt{\mathrm{Tr}\,(\rho\tilde{\sigma})} \\
&\overset{(iv)}{=} 1 - \sqrt{R}\sqrt{\mathrm{Tr}\,(\rho\sigma)} \\
&\overset{(v)}{\geqslant} 1 - \sqrt{R}\,F(\rho, \sigma) \\
&\overset{(vi)}{\geqslant} 1 - \sqrt{R}\sqrt{1 - D(\rho, \sigma)^2}
\end{aligned}$$

$$\overset{(vii)}{\geqslant} 1 - \sqrt{2R\epsilon} \tag{51}$$

The steps are justified as follows: (*i*) holds because a possible LOCC strategy is the one-way communication one with the first step consisting in measuring in the classical basis (for ρ) of A; (*ii*) and (*vi*) are due to equation (50); (*iii*) and (*v*) hold because of equation (47); (*iv*) holds because of the cyclic property of the trace; (*vii*) holds because of hypothesis equation (49). □

Our result points out how, with the use of a classical state, it is impossible to have a hiding scheme with $\epsilon = 0$. Indeed, our bound implies that perfect distinguishability ($\epsilon = 0$) by global operations implies perfect distinguishability ($\delta = 1$) also by LOCC. On the other hand, it is known that there exist good hiding schemes with perfect distinguishability; they necessarily make use of non-classical states. We will consider such a case in the example below.

We remark that our result just puts limits on a hiding scheme that uses at least one classical state, but hiding schemes that make use of at least a classical state do exist. For example, (Hayden *et al* 2004) provide an example of a hiding pair in $\mathbb{C}^d \otimes \mathbb{C}^d$, where one of the states is simply the maximally mixed state, $\mathbb{1}/d^2$, and the other state is the result of the action of an approximately randomizing random-unitary map $\mathcal{R}$ on part of a maximally entangled, i.e., the state $\mathcal{R} \otimes \mathsf{id}[\psi^+]$, with

$$\mathcal{R}[\rho] = \frac{1}{n}\sum_{i=1}^{n} U_i \rho U_i^\dagger,$$

satisfying

$$\left\| \rho - \frac{\mathbb{1}}{d} \right\|_\infty \leqslant \frac{\eta}{d}.$$

As proven in (Aubrun 2009), improving on (Hayden *et al* 2004), this can be achieved with independent Haar-random unitaries U_i and $n \geqslant Cd/\eta^2$, with C a constant. It is immediate to check that such a scheme achieves $\delta \leqslant \eta/2$ and $\epsilon \leqslant n/d^2 \approx C/(d\eta^2)$.

4.2. Ensemble quantumness bounds the quality of quantum data hiding

We have seen that the classicality of one of the hiding states does not prevent the hiding scheme from working, although it puts some 'quality' constraints on it. With the next theorem, we will see that the two states must nonetheless display a large ensemble quantumness of correlations.

Theorem 4.4. *The hiding capability of a pair of bipartite states is bounded above by the* $(\|\cdot\|_1, \{\Pi_A\})$*-quantumness of the ensemble consisting of the two states with equal weights:*

$$\Delta_{\mathrm{H}}[\rho_{AB}, \sigma_{AB}] \leqslant 2\, Q_{\|\mathbb{H}\|_1, \{\Pi_A\}}\left[\left\{\left(\frac{1}{2}, \rho_{AB}\right), \left(\frac{1}{2}, \sigma_{AB}\right)\right\}\right]. \tag{52}$$

Proof. By definition,

$$\Delta_{\mathrm{H}}[\rho_{AB}, \sigma_{AB}] = \tfrac{1}{2}\left(\left\| \rho_{AB} - \sigma_{AB} \right\|_1 - \left\| \rho_{AB} - \sigma_{AB} \right\|_{\mathrm{LOCC}} \right)$$

$$
\begin{aligned}
&= \tfrac{1}{2}\left(\left\| \rho_{AB} - \sigma_{AB} \right\|_1 - \max_{\mathcal{M}\in \mathrm{LOCC}} \left\| \mathcal{M}[\rho_{AB}] - \mathcal{M}[\sigma_{AB}] \right\|_1 \right) \\
&\leqslant \tfrac{1}{2}\left(\left\| \rho_{AB} - \sigma_{AB} \right\|_1 - \max_{\Pi_A} \left\| \Pi_A[\rho_{AB}] - \Pi_A[\sigma_{AB}] \right\|_1 \right) \\
&= \tfrac{1}{2} \min_{\Pi_A}\left(\left\| \rho_{AB} - \sigma_{AB} \right\|_1 - \left\| \Pi_A[\rho_{AB}] - \Pi_A[\sigma_{AB}] \right\|_1 \right) \\
&\leqslant \tfrac{1}{2} \min_{\Pi_A}\Big(\left\| \rho_{AB} - \Pi_A[\rho_{AB}] \right\|_1 \\
&\quad + \left\| \Pi_A[\rho_{AB}] - \Pi_A[\sigma_{AB}] \right\|_1 + \left\| \Pi_A[\sigma_{AB}] - \sigma_{AB} \right\|_1 \\
&\quad - \left\| \Pi_A[\rho_{AB}] - \Pi_A[\sigma_{AB}] \right\|_1 \Big) \\
&= 2\, Q_{\|\cdot\|_1,\{\Pi_A\}}\left[\left\{ \left(\tfrac{1}{2}, \rho_{AB}\right), \left(\tfrac{1}{2}, \sigma_{AB}\right) \right\} \right].
\end{aligned} \tag{53}
$$

The first inequality above follows from the fact that one-way LOCC measurements that start with a projective measurement are a subset of all LOCC measurements. The second inequality follows from repeated application of the triangle inequality for the trace norm. □

Notice that all the steps above could be adapted to the case of projective local measurements on both A and B, leading to $\Delta_{\mathrm{H}}[\rho_{AB}, \sigma_{AB}] \leqslant Q_{\|\cdot\|_1,\{\Pi_A\otimes\Pi_B\}}\left[\left\{ \left(\tfrac{1}{2}, \rho_{AB}\right), \left(\tfrac{1}{2}, \sigma_{AB}\right) \right\} \right]$.

Example: Werner hiding pairs. A well-known hiding pair constituted by the two Werner states,

$$
\sigma_{\pm} := \frac{\mathbb{1}\otimes\mathbb{1} \pm W}{d(d\pm 1)}, \tag{54}
$$

with W, we recall, the swap operator. The states σ_+ and σ_- are in fact normalized projectors onto the symmetric and antisymmetric subspaces, respectively. They form a hiding pair, with

$$
\frac{1}{2}\left\| \sigma_+ - \sigma_- \right\|_1 = 1,
$$

since they are orthogonal, and

$$
\frac{1}{2}\left\| \sigma_+ - \sigma_- \right\|_{\mathrm{LOCC}} = \frac{2}{d+1}. \tag{55}
$$

That equation (55) holds comes from the fact that even positive-under-partial-transposition (PPT) measurements, more general than LOCC, do not do better [see (Matthews *et al* 2009, Eggeling and Werner 2002, DiVincenzo *et al* 2002)], and there are LOCC measurements that achieve the bound [interestingly, the bound is achieved exactly via local orthogonal projections, as easily verified[11]]. Therefore, the hiding gap for this pair is exactly

[11] John Watrous, private communication; in turn, J. Watrous learnt of it from Māris Ozols.

$$\Delta_{\mathrm{H}}[\sigma_+, \sigma_-] = 1 - \frac{2}{d+1} = \frac{d-1}{d+1}. \tag{56}$$

We calculate the ensemble quantumness of correlations to be

$$\begin{aligned}
Q_{\|\cdot\|_1,\{\Pi_A\}}\left[\left\{\left(\tfrac{1}{2}, \sigma_+\right), \left(\tfrac{1}{2}, \sigma_-\right)\right\}\right] &= \min_{\Pi_A}\frac{1}{4}\left[\left(\|\sigma_+ - \Pi_A[\sigma_+]\|_1 + \|\sigma_+ - \Pi_A[\sigma_+]\|_1\right)\right.\\
&= \min_{\Pi_A}\frac{1}{4}\left(\left\|\tfrac{\mathbb{1}\otimes\mathbb{1}+W}{d(d+1)} - \Pi_A\left[\tfrac{\mathbb{1}\otimes\mathbb{1}+W}{d(d+1)}\right]\right\|_1 + \left\|\tfrac{\mathbb{1}\otimes\mathbb{1}-W}{d(d-1)} - \Pi_A\left[\tfrac{\mathbb{1}\otimes\mathbb{1}-W}{d(d-1)}\right]\right\|_1\right)\\
&= \min_{\Pi_A}\frac{1}{4}\left(\tfrac{1}{d(d+1)}\left\|W - \Pi_A[W]\right\|_1 + \tfrac{1}{d(d-1)}\left\|W - \Pi_A[W]\right\|_1\right)\\
&= \frac{1}{2\left(d^2-1\right)}\left\|W - \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i|\right\|_1\\
&= \frac{1}{2\left(d^2-1\right)}\left\|\mathbb{1} - \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i|\right\|_1\\
&= \frac{1}{2\left(d^2-1\right)}\left(d^2-d\right)\\
&= \frac{d}{2(d+1)}
\end{aligned}$$

Thus, our bound (52) reads $\Delta_H \leqslant 2\frac{d}{2(d+1)} = \frac{d}{d+1}$ and is quite tight in this case, almost matching the actual quality of the hiding scheme (56).

5. Conclusions

Both the quantumness of ensembles and the quantumness of correlations have been investigated quite intensively in the recent past. These two notions of quantumness are deeply connected. On one hand, any single-system ensemble of states that exhibits quantumness can be used to construct a distributed state that exhibits some quantumness of correlations (Piani *et al* 2008, Luo *et al* 2010, 2011, Yao *et al* 2013). On the other, the study of the quantumness of correlations has often relied on the study of the quantumness of ensembles, intended, e.g., in terms of the impossibility of simultaneously cloning/broadcasting non-commuting single-system states (Barnum *et al* 1995, Piani *et al* 2008, Luo and Sun 2010).

In this paper, in a sense, we combined the notions of quantumness related to dealing with multiple states and the one related to non-classical correlations. We did so by introducing and studying the notion of ensemble quantumness of correlations. Such a notion, we argued, actually fits in a larger unified framework for the study of quantum properties, which encompasses the notion of quantumness of single-system states, as well as of quantumness of correlations of a single bi- or multi-partite state. In our case we chose to depict such a unified framework as based on the quantumness revealed by disturbance under (projective) measurements.

We argued that the ensemble quantumness of correlations plays an important role in one of the basic tasks in quantum information processing: quantum data hiding. Indeed, we noticed

how quantum data hiding does not require entanglement, in the sense that there are pairs of hiding states—states used to encode a bit, so that such a bit is recoverable by global quantum operations but not by local operations assisted by classical communication—that are not entangled, and still ensure a good hiding scheme. In this paper, we proved that even though quantum data hiding does not require the strong non-classicality linked to entanglement, some non-classicality of correlations must necessarily be present. More precisely, based on existing schemes for quantum data hiding, we argued that the key property is not the quantumness of correlations of the individual states in the hiding pair, as there are hiding schemes that use at least one strictly classical bipartite state. The strictly necessary property seems to rather be the ensemble quantumness of correlation. Indeed, we prove that, if the latter is small, then the quality of the hiding scheme is also necessarily small. This kind of observation is very similar in spirit to the one that relates the quantumness of correlations to entanglement distribution. For the latter task, Cubitt *et al* (Cubitt *et al* 2003) had proven that two parties can increase their entanglement by exchanging a quantum carrier that is unentangled with both parties. Nonetheless, it was proven in (Streltsov, Kampermann and Brub 2012, Chuan *et al* 2012) that the increase is bounded by the amount of general non-classical correlations between the particle and the two parties.

After introducing the notion of ensemble quantumness of correlations, we have focused on providing some general bounds on it. This has naturally led us to study in detail the disturbance, as measured by the trace-distance, induced by local projective measurements on a pure bipartite state. Several researchers interested in the quantumness of correlations had already considered the disturbance induced by local projective measurement on quantum states (Luo 2008b, Luo and Fu 2013, Nakano *et al* 2013, Paula *et al* 2013). Nonetheless, as far as we know, we are the first to provide an analytical formula for such a disturbance, as measured by trace distance, for all pure states. We actually proved that said disturbance is an entanglement monotone on pure states, in the sense that it is monotonically non-increasing *on average* under LOCC transformations. This qualifies it to be a good entanglement measure for pure states, which we call *entanglement of disturbance*, and enables a meaningful extension to mixed states by means of a standard convex roof construction. Returning to ensemble quantumness, we studied several examples, going from the quantumness of ensembles of single-qubit states, to the Haar ensembles for both single systems and bipartite systems. The latter examples perfectly illustrate how the ensemble quantumness of correlations is different from the quantumness of correlations of single states.

The main open problem regards the existence of hiding schemes where both states are individually strictly classical, although obviously (given our results) the pair must exhibit ensemble quantumness. Indeed, thanks to existing examples, we know that at least one state in the hiding pair can be strictly classical, but we have proven that its presence poses strong constraints on the hiding scheme. So the question is: Is there a no-go theorem for hiding by means of strictly classical states, even if they are quantum with respect to one another?

Acknowledgements

We acknowledge discussions with G Adesso, A Brodutch, A Streltsov, J Watrous and A Winter. We thank D. Reeb for correspondence related to the connection between the results of this paper and (Jivulescu *et al* 2014) (see the note added below). V N started working on this

project during his studies at the Institute for Quantum Computing at the University of Waterloo, and is grateful to N. Lütkenhaus for support and encouragement. J C is grateful to N Lütkenhaus and M P for hosting him at the Institute for Quantum Computing, where this work was initiated. M P acknowledges support by NSERC, CIFAR and Ontario Centres of Excellence. J C acknowledges support from Spanish MINECO (project FIS2008-01236) with FEDER funds.

Note added in proof. After the submission of this manuscript, a work by Jivulescu et al. containing related results appeared (Jivulescu *et al* 2014). Jivulescu *et al* focus on the problem of whether all bipartite quantum states having a prescribed spectrum satisfy the reduction criterion for separability (Cerf *et al* 1999, Horodecki and Horodecki 1999). In order to attack this problem, Jivulescu *et al* evaluate the spectrum of the operator resulting from the action of the reduction map (Cerf *et al* 1999, Horodecki and Horodecki 1999) on one party of an arbitrary bipartite pure state, providing an alternative proof of the main formula of theorem 3.3. The connection between the present paper and the results of (Jivulescu *et al* 2014) is further discussed in the most recent version of (Jivulescu *et al* 2014).

References

Adesso G, D'Ambrosio V, Nagali E, Piani M and Sciarrino F 2014 *Phys. Rev. Lett.* **112** 140501
Aubrun G 2009 *Commun. Math. Phys.* **288** 1103–16
Barnum H, Caves C M, Fuchs C A, Jozsa R and Schumacher B 1996 *Phys. Rev. Lett.* **76** 2818–21
Bengtsson I and Życzkowski K 2006 *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge: Cambridge University Press)
Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
Bhatia R 1997 *Matrix Analysis* vol 169 (Berlin: Springer)
Bravyi S 2003 *Phys. Rev.* A **67** 012313
Brodutch A 2013 *Phys. Rev.* A **88** 022307
Cerf N, Adami C and Gingrich R 1999 *Phys. Rev.* A **60** 898
Chuan T, Maillard J, Modi K, Paterek T, Paternostro M and Piani M 2012 *Phys. Rev. Lett.* **109** 070501
Ciccarello F, Tufarelli T and Giovannetti V 2014 *New J. Phys.* **16** 013038
Coles P J 2012 *Phys. Rev.* A **86** 062334
Cover T M and Thomas J A 2012 *Elements of Information Theory* (Hoboken, NJ: Wiley)
Cubitt T S, Verstraete F, Dür W and Cirac J 2003 *Phys. Rev. Lett.* **91** 037902
D'Ariano G M 2003 *Fortschr. Phys.* **51** 318–30
Debarba T, Maciel T O and Vianna R O 2012 *Phys. Rev.* A **86** 024302
DiVincenzo D P, Leung D W and Terhal B M 2002 *IEEE Trans. Inf. Theory* **48** 580–98
Eggeling T and Werner R F 2002 *Phys. Rev. Lett.* **89** 097905
Ferraro A, Aolita L, Cavalcanti D, Cucchietti F and Acin A 2010 *Phys. Rev.* A **81** 052318
Fuchs C A and Sasaki M 2003 *Quantum. Inf. Comput.* **3** 377–404
Gharibian S, Piani M, Adesso G, Calsamiglia J and Horodecki P 2011 *Int. J. Quantum Inf.* **9** 1701–13
Gharibian S 2012 *Phys. Rev.* A **86** 042106
Groisman B, Kenigsberg D and Mor T 2007 arXiv:quant-ph/0703103
Hayden P, Leung D, Shor P W and Winter A 2004 *Commun. Math. Phys.* **250** 371–91
Henderson L and Vedral V 2001 *J. Phys. A: Math. Gen.* **34** 6899
Hiai F, Ohya M and Tsukada M 1981 *Pac. J. Math.* **96** 99–109

Horodecki M, Horodecki P, Horodecki R, Oppenheim J, Sen(De) A, Sen U and Synak-Radtke B 2005 *Phys. Rev.* A **71** 062307
Horodecki M, Horodecki P, Horodecki R and Piani M 2006 *Int. J. Quantum Inf.* **4** 105–18
Horodecki M and Horodecki P 1999 *Phys. Rev.* A **59** 4206
Horodecki M, Horodecki R, De A S and Sen U 2005 *Found. Phys.* **35** 2041–9
Horodecki M 2001 *Quant. Inf. Comput.* **1** 3
Horodecki M 2005 *Open Syst. Inf. Dyn.* **12** 231–7
Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Mod. Phys.* **81** 865–942
Jivulescu M A, Lupa N, Nechita I and Reeb D 2014 arXiv:1406.1277
Jozsa R 1994 *J. Mod. Opt* **41** 2315
Kretschmann D, Schlingemann D and Werner R F 2008 *IEEE Trans. Inf. Theory* **54** 1708–17
Luo S and Fu S 2013 *Int. J. Mod. Phys.* B **27** 1345026
Luo S, Li N and Fu S 2011 *Theor. Math. Phys.* **169** 1724–39
Luo S, Li N and Sun W 2010 *Quant. Inf. Process* **9** 711–26
Luo S and Sun W 2010 *Phys. Rev.* A **82** 012338
Luo S 2008 *Phys. Rev.* A **77** 042303
Luo S 2008 *Phys. Rev.* A **77** 022301
Matthews W, Wehner S and Winter A 2009 *Commun. Math. Phys.* **291** 813–43
Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 *Rev. Mod. Phys.* **84** 1655–707
Modi K, Paterek T, Son W, Vedral V and Williamson M 2010 *Phys. Rev. Lett.* **104** 080501
Nakano T, Piani M and Adesso G 2013 *Phys. Rev.* A **88** 012117
Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
Nielsen M A 1999 *Phys. Rev. Lett.* **83** 436
Ollivier H and Zurek W H 2001 *Phys. Rev. Lett.* **88** 017901
Paula F M, de Oliveira T R and Sarandy M S 2013 *Phys. Rev.* A **87** 064101
Piani M and Adesso G 2012 *Phys. Rev.* A **85** 040301
Piani M, Gharibian S, Adesso G, Calsamiglia J, Horodecki P and Winter A 2011 *Phys. Rev. Lett.* **106** 220403
Piani M, Horodecki P and Horodecki R 2008 *Phys. Rev. Lett.* **100** 090502
Piani M 2009 *Phys. Rev. Lett.* **103** 160504
Rana S and Parashar P 2013 *Phys. Rev.* A **87** 016301
Schumacher B and Westmoreland M D 2002 *Quant. Inf. Proc* **1** 5
Streltsov A, Adesso G, Piani M and Bruß D 2012 *Phys. Rev. Lett.* **109** 050503
Streltsov A, Kampermann H and Bruß D 2011 *Phys. Rev. Lett.* **106** 160401
Streltsov A, Kampermann H and Bruß D 2012 *Phys. Rev. Lett.* **108** 250501
Terhal B M, DiVincenzo D P and Leung D W 2001 *Phys. Rev. Lett.* **86** 5807–10
Uhlmann A 1976 *Rep. Math. Phys.* **9** 273–9
Vedral V and Plenio M B 1998 *Phys. Rev.* A **57** 1619
Vedral V, Plenio M, Rippin M and Knight P 1997 *Phys. Rev. Lett.* **78** 2275
Vidal G and Werner R 2001 *Phys. Rev.* A **65** 032314
Vidal G 2000 *J. Mod. Opt* **47** 355–76
Wootters W K 1998 *Phys. Rev. Lett.* **80** 2245
Yao Y, Huang J Z, Zou X B and Han Z F 2014 *Quantum Inf. Process* **13** 1583–94