Two-qubit correlations revisited: average mutual information, relevant (and useful) observables and an application to remote state preparation

Two-qubit correlations revisited: average mutual information, relevant (and useful) observables and an application to remote state preparation

Paolo Giorda[1] **and Michele Allegra**[2]

[1] Consorzio Nazionale Interuniversitario per le Scienze Fisiche della Materia (CNISM), I-20133 Milan, Italy
[2] Scuola Internazionale Superiore di Studi Avanzati (SISSA), I-34136 Trieste, Italy

E-mail: magpaolo16@gmail.com and mallegra@sissa.it

Abstract

Understanding how correlations can be used for quantum communication protocols is a central goal of quantum information science. While many authors have linked the global measures of correlations such as entanglement or discord to the performance of specific protocols, in general the latter may require only correlations between specific observables. In this work, we first introduce a general measure of correlations for two-qubit states, based on the classical mutual information between local observables. Our measure depends on the state's purity and the symmetry in the correlation distribution, according to which we provide a classification of maximally mixed marginal states (MMMS). We discuss the complementarity relation between correlations and coherence. By focusing on a simple yet paradigmatic example, i.e. the remote state preparation protocol, we introduce a method to systematically define the proper protocol-tailored measures of the correlations. The method is based on the identification of those correlations that are relevant (useful) for the protocol. On the one hand, the approach allows the role of the symmetry of the correlation distribution to be discussed in determining the efficiency of the protocol, both for MMMS and general two-qubit quantum states, and on the other hand, it allows an optimized protocol for non-MMMS to be devised, which is more efficient with respect to the standard one. Overall, our findings clarify how the key resources in simple communication protocols are the purity of the state used and the symmetry of the correlation distribution.

(Some figures may appear in colour only in the online journal)

1. Introduction

The study of correlations in quantum systems has a long, deep and complex history indeed. In particular, enormous effort has been devoted to characterizing the 'quantumness' of correlations, or devising measures of correlations aimed at capturing the 'quantum content' present in a generic quantum state, such as quantum entanglement [1, 2] and quantum discord [8, 9]. Three premises underlie the derivation of such measures [10]: (i) in a quantum state there can be 'classical' and 'quantum' correlations that coexist; (ii) it is possible to algorithmically identify and separate the quantum versus the classical part of the correlations; and (iii) both parts can be quantified by means of a single number. In agreement with these assumptions, measures of the correlations have been used to establish a classification of quantum states based on a clear-cut distinction between the quantum versus the classical states (e.g. separable versus entangled states and discordant versus zero-discord states). Furthermore, the correlation measures have been directly connected to the performance of specific quantum protocols. An additional premise is implicit in this effort: (iv) quantum correlations, interpreted as properties of a given quantum state as a whole, underlie the efficiency of quantum protocols, and in particular they are responsible for the 'quantum advantage' over classical protocols [14]. For instance, entanglement has been cited as an essential resource for quantum computation [3], quantum teleportation [4], quantum dense coding [5], quantum cryptography [6] and quantum metrology [7]. Quantum discord has been indicated as a resource in mixed-state quantum computation [11], quantum cryptography [12] and quantum communication [13, 24].

However, the strategy that follows the above premises (i)–(iv) is sometimes unable to unequivocally provide a connection between the performance of the protocol, as measured by a suitable figure-of-merit, and a given measure of quantum correlations. Therefore, the search for other perspectives is indeed possible and also in order. In particular, we propose to 'forget' about the quantum versus classical distinction, and rather focus on *(classical) correlations between sets of local observables*. Our proposal is based on an idea that has been highlighted within the framework of the consistent (decoherent) history approach to quantum mechanics [17, 18] (and sometimes also within the standard interpretation [16]). The state ρ of a system, rather than being a 'property' of the system, can be intended as a 'pre-probability', i.e. a mathematical device that is useful for calculating the probabilities of the measurement outcomes pertaining to (possibly incompatible) experiments. In a bipartite setting for example, where A and B share a given state ρ and want to implement a communication task, the probability distributions pertaining to all pairs of local observables define the set of 'available correlations' stored in the state. When a specific protocol is enacted, one is led to identify the subset of pairs of local observables that are relevant for its realization, and therefore the corresponding subset of *relevant correlations*. In this sense, a bipartite state can be imagined as a multiple-input/ multiple-output system [19], i.e. a communication system that can exploit several parallel channels linking the transmitter and the receiver; the 'relevant channels' are those identified by the pairs of local observables that are relevant for a given protocol. From this perspective, on the one hand quantum states can be characterized as a whole by the average amount of (classical) correlations between all pairs of local observables. As we will show, this value is determined by the purity of the state and the symmetry of the correlation distribution, i.e. the

symmetry group that connects pairs of local observables that have equal correlations. On the other hand, the efficiency of specific quantum protocols can be connected with specific sets of local observables and their mutual correlations. In this way, one is able to find protocol-specific measures of correlations and, as we demonstrate with a specific example, modify existing protocols in order to enhance their efficiency.

In order to thoroughly examine the proposed strategy, here we focus on the simplest case of quantum communication bipartite channels provided by two-qubit quantum states ρ_{AB}, where the tensor product structure $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ naturally provides the sets of local observables to study. In particular, we start our analysis by focusing on states with maximally mixed marginals (MMMS). The latter are particularly simple to study and have been widely used in the literature as prototypical instances of bipartite communication channels [1, 8, 15]. We will consider pairs of local von Neumann observables and their correlations, as measured by the classical mutual information $\mathcal{I}$ of measurement outcomes. On the basis of $\mathcal{I}$, in the first place we define a measure of the 'available correlations' by taking a suitable average $\langle \mathcal{I} \rangle_\Omega$ over the manifold Ω of local observables (which, in the case of two qubits, are given by the product of two spheres $\Omega = S_2 \times S_2$). However, two states, with possibly different purities, can well have the same amount of average correlations $\langle \mathcal{I} \rangle_\Omega$ (just as two states can have the same amount of entanglement or discord) and yet be strikingly different from the point of view of how the correlations are distributed among the various observables. From this perspective, bipartite quantum states can be classified on the basis of both the purity-dependent quantity given by the *average correlations*, and by the purity-independent feature given by the *symmetry* of the correlation distribution. Furthermore, it is possible to introduce a relation between the correlations of the pairs of observables and the coherence of the product bases they define. In this respect, we show that fixed purity correlations and coherence can in general be identified as complementary resources.

To assess the role of correlations in a quantum protocol, $\langle \mathcal{I} \rangle_\Omega$ may not be the most significant quantity. When analyzing a given communication task, one should pick out the set of observables that is relevant for its realization. This is possible, for example, when there exists a figure-of-merit $\mathcal{F}$ for the protocol that explicitly depends on a specific subset of observables, i.e. a set $\Omega_{RO} \subseteq \Omega$ of *relevant observables* (RO). If this is the case, then one can immediately derive a protocol-related measure of correlations by taking the average $\langle \mathcal{I} \rangle_{\Omega_{RO}}$ on this subset only. From the conceptual point of view, our perspective is radically different from others: instead of considering an overall property of the state, such as the entanglement, the discord or the average mutual information $\langle \mathcal{I} \rangle_\Omega$, we establish a direct connection between the (average) performance of the protocol and the correlations pertaining to the relevant observables. In the following, we will fully develop the first example of this method by applying it to the (two-qubit) remote state preparation (RSP) protocol [20–23]. The latter has been widely studied in the literature and there have been many attempts to link its performance to specific kinds of quantum correlations, such as quantum discord [24] or entanglement [26]. However, it has been shown that on the one hand discord is neither sufficient nor necessary for the efficiency of the protocol [25], and on the other hand that states with a lower content of entanglement or discord can provide better efficiency than states with higher values of both quantities [31]. In our case, we will analyze the protocol for both MMMS and general non-MMMS states. We will define a functional $\mathcal{F}$ for RSP that allows us to identify the set of relevant observables. While for states with maximally mixed marginals (MMMS) all relevant observables are useful, i.e. they can always be used to enhance $\mathcal{F}$, for general non-MMMS only a subset of the relevant observables has this property. One can therefore define the set of *useful observables* $\Omega_U \subseteq \Omega_{RO}$ and correspondingly introduce an alternative way of enacting RSP based on useful observables only, such that the overall efficiency of the protocol is improved. In both cases

(MMMS and non-MMMS), we measure the advantage of using the correlations versus not using them by means of a gain function $\mathcal{G}$, which explicitly depends on the correlation of the useful observables. The average gain will provide the link to the desired measure of correlations pertaining to the protocol.

Throughout the whole discussion, we analyze how the purity versus the symmetry of the correlations affect the protocol. In general, the purity and the symmetry of the correlations can be thought of as two fundamental resources: the purity fixes the amount of available correlations, and the symmetry determines how the correlations are distributed between the relevant observables. As for symmetry alone, we finally show how it can be recognized as the key resource that allows the communication channel between parties A and B to be established *before* the state one wants to transfer is known.

The paper is organized as follows. In section 2.1 we briefly define the formalism and the conventions used. In section 2.2 we introduce our measure of correlations and study the general properties of $\langle \mathcal{I} \rangle_\Omega$, as well as their relation to the state's symmetry for MMMS. In section 3, we discuss in detail the RSP protocol for MMMS and non-MMMS. In section 4 we finally discuss the relation between symmetry and freedom in implementing the different steps of RSP. In section 5 we derive our conclusions.

2. Classification of quantum states based on correlations between observables

We start by discussing how two-qubit quantum states can be characterized on the basis of the pairwise correlations between local observables, $\mathcal{I}(\hat{n}, \hat{m})$. For simplicity, we focus on a subset of states: those with maximally mixed marginals (MMMS). We show that MMMS can be characterized by the average $\langle \mathcal{I} \rangle_\Omega$ as well as the symmetry of $\mathcal{I}(\hat{n}, \hat{m})$, as defined below. Finally, we discuss how the correlation content described by $\mathcal{I}(\hat{n}, \hat{m})$ is complementary to the coherence of the product basis defined by $\hat{n}, \hat{m}$ in the given state.

2.1. Notation

By using the Bloch–Fano representation, one can show that an arbitrary two-qubit state is equivalent, up to the local unitary operations $U_A \otimes U_B$, to the state:

$$\rho_{AB} = \frac{1}{4}(\mathbb{I}^A \otimes \mathbb{I}^B + \vec{a} \cdot \vec{\sigma}^A \otimes \mathbb{I}^B + \mathbb{I}^A \otimes \vec{b} \cdot \vec{\sigma}^B + \kappa \sum_i c_i \sigma_i^A \otimes \sigma_i^B) \tag{1}$$

where $\vec{a} = |a|\hat{a}$ and $\vec{b} = |b|\hat{b}$ are the Bloch vectors of the marginal states, $E = \kappa \; \mathrm{diag}(c_1, c_2, c_3)$ is the correlation matrix in its diagonal form, and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of the Pauli matrices. Therefore, the state is identified by three vectors: the vectors $\vec{a}, \vec{b}$ describing the reduced density matrices ρ_A, ρ_B and the correlation vector $\vec{c} = \kappa \hat{c} = \kappa(c_1, c_2, c_3)$, $\kappa = |\vec{c}|$. In the following, we will focus on maximally mixed marginal states (MMMS), defined as the states for which $\vec{a} = \vec{b} = \vec{0}$, and which hence have maximally mixed reduced states on $\rho_A = \rho_B = \frac{1}{2}\mathbb{I}$:

$$\rho_{AB}^{(\mathrm{MMMS})} = \frac{1}{4}(\mathbb{I}^A \otimes \mathbb{I}^B + \kappa \sum_i c_i \sigma_i^A \otimes \sigma_i^B).$$

The MMMS are completely characterized by the correlation vector $\vec{c}$. The condition for ρ_{AB} to be a good quantum state is the positivity condition $\rho_{AB} > 0$. The latter implies that

$\vec{c} \in \mathcal{T}$, i.e. $\vec{c}$ is a vector in $\mathbb{R}^3$ contained in the tetrahedron $\mathcal{T}$ with the vertices $(-1, -1, -1)$, $(-1, 1, 1)$, $(1, -1, 1)$, $(1, 1, -1)$ [15]. The value of the parameter κ defines the purity of the state, which reads $(1 + \kappa^2)/4$.

In the following, we will focus on pairs of von Neumann observables. The latter are operators that can be represented as $O_{A(B)} = \sum_k o_k \Pi_k^{A(B)}$, with $\left\{ \Pi_k^{A(B)} \right\}$ being a complete orthogonal set of projectors on the Hilbert space $\mathcal{H}_{A(B)}$. Since we are dealing with qubits, any projector can be written in terms of the Pauli matrices as

$$\Pi_{\pm}^{A(B)}(\hat{m}) = \left(\mathbb{I} \pm \hat{m} \cdot \vec{\sigma}^{A(B)} \right) / 2$$

where $\hat{m}$ is a unit vector belonging to a single qubit Bloch sphere and $\Pi_{\pm} = |\pm\hat{m}\rangle\langle\pm\hat{m}|$. We are interested in the correlations between pairs of observables $\hat{n} \cdot \vec{\sigma}^A$, $\hat{m} \cdot \vec{\sigma}^B$ (pertaining to the subsystems A and B respectively), whose projectors are given by $\Pi_{\pm}^A(\hat{n})$, $\Pi_{\pm}^B(\hat{m})$. The measure of correlations we use is the standard classical mutual information $\mathcal{I}(\hat{n}, \hat{m}) \equiv \mathcal{I}(\Pi_{\pm}^A(\hat{n}), \Pi_{\pm}^B(\hat{m}))$, which can be written in terms of the joint probability distribution

$$p_{ij} = Tr \left[\rho_{AB} \Pi_i^A(\hat{n}) \otimes \Pi_j^B(\hat{m}) \right], \qquad i, j = \pm$$

and of the marginals $p_i = Tr \left[\rho_A \Pi_i^A(\hat{n}) \right]$, $p_j = Tr \left[\rho_B \Pi_j^B(\hat{m}) \right]$ as

$$\mathcal{I}(\hat{n}, \hat{m}) = - \sum_i p_i \log_2 p_i - \sum_j p_j \log_2 p_j + \sum_{ij} p_{ij} \log_2 p_{ij}.$$

For MMMS, the probability for the joint measurements defined by $(\hat{n}, \hat{m})$ can be expressed in terms of the correlation matrix as $p_{ij} = \left(1 + ij \, \hat{m} E \hat{n}^T \right) / 4$, $i, j = \pm$, whereas the probabilities for the single local measurements yield $p_{\pm}^{A(B)} = 1/2$.

2.2. Symmetry and distribution of correlations

With the above notations, the mutual information between two local observables $\hat{n}, \hat{m}$ in MMMS can be simply expressed as

$$\mathcal{I}(\hat{n}, \hat{m}) = \frac{1}{2} \Big((1 - x) \log_2 (1 - x) + (1 + x) \log_2 (1 + x) \Big)$$

where $x = \hat{n} E \hat{m}^T = \kappa \, \hat{n} \text{diag}(c_1, c_2, c_3) \hat{m}^T$. From this formula, it immediately follows that the correlations between any two observables are a monotonic function of κ, i.e. of the purity, and that for any fixed κ the distribution of correlations between different pairs of observables depends on the direction of the correlation vector $\hat{c}$. States, identified by their $\hat{c}$, can be classified on the basis of the distribution of the correlations they yield.

A first classification of the states and the corresponding directions $\hat{c}$ can be done on the basis of the local symmetries of the correlations, which follow from the local symmetries for the state. A state ρ has a local unitary symmetry if there are local unitaries $U_A \otimes U_B$ such that $U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger = \rho$. The local unitary symmetries of the state form a group $\mathcal{LU}$ called a local unitary stabilizer [29], which is a discrete or continuous subgroup of $SU(2) \otimes SU(2)$. Local unitaries $U \in SU(2)$ acting on the Hilbert space can be mapped to rotations $O \in SO(3)$ acting on the Bloch sphere: indeed, there exists a (unique) rotation $O \in SO(3)$ such that $U\hat{n} \cdot \vec{\sigma} U^\dagger = (O\hat{n}) \cdot \vec{\sigma}$. By virtue of this $SU(2) \to SO(3)$ mapping, local unitary symmetries can be expressed in terms of *special orthogonal* transformations that leave the correlation matrix invariant:

$$O_A E O_B^T = E \tag{2}$$

where $O_A, O_B \in SO(3)$. The fact that a state defined by $\vec{c}$ has a symmetry group $\mathcal{LU}$ can be viewed in two equivalent ways. On the one hand, for all $\hat{n}, \hat{m}$, $\mathcal{I}(\hat{n}, \hat{m})(\vec{c})$ is also left invariant by the action of $\mathcal{LU}$ on ρ. On the other hand, local symmetries of the state imply a symmetry in the distribution of correlations: given a pair of local observables $(\hat{n}, \hat{m})$, all the pairs $(\hat{n}', \hat{m}') = (\hat{n}O_A, \hat{m}O_B)$ have the same value of mutual information.

Given a direction $\hat{c}$ with a specific $\mathcal{LU}$, we are interested in identifying the equivalence class of directions that yield isomorphic distributions of correlations for fixed κ (purity). Formally, for any fixed κ and any given $\hat{c}$, we want to identify the directions $\hat{d}$, such that for any pair of observables $(\hat{n}, \hat{m})$ there exists a pair of observables $(\hat{n}', \hat{m}')$ such that $\mathcal{I}(\hat{n}, \hat{m})(\kappa\hat{c}) = \mathcal{I}(\hat{n}', \hat{m}')(\kappa\hat{d})$, i.e. there exists a bijective map $\phi : (\hat{n}, \hat{m}) \to (\hat{n}', \hat{m}')$, realizing a change of local coordinates on the Bloch spheres, such that $\mathcal{I}(\hat{n}, \hat{m})(\kappa\hat{c}) = \mathcal{I}(\phi(\hat{n}, \hat{m}))(\kappa\hat{d})$. Thus, given a direction $\hat{c} = (c_1, c_2, c_3)$, we want to identify the following equivalence class $\mathcal{LU}_{\hat{c}}^{\text{eq}}$ of directions $\hat{d} = (d_1, d_2, d_3)$:

$$\mathcal{LU}_{\hat{c}}^{\text{eq}} \equiv \left\{ \hat{d} \; : \; \exists \kappa \mid \forall (\hat{m}, \hat{n}), \; \exists (\hat{m}', \hat{n}') \mid \mathcal{I}(\hat{n}, \hat{m})(\kappa\hat{d}) = \mathcal{I}(\hat{n}', \hat{m}')(\kappa\hat{c}) \right\}.$$

In order to identify the components of a given class, one has to notice that a local change of coordinates on the Bloch spheres $S_2 \times S_2$ corresponds to a pair of *orthogonal* transformations $O_A, O_B \in O(3)$ acting on $\hat{n}, \hat{m}$ as $\hat{n}' = \hat{n}O_A$ and $\hat{m}' = \hat{m}O_B$. In order to have $\mathcal{I}(\hat{n}, \hat{m})(\kappa\hat{d}) = \mathcal{I}(\hat{n}', \hat{m}')(\kappa\hat{c})$ we must have

$$|\hat{n}' \text{diag}(d_1, d_2, d_3)\hat{m}'^T| = |\hat{n}\text{diag}(c_1, c_2, c_3)\hat{m}^T|$$

which can be rewritten as

$$O_A \text{diag}(c_1, c_2, c_3)O_B^T = \pm \text{diag}(d_1, d_2, d_3). \tag{3}$$

Equation (3) severely constrains the form of $\hat{d}$. Indeed, since the matrices $\text{diag}(c_1, c_2, c_3)$ and $\text{diag}(d_1, d_2, d_3)$ are related by two orthogonal rotations as above, they must have the same singular values. This implies that $|d_1|, |d_2|, |d_3|$ are related to $|c_1|, |c_2|, |c_3|$ by a permutation. As a result, we must have

$$\mathcal{LU}_{\hat{c}}^{\text{eq}} = \left\{ \hat{d} = (s_1 c_{\sigma(1)}, s_2 c_{\sigma(2)}, s_3 c_{\sigma(3)}) \mid s_i \in \{\pm\}, \vec{\sigma} \in P(1, 2, 3) \right\} \tag{4}$$

where $P(1, 2, 3)$ is the set of permutations of three indices. $\mathcal{LU}_{\hat{c}}^{\text{eq}}$ can be seen as the orbit of a discrete subgroup of $O(3)$ that acts on the given $\hat{c}$ and is isomorphic to $G \sim S_3 \otimes E_8$, where S_3 is the symmetric group of order 3, corresponding to the permutations of three indices, and E_8 is the elementary Abelian group of order 8 that realizes the changes of signs s_i in equation (4). As discussed in the appendix A, the transformations in G can be realized by a combination of local unitary rotations and a non-unitary local spin-flip that implements the transformation $\hat{c} \to -\hat{c}$; furthermore, the total number of *different* equivalent directions $|\mathcal{LU}_{\hat{c}}^{\text{eq}}| \leqslant 48$ depends on the specific $\mathcal{LU}$ and $\hat{c}$.

In [29] a complete classification of the continuous $\mathcal{LU}$ for *N*-qubit states was given; starting from such a classification we identify the following classes of MMMS:

1. $\rho_{3\text{iso}}$ states ('isotropic states'), which belong to the class $\mathcal{LU}_{\hat{c}}^{\text{eq}}$ with $\hat{c} = (1, 1, 1)/\sqrt{3}$. These states are invariant with respect to local unitaries of the kind $U \otimes U$, $U \in SU(2)$ and we define the class as $\mathcal{LU}_{3\text{iso}}$ with $|\mathcal{LU}_{3\text{iso}}| = 8$. Bell and Werner states belong to this class of isotropic states.

2. $\rho_{2\text{iso}}^{\epsilon}$ states, which are equivalent to $\hat{c} = (\epsilon, \epsilon, \sqrt{1 - 2\epsilon^2})$, $0 < \epsilon^2 \leqslant 1/2$; these states are invariant with respect to the subset of the local unitaries of the kind $U \otimes U$, $U = \exp -i\theta\sigma_z^{A(B)}$; we define the class as $\mathcal{LU}_{2\text{iso}}^{\epsilon}$, which has $|\mathcal{LU}_{2\text{iso}}^{\epsilon}| = 24$ elements if $\epsilon \neq 0$ and $|\mathcal{LU}_{2\text{iso}}^{\epsilon}| = 12$ elements if $\epsilon^2 = 1/2$.

3. $\rho_{2\text{iso}}^{0}$ states, which are equivalent to $\hat{c} = (0, 0, 1)$; these states are invariant with respect to the subset of local unitaries of the kind $U_A \otimes U_B$, $U_A = \exp -i\theta\sigma_z^A$, $U_B = \exp -i\eta\sigma_z^B$, where in general $\theta \neq \eta$. We define the class as $\mathcal{LU}_{2\text{iso}}^{0}$, which has $|\mathcal{LU}_{2\text{iso}}^{0}| = 6$. This class coincides with the MMMS states that are called 'classical' in the literature because they are diagonal on a product basis and have zero quantum discord [8].

The above classes constitute a fine-graining of the local stabilizer formalism. For example, while in our case $\mathcal{LU}_{2\text{iso}}^{\epsilon}$ consitute different classes for different values of ϵ, since they give rise to an inequivalent distribution of correlations, they are all equivalent in the local stabilizer setting.

2.3. Average correlations

Given the above classification, we now move on to analyze the average amount of pairwise correlations between observables as measured by the average mutual information

$$\langle \mathcal{I} \rangle_{\Omega} = \frac{1}{2} \langle (1 - x) \log_2(1 - x) + (1 + x) \log_2(1 + x) \rangle_{\Omega} \tag{5}$$

where the average [27] is taken over $(\hat{m}, \hat{n}) \in \Omega = S^2 \times S^2$ i.e. the Bloch spheres for the two qubits where the observables are identified by the unit vectors $\hat{n}, \hat{m}$. The study of this function will allow us to identify, among the above classes of states, those that are extremal with respect to $\langle \mathcal{I} \rangle_{\Omega}$. Evidently, for a fixed direction of the correlation vector $\hat{c}$ the average $\langle \mathcal{I} \rangle_{\Omega}$ is a growing function of κ, and hence of the state's purity. In order to perform the average, we can first evaluate the average over $\hat{n}$ only. To this end, we use the expansion $\ln(1 + x) = \sum_{n=1}^{\infty} \frac{(-1)^{(n+1)}}{n} x^n$ and the fact that $\langle x^{2n+1} \rangle_{(\hat{n})} = 0$ to obtain

$$\frac{1}{2} \langle (1 + x) \log_2(1 + x) + (1 - x) \log_2(1 - x) \rangle_{\hat{n} \in S^2} = \frac{1}{(2 \ln 2)} \sum_{h=1}^{\infty} \frac{\langle x^{2h} \rangle_{\hat{n} \in S^2}}{h(2h - 1)}.$$

Integrating with respect to $\hat{n}$, we get $\langle x^{2h} \rangle_{\hat{n} \in S^2} = \frac{1}{2h+1} R^h$, with $R = (c_1^2 m_1^2 + c_2^2 m_2^2 + c_3^2 m_3^2)$. Upon resumming the series, the overall average mutual information $\langle \mathcal{I} \rangle_{S^2} (\hat{m})$ for a single observable $\hat{m}$ can thus be evaluated as

$$\langle \mathcal{I} \rangle_{S^2} (\hat{m}) = \frac{(1 + R) \operatorname{atanh}\sqrt{R} - \sqrt{R}(1 - \ln(1 - R))}{\sqrt{R} \ln 4}. \tag{6}$$

$\langle \mathcal{I} \rangle_{S^2} (\hat{m})$ is a monotonically growing function of $R = \hat{m} E E^T \hat{m}^T$, and we have $0 \leqslant \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m}) \leqslant 0.278\,65$. The average mutual information $\langle \mathcal{I} \rangle_{\Omega}$ can be obtained by further averaging with respect to $\hat{m}$. The average can only be expressed analytically in simple cases. For the states $\rho_{2\text{iso}}^{0}$, we get

$$\langle \mathcal{I} \rangle_{\Omega} (\kappa) = \frac{-6\kappa + (6 + 2\kappa^2) \operatorname{atanh}\kappa}{8\kappa \log 2} + \frac{\kappa^3 \Phi(\kappa^2, 2, \frac{3}{2}) + 4\kappa \log(1 - \kappa^2)}{8\kappa \log 2}$$

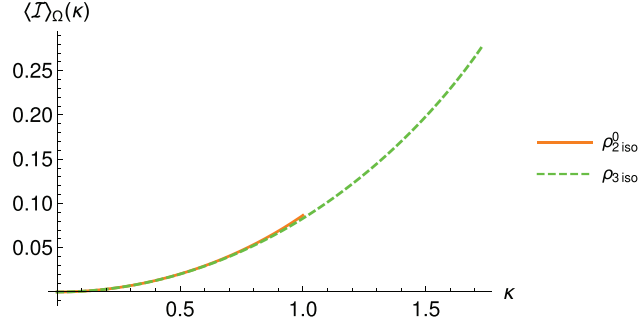where Φ is the Lerch transcendent function. For the isotropic states $\rho_{3\text{iso}}$,

Figure 1. Average mutual information $\langle\mathcal{I}\rangle_\Omega (\kappa)$ for $\rho^0_{2\text{iso}}$ and $\rho_{3\text{iso}}$. The average shows a weak dependence on the symmetry class of the states (see text for discussion).

$$\langle\mathcal{I}\rangle_\Omega (\kappa) = \frac{(3 + \kappa^2)\text{atanh}(\kappa/\sqrt{3})}{\sqrt{3}\kappa \log 4} - \frac{\sqrt{3}\kappa \left(1 - \log\left(1 - \kappa^2/3\right)\right)}{\sqrt{3}\kappa \log 4}.$$

At fixed κ, $\rho^0_{2\text{iso}}$ and $\rho_{3\text{iso}}$ are found to be extremal in terms of the average correlations. Indeed, one can study some general properties of MMMS with respect to $\langle\mathcal{I}\rangle_\Omega (\kappa\hat{c})$ as a function of $\hat{c} = (\sin\alpha\cos\beta, \sin\alpha\sin\beta, \cos\beta)$. The results can be summarized in the following proposition.

Proposition 1. *For fixed $\kappa \leqslant 1$, the states with minimal $\langle\mathcal{I}\rangle_\Omega (\kappa\hat{c})$ are $\rho_{3\text{iso}}$ and the states with maximal $\langle\mathcal{I}\rangle_\Omega (\kappa\hat{c})$ are $\rho^0_{2\text{iso}}$. If $\kappa \geqslant 1$, the minima remain in correspondence with $\rho_{3\text{iso}}$, while the maxima are to be found on the intersection between the sphere of radius κ and the tetrahedron $\mathcal{T}$.*

The proof of proposition 1 can be found in appendix B. In figure 1, we plot $\langle\mathcal{I}\rangle_\Omega (\kappa\hat{c})$ for $\rho_{3\text{iso}}$ and $\rho^0_{2\text{iso}}$. From this plot, one can see that for $\kappa \leqslant 1$ the value of $\langle\mathcal{I}\rangle_\Omega (\kappa\hat{c})$ is essentially determined by the purity of the state and has weak dependence on the direction $\hat{c}$. This fact dims the relevance of the symmetry properties of the correlation distribution, which becomes quite evident when one considers a specific communication protocol, for which only a specific subset of correlations is relevant. For example, the effect of the symmetry is very apparent when one considers the subset of maximally correlated observables, i.e. the subset $\Omega_{\text{Max}} \subset S_2 \times S_2$ defined by $\Omega_{\text{Max}} = \{(\hat{n}_M, \hat{m}_M) \,|\, \hat{n}_M E\hat{m}_M = \max_{\hat{n},\hat{m}} \hat{n}E\hat{m}\}$. For the classes $\mathcal{LU}^{\text{eq}}$ identified above:

- For $\rho^0_{2\text{iso}}$, Ω_{Max} is defined by the equation $n_3 m_3 = 1$, which is only satisfied if $\hat{n} = (0, 0, \pm 1), \hat{m} = (0, 0, \pm 1)$. We have $\Omega_{\text{Max}} = \{\hat{n} = (0, 0, \pm 1), \hat{m} = (0, 0, \pm 1)\}$ with $\dim \Omega_{\text{Max}} = 0$.
- For $\rho^\epsilon_{2\text{iso}}$ and $\epsilon \in \left(1/\sqrt{3}, 1/\sqrt{2}\right)$, Ω_{Max} is defined by the equation $n_1 m_1 + n_2 m_2 = 1$, which is satisfied if the directions of both observables lie on the equatorial circle S_1 (i.e. $m_3 = n_3 = 0$) and are coincident. We have $\Omega_{\text{Max}} \sim S_1$ with $\dim \Omega_{\text{Max}} = 1$.
- For $\rho_{3\text{iso}}$, Ω_{Max} is defined by the equation $\hat{n} \cdot \hat{m} = 1$, which is satisfied if the direction of the two observables coincide. Thus, $\Omega_{\text{Max}} \sim S_2$ with $\dim \Omega_{\text{Max}} = 2$.

Therefore, it is evident that the symmetry can have important implications for protocols based on maximally correlated observables. This will become clear in the discussion about RSP, see for example figure 2 and the related discussion.
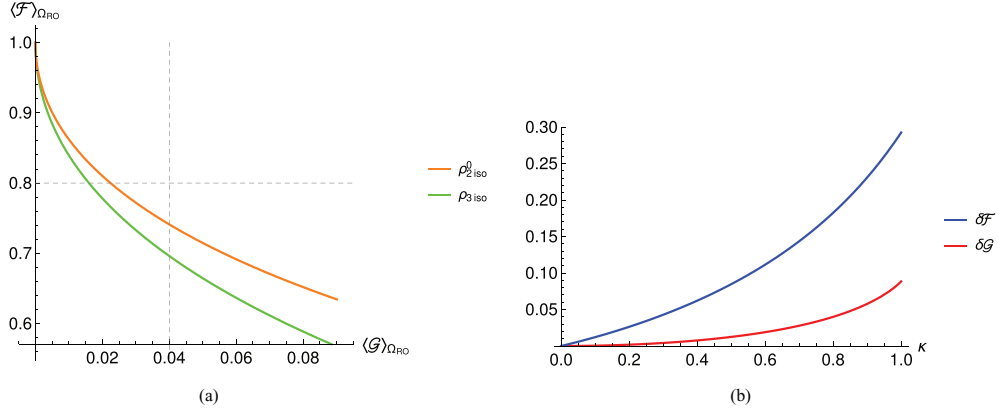
Figure 2. (a) The figure-of-merit $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ versus gain $\langle \mathcal{G} \rangle_{\Omega_{RO}}$ for $\rho^0_{2\mathrm{iso}}$ and $\rho_{3\mathrm{iso}}$ and $0 < \kappa < 1$. At fixed $\langle \mathcal{G} \rangle_{\Omega_{RO}}$ (vertical dashed line), $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ is lower for $\rho_{3\mathrm{iso}}$. At fixed $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ (horizontal dashed line), $\langle \mathcal{G} \rangle_{\Omega_{RO}}$ is lower for $\rho_{3\mathrm{iso}}$. (b) The relative difference between the average gains $\Delta \mathcal{G}$ and the relative difference between the average figures-of-merit $\delta \mathcal{F}$ for $\rho^0_{2\mathrm{iso}}$ and $\rho_{3\mathrm{iso}}$. At fixed purity, the symmetry properties entail differences of up to 8% for the gains and up to 25% for the figures-of-merit.

2.4. Complementarity between correlations and coherence

An important aspect of the correlations between between observables $(\hat{n}, \hat{m})$ is that they can be seen as complementary to the coherence properties of the product basis identified by $\hat{n}, \hat{m}$, i.e. $\mathcal{B}_{(\hat{n}, \hat{m})} = \{|\pm \hat{n}\rangle |\pm \hat{m}\rangle\}$, with respect to the given state. In order to address this point, one can use the coherence function [30, 32] given by $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c}) = \mathcal{H}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c}) - \mathcal{S}(\rho)$ where $\mathcal{H}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c})$ is the entropy of the joint probability distribution obtained by a measurement of the observables identified by $\hat{n}, \hat{m}$. For MMMS, we obtain

$$\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c}) = 2 - \mathcal{I}(\hat{n}, \hat{m})(\vec{c}) - \mathcal{S}(\rho) \tag{7}$$

where $\mathcal{S}(\rho)$ is the von Neumann entropy of ρ. The above formula establishes a clear link between the correlations of the local observables and the coherence of the product bases they define. Therefore, the coherence properties for MMMS can be inferred from $\mathcal{I}(\hat{n}, \hat{m})$ and $\langle \mathcal{I} \rangle_{\Omega}$. We obtain that:

Proposition 2. (*i*) *For fixed $\hat{c}$, $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c})$ and $\langle \mathrm{Coh}(\vec{c}) \rangle_{\Omega}$ are a growing function of κ, i.e. of the purity of the state; (ii) at fixed κ, the higher the correlations between pairs of observables $(\hat{n}, \hat{m})$ the lower their coherence with respect to the global state ρ. (iii) At fixed κ, for all states such that $\hat{c} \in \mathcal{LU}^{\mathrm{eq}}_{\hat{c}}$, $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}$ enjoys the $\mathcal{LU}$ symmetry. (iv) At fixed κ, in general $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c}) \neq \mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(-\vec{c})$, since in general $\mathcal{S}(\rho_{\vec{c}}) \neq \mathcal{S}(\rho_{-\vec{c}})$, and therefore each equivalence class splits as $\mathcal{LU}^{\mathrm{eq}}_{\hat{c}} = \tilde{\mathcal{LU}}^{\mathrm{eq}}_{+\hat{c}} \bigcup \tilde{\mathcal{LU}}^{\mathrm{eq}}_{-\hat{c}}$. (v) All the states such that $\hat{d} \in \tilde{\mathcal{LU}}^{\mathrm{eq}}_{+\hat{c}} \left(\tilde{\mathcal{LU}}^{\mathrm{eq}}_{-\hat{c}} \right)$ have the same value of $\langle \mathrm{Coh}(\vec{c}) \rangle_{\Omega} \left(\langle \mathrm{Coh}(-\vec{c}) \rangle_{\Omega} \right)$.*

The first property simply stems from the fact that the coherence function $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}, \hat{m})}}(\vec{c}) = \mathcal{H}_{\mathcal{B}_{(\hat{n}, \hat{m})}} - \mathcal{S}(\rho)$, since $\mathcal{H}_{\mathcal{B}_{(\hat{n}, \hat{m})}}$ is a growing function of κ and $\mathcal{S}(\rho)$ is a decreasing function of κ.

The second property is quite relevant since it can be stated that for pairs of observables $(\hat{n}, \hat{m})$ correlations and coherence are complementary properties. In particular, for pure (Bell) states, the pairs $(\hat{n}, \hat{m}) \in \Omega_{\mathrm{Max}}$ that have maximal mutual information have minimal coherence. Therefore, communication protocols involving MMMS and that are based on $(\hat{n}, \hat{m})$

pairs can, in principle, be divided into two different categories: those that rely on correlations and those that rely on coherence. Although this subdivision is in principle sharp, we will see that the RSP protocol, for example, falls into the first category. In [33], we have provided an example of a protocol that falls into the second category—quantum phase estimation—which turns out to be based on coherence rather than correlations.

The third property descends from the fact that $\mathcal{S}(\rho)$ is invariant with respect to any unitary rotation in $SU(4)$, and it allows us to extend the discussion had already regarding $\mathcal{I}(\hat{n}, \hat{m})(\vec{c})$ and $\langle \mathcal{I}(\vec{c}) \rangle_\Omega$ to $\mathrm{Coh}_{\mathcal{B}_{(\hat{n}\hat{m})}}(\vec{c})$ and $\langle \mathrm{Coh}(\vec{c}) \rangle_\Omega$, since they inherit the same symmetry properties.

The fourth property marks a difference between the set of states that is locally unitarily equivalent to $\vec{c} = \kappa\hat{c}$ and those that are unitarily equivalent to $\vec{c} = -\kappa\hat{c}$: they both have the same purity, and therefore the same linear entropy, but in general different $\mathcal{S}(\rho_{\vec{c}})$, since the transformation $\hat{c} \to -\hat{c}$ does not preserve the spectrum of ρ. For the states that have higher $\mathcal{S}(\rho_{\vec{c}})$, the pairs $(\hat{n}, \hat{m})$ have the lower coherence. This is a property which is consistent with the fact that states with higher values of $\mathcal{S}(\rho_{\vec{c}})$ are more 'mixed' or entropic when one considers them in terms of their global $SU(4)$ property $\mathcal{S}(\rho)$, which depends on the spectrum.

The fifth property is analogous to the same property for $\mathcal{I}(\hat{n}, \hat{m})(\vec{c})$ and $\langle \mathcal{I}(\vec{c}) \rangle_\Omega$, since $\mathcal{S}(\rho_{\vec{c}})\big(\mathcal{S}(\rho_{-\vec{c}})\big)$ is constant for fixed κ.

3. Relevant observables, useful correlations and performance in RSP

We are now ready to introduce the main quantifiers necessary for the description of how the correlations are used in a remote state preparation protocol. We first define the figure-of-merit $\mathcal{F}$, optimize it, and find out what the *relevant observables* for the protocol are. This will allow us to introduce the *gain* $\mathcal{G}$, which measures the advantage of using the correlations in the protocol. While we mainly focus our discussions on the relevant classes of states previously defined, the tools and procedures we outline can, in general, be applied to any two-qubit state.

3.1. Remote state preparation

Let us start with a brief review of the remote state preparation (RSP) protocol [20, 24]. Starting with a state ϱ_{AB}, two parties A and B wish to prepare an arbitrary pure state $|\hat{n}\rangle$ on the B side belonging to the Bloch sphere circle orthogonal to a given Bloch sphere axis $\hat{\beta}$, where $\hat{n}$ is the vector identifying the state in the Bloch sphere of B, such that $\hat{n} \cdot \hat{\beta} = 0$ (note that here and in the following we will use $\hat{n}$ for both the state $|\hat{n}\rangle$ and the observable $\hat{n} \cdot \vec{\sigma}$; the meaning will be clear from the context). To prepare the state $\hat{n}$ on B, A performs a local measurement on her qubit corresponding to the observable $\hat{m} \cdot \vec{\sigma}$. Depending on the outcome $i = \pm$, the conditional post measurement states of B are identified by the vectors

$$\vec{r}_i = \frac{\vec{b} + i\hat{m}E^T}{2p_i^A} \tag{8}$$

where $p_i^A = \frac{1}{2}(1 + i\hat{m} \cdot \vec{a})$. Upon measurement, A sends a classical message to B revealing the measurement outcome i. If $i = 1$, B leaves his qubit unperturbed; if $i = -1$ he performs a rotation of π around the axis $\hat{\beta}$, $R^\pi(\hat{\beta})$. Taking into account B's conditional rotations, the state in B is:

$$\tilde{\varrho}^B(\hat{m}) = p_+^A \varrho_{B|+} + p_-^A R^\pi(\hat{\beta})\varrho_{B|-} \tag{9}$$

where $\varrho_{B|i}$ are the corresponding post measurement states identified by $\vec{r}_i$. The state $\tilde{\varrho}^B(\hat{m})$ is identified by the Bloch vector

$$\vec{r} = \hat{m}E^T + \left(\vec{b} - \hat{m}E^T\right) \cdot \hat{\beta}\ \hat{\beta} \tag{10}$$

The effectiveness of the protocol depends on how close $\vec{r}$ is to the target state $\hat{n}$.

3.2. Figure-of-merit, relevant observables and gain for MMMS

We now start to analyze the RSP protocol for MMMS and later extend the results to other classes of states. For MMMS, we have

$$p_i^A = \frac{1}{2} \qquad \vec{r}_i = \mathrm{i}\hat{m}E^T \qquad \vec{r} = \hat{m}E^T - \left(\hat{m}E^T\right) \cdot \hat{\beta}\ \hat{\beta}.$$

We first want to estimate the efficiency of the RSP procedure. One natural possibility is to compare the probabilities of a $|\pm\hat{n}\rangle$ measurement performed by **B** on: (i) the desired output state $+\hat{n}$, i.e. $p_+ = 1, p_- = 0$; (ii) the actual output of the protocol $\vec{r}$, i.e. $p_\pm^E = (1 \pm \hat{n} \cdot \vec{r})/2 = \left(1 \pm \hat{n}E\hat{m}^T\right)/2$. We therefore define, as the relevant figure-of-merit, the relative entropy between these probability distributions:

$$\mathcal{F}(\hat{n}, \hat{m}) = p_+ \log_2 \frac{p_+}{p_+^E} + p_- \log_2 \frac{p_-}{p_-^E} = 1 - \log_2(1 + \hat{n}E\hat{m}^T). \tag{11}$$

This function describes how much the probability distribution given by a measurement of $\hat{n}$ onto $\vec{r}$ is statistically distinguishable from the probability distribution given by $p_+ = 1, p_- = 0$. One has that $0 \leqslant \mathcal{F}(\hat{n}, \hat{m})$; $\mathcal{F}(\hat{n}, \hat{m}) = 0$ when $\vec{r} = \hat{n}$; $\mathcal{F}(\hat{n}, \hat{m}) = 1$ when $\hat{n} \cdot \vec{r} = 0$; and $\mathcal{F}(\hat{n}, \hat{m}) \to \infty$ when $\vec{r} \to -\hat{n}$. Therefore, the optimization with respect to the measurement axis $\hat{m}$ along which A has to measure is simple, as $\mathcal{F}(\hat{n}, \hat{m})$ is a decreasing function of $\hat{n}E\hat{m}^T$. Then, since $\hat{n}E\hat{m}^T = (\hat{n}E) \cdot \hat{m}$, the protocol is optimized when $\hat{m}$ is parallel to $\hat{n}E$, i.e. when A measures the observable defined by $\hat{m} = \hat{n}_E \equiv \hat{n}E/|\hat{n}E|$; in this case the post-measurement state on B is defined by $\vec{r}_{\mathrm{opt}} = \hat{n}^E E^T - \left(\hat{n}^E E^T \cdot \hat{\beta}\right)\ \hat{\beta}$, while $\mathcal{F}(\hat{n}, \hat{m})$ is minimal and reads

$$\mathcal{F} \equiv \mathcal{F}(\hat{n}, \hat{n}^E) = 1 - \log(1 + |\hat{n}E|). \tag{12}$$

Note that $\mathcal{F}(\hat{n}, \hat{m})$ is a monotonic function of $\hat{n}E\hat{m}$, which in the literature is called the 'payoff' of the protocol (see e.g. [24]); correspondingly, the optimal measurement n^E is the same as that found in the literature, and $\mathcal{F}$ is a monotonic function of the 'optimal payoff' $|\hat{n}E|$ (for a discussion about different figures-of-merit see also [26]). The above definition immediately leads to the identification of the sub-manifold of *relevant observables* $\Omega_{\mathrm{RO}} \subset S^2 \times S^2$ as the set $\Omega_{\mathrm{RO}} = \left\{ \left(\hat{n}^E, \hat{n}\right) \mid \hat{n} \in S^2 \right\}$. In order to evaluate the average performance of the protocol we compute $\langle \mathcal{F} \rangle = \left\langle \mathcal{F}(\hat{n}, \hat{n}^E) \right\rangle_{\Omega_{\mathrm{RO}}}$, where the average is taken over the submanifold of the relevant observables Ω_{RO}; since $\Omega_{\mathrm{RO}} \sim S^2$, the average is computed with respect to the Haar measure over S^2. Since $|\hat{n}E| = \sqrt{\hat{n}EE^T\hat{n}^T}$, one gets:

Proposition 3. *At fixed κ, for all states corresponding to a given class $\mathcal{LU}_{\hat{c}}^{\mathrm{eq}}$ defined by $\hat{c}$: (i) $\mathcal{F}(\hat{n}, \hat{n}^E)$ is invariant with respect to the action of $\mathcal{LU}$ on ρ; given a state $\hat{n}$ to be transferred, all states connected via $\hat{n} = \hat{n}O_B$, where O_B is the SO(3) representation of U_B such that $U_A \otimes U_B \in \mathcal{LU}$, have the same value of $\mathcal{F}(\hat{n}, \hat{n}^E)$; (ii) the average payoff $\langle \mathcal{F} \rangle_{\Omega_{\mathrm{RO}}}$ is the same for all states corresponding to $\mathcal{LU}_{\hat{c}}^{\mathrm{eq}}$.*

The first property is simply a consequence of the symmetry of the states, i.e. $\hat{n}E\hat{m}^T = \hat{n}O_A EO_B^T \hat{m}^T = \hat{n}_A E\hat{m}_B$; in order to transfer $\hat{n}_A$ one has to measure onto $\hat{m}_B = \hat{n}O_A/|\hat{n}O_A|$ with $|\hat{n}O_A| = |\hat{n}E|$. The second property is a consequence of the invariance of the Haar measure with respect to the local changes of bases that realize the given $\mathcal{LU}$. Finally, both $\mathcal{F}, \langle\mathcal{F}\rangle_{\Omega_{RO}}$ are decreasing functions of κ: the purer the state, the better the (average) result of the protocol.

After having identified the relevant observables, one wants to know what the benefit of using the correlations present in the state is. By this we mean the following. Suppose one does not use the correlations present in the state; this means that B does not perform the conditional rotation on his qubit, so the output of the protocol is $\vec{r} = \vec{b} = \vec{0}$, corresponding to the identity operator $\tilde{\varrho}^B(\vec{r}) = \mathbb{I}_2$. In this case $\mathcal{F}$ (12) is independent of $\hat{n}$ and simply reads

$$\mathcal{F}_{\vec{0}} = 1. \tag{13}$$

Note that the same result is obtained if: (i) A measures an observable $\hat{m}$ such that $\hat{n}E\hat{m} = 0$, i.e. an observable that has zero correlations with respect to $\hat{n}$; (ii) A does not implement any measurement and always sends the bit 0 to B. For any desired output $\hat{n}$, a simple way to compare the two protocols—the one that uses the correlations versus the one that does not—is to compare the corresponding probability distributions: $p_\pm(\vec{r}_{\text{opt}}) = (1 + |\hat{n}E|)/2$, i.e. the probability of measuring $\pm\hat{n}$ on $\vec{r}_{\text{opt}}$; and $p_\pm(\vec{0}) = 1/2$, i.e. the probability of measuring $\pm\hat{n}$ on $\vec{r} = \vec{0}$. By computing the relative entropy of the two distributions, and with some simple algebra, one obtains

$$\mathcal{D}(\vec{r}^{\text{opt}}\|\vec{0}) = \sum_{i=\pm} p_i(\vec{r}_{\text{opt}}) \log_2 \frac{p_i(\vec{r}_{\text{opt}})}{p_i(\vec{0}^E)} = \mathcal{I}(\hat{n}^E, \hat{n}). \tag{14}$$

We define $\mathcal{G}(\hat{n}, \hat{n}^E) \equiv \mathcal{D}(\vec{r}^{\text{opt}}\|\vec{0}) = \mathcal{I}(\hat{n}^E, \hat{n})$ as the *gain function* of the protocol. The meaning of the gain stems, in the first place, from its definition in terms of relative entropy: the higher the $\mathcal{G}$, the higher the statistical distinguishability between the probability distributions $p_\pm(\vec{r}_{\text{opt}})$, $p_\pm(\vec{0})$ obtained by using or not using the correlations. In particular, if $p_\pm(\vec{r}_{\text{opt}}) = p_\pm(\vec{0})$, then $\mathcal{G} = 0$ and there is no profit in using the correlations. Equation (14) establishes a clear connection between the gain one gets in using the correlations in the state and the correlations between the relevant observables Ω_{RO} as measured by the mutual information $\mathcal{I}(\hat{n}^E, \hat{n})$. This is one of the main results of our analysis: among the available correlations, the ones pertaining to the RSP for a given state ρ_{AB} are those that are relevant for the protocol. Thus, if one evaluates the average gain $\langle\mathcal{G}\rangle_{\Omega_{RO}} = \langle\mathcal{I}\rangle_{\Omega_{RO}}$, where the average is taken over the set of relevant observables Ω_{RO}, one immediately has a measure of the correlations tailored to the overall protocol. The next proposition shows that the gain enjoys the same properties as the figure-of-merit $\mathcal{F}$.

Proposition 4. *At fixed κ, for all states corresponding to a given class $\mathcal{LU}_{\hat{c}}^{\text{eq}}$: (i) $\mathcal{G}(\hat{n}, \hat{n}^E)$ is invariant with respect to the action of any $U_A \otimes U_B \in \mathcal{LU}$; in particular, $\forall\hat{n}$ all observables $\hat{n}O_B$, where O_B is the SO(3) representation of U_B such that $U_A \otimes U_B \in \mathcal{LU}$ have the same value of $\mathcal{G}(\hat{n}, \hat{n}^E)$; (ii) the average gain $\langle\mathcal{G}\rangle_{RO}$ is the same for all states corresponding to $\mathcal{LU}_{\hat{c}}^{\text{eq}}$.*

The proof simply follows from the proof of proposition 3 and the fact that both $\mathcal{F}(\hat{n}, \hat{n}^E)$ and $\mathcal{G}(\hat{n}, \hat{n}^E)$ only depend on $|\hat{n}E|$. One has that both $\mathcal{G}, \langle\mathcal{G}\rangle_{\Omega_{RO}}$ are increasing functions of κ, i.e. the purer the state the higher (on average) the correlations between the relevant observables, and the higher the profit one gets in using the correlations. Finally, due to the above definitions of $\mathcal{F}$ and $\mathcal{G}$—and thanks to the connection between the correlation and coherence previously found (7)—one has that for MMMS:

Proposition 5. *Given the desired output $\hat{n}$ and the measurement $\hat{m}$ on A: the optimization of the RSP protocol is equivalent to maximizing the correlations between the observables $\hat{n} \cdot \vec{\sigma}_A$ and $\hat{m} \cdot \vec{\sigma}_B$, or equivalently to minimizing coherence with respect to ρ_{AB} of the product bases defined by $\hat{n}$ and $\hat{m}$.*

Our scheme therefore allows one to neatly distinguish what the relevant resource that matters for the optimization of the RSP protocol is, and to quantify it in the form of the average gain $\langle \mathcal{G} \rangle_{\Omega_{RO}}$. In particular, our scheme allows one to identify the RSP as a protocol that is based on correlations rather than on coherence.

$$\langle \mathcal{F} \rangle_{\Omega_{RO}} \text{ and } \langle \mathcal{G} \rangle_{\Omega_{RO}} \text{ for } \mathcal{LU}_{\hat{c}}^{eq} \text{ states.}$$

We now specify the previous results of some of the classes of states $\mathcal{LU}_{\hat{c}}^{eq}$ defined in the previous section, and we discuss their properties. Both $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ and $\langle \mathcal{G} \rangle_{\Omega_{RO}}$ can be analytically evaluated in simple cases, i.e. for the classes $\mathcal{LU}_{3iso}$ and $\mathcal{LU}_{2iso}^0$. For ρ_{3iso} states $\kappa \in \left[0, \sqrt{3}\right]$ and one has

$$\langle \mathcal{F}_{3iso} \rangle_{\Omega_{RO}} = 1 - \log_2(1 + \kappa/\sqrt{3}) \tag{15}$$

$$\langle \mathcal{G}_{3iso} \rangle_{\Omega_{RO}} = \langle \mathcal{I}_{3iso} \rangle_{\Omega_{RO}} = \frac{1}{2}\left((1 + \kappa/\sqrt{3}) \log_2(1 + \kappa/\sqrt{3}) + (1 - \kappa/\sqrt{3}) \log_2(1 - \kappa/\sqrt{3})\right). \tag{16}$$

For ρ_{2iso}^0 (the so-called 'classical states') $\kappa \in [0, 1]$ and

$$\left\langle \mathcal{F}_{2iso}^0 \right\rangle_{\Omega_{RO}} = 1 - \frac{(1 + \kappa) \ln(1 + \kappa) - \kappa}{\kappa \ln 2} \tag{17}$$

$$\left\langle \mathcal{G}_{2iso}^0 \right\rangle_{\Omega_{RO}} = \left\langle \mathcal{I}_{2iso}^0 \right\rangle_{\Omega_{RO}} = \frac{(1 + \kappa)^2 \ln(1 + \kappa)}{4\kappa \ln 2} - \frac{(1 - \kappa)^2 \ln(1 - \kappa) + 2\kappa}{4\kappa \ln 2}. \tag{18}$$

The above functions are important since the classes of states $\mathcal{LU}_{3iso}$ and $\mathcal{LU}_{2iso}^0$ are *extremal* in the sense specified by the following proposition, which holds for all two-qubit states, as we shall see when we discuss non-MMMS.

Proposition 6. *(i) For purity $\kappa \leqslant 1$, ρ_{3iso} states attain the minimum of both $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ and $\langle \mathcal{G} \rangle_{\Omega_{RO}}$, while the maximum is attained by the class of ρ_{2iso}^0 states; (ii) For $1 \leqslant \kappa \leqslant \sqrt{3}$, the minimum of both $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ and $\langle \mathcal{G} \rangle_{\Omega_{RO}}$ is attained by ρ_{3iso}, while the maxima are found at the intersection between the sphere of radius κ and the tetrahedron $\mathcal{T}$.*

The proof is given in appendix B. Proposition 6 identifies the classes of states, i.e. ρ_{3iso}, which allow us to obtain, at fixed κ, the best performance both in terms of $\mathcal{F}$ and the resources needed in RSP. From proposition 6, it follows that the ρ_{3iso} states are those that give the best performance for a fixed amount of average relevant resources $\langle \mathcal{G} \rangle_{\Omega_{RO}}$, i.e. the smallest $\langle \mathcal{F} \rangle_{\Omega_{RO}}$. On the other hand, if one fixes the value of $\langle \mathcal{F} \rangle_{\Omega_{RO}}$, the ρ_{3iso} states are those that require the least amount of resources to obtain the same performance. The previous statements are exemplified in figure 2(a).

These results can be understood, since in the case of ρ_{3iso} states the output state of the protocol $\hat{r} = E^T \hat{n}^E \propto \hat{n}$, i.e. it is always orthogonal to the given $\hat{\beta}$ and parallel to the desired output state $\hat{n}$. Therefore, $\Omega_{RO} \sim S^2 \equiv \Omega_{Max}$, i.e. the manifold of relevant observables coincides with the manifold of maximally correlated observables. For non-isotropic states this is no longer true except for a subset of states. For example, for ρ_{2iso}^ϵ this is true iff $\hat{\beta} = \hat{z}$, i.e. for the manifold $S^1 \sim \Omega_{Max} \subset \Omega_{RO}$ of maximally correlated states, while for ρ_{2iso}^0 this is true

for a single pair of observables ($\hat{m} = \hat{z}, \hat{n} = \hat{z}$). Therefore, for non-isotropic states and for a general desired output $\hat{n}$ and $\hat{r} \nparallel \hat{n}$, in order to obtain the same value of $|\hat{n}E|$—and thus the same $\mathcal{F}$—non-isotropic states must have a higher value of κ: they must be purer and employ more resources—in terms of the correlations between the relevant observables—than the isotropic ones.

Our results can be summarized in the following way: for a given state ρ_{AB} the actual resources used in RSP are, on the one hand, the purity, which determines the amount of correlations between the relevant observables as measured by $\langle \mathcal{G} \rangle_{\Omega_{RO}}$, and on the other hand, the way (symmetry) in which the correlations are distributed. Figure 2(b) exemplifies the role of symmetry at a fixed purity by showing the relative differences $\delta\mathcal{G} = \left(\langle \mathcal{G}^0_{2\text{iso}} \rangle_{\Omega_{RO}} - \langle \mathcal{G}_{3\text{iso}} \rangle_{\Omega_{RO}} \right) / \langle \mathcal{G}_{3\text{iso}} \rangle_{\Omega_{RO}}$ and $\delta\mathcal{F} = \left(\langle \mathcal{F}^0_{2\text{iso}} \rangle_{\Omega_{RO}} - \langle \mathcal{F}_{3\text{iso}} \rangle_{\Omega_{RO}} \right) / \langle \mathcal{F}_{3\text{iso}} \rangle_{\Omega_{RO}}$ as a function of κ; while the gains differ by at most 8%, the corresponding figures-of-merit differ by up to 25%. At fixed purity, the symmetry properties entail large differences in the figures-of-merit.

Our treatment of the RSP explains the results presented in the literature from quite a different point of view. For example, in [24], the average performance at a given axis $\hat{\beta}$ is expressed in terms of $\langle |E\hat{n}|^2 \rangle_{S(\hat{\beta})}$, where $S(\hat{\beta})$ is the circle on the Bloch sphere orthogonal to $\hat{\beta}$. If one minimizes this average performance with respect to the choice of $\hat{\beta}$, one has that $\min_{\hat{\beta}} \langle |E\hat{n}|^2 \rangle_{S(\hat{\beta})} = (c_1^2 + c_2^2)/2$, where $|c_1|, |c_2|$ are the minimal singular values of the correlation tensor E. Therefore, the worst case is given by the $\rho^0_{2\text{iso}}$ states for which $\min_{\hat{\beta}} \langle |E\hat{n}|^2 \rangle_{S(\hat{\beta})} = 0$. In our language, this simply follows from the symmetry properties of such states that imply the existence of a circle $S(\hat{\beta})$ of relevant observables, which are in fact uncorrelated; therefore on this circle $\mathcal{G} = 0$ and $\mathcal{F}$ is maximal (worst).

3.3. States with non-maximally mixed marginals $\vec{a}, \vec{b} \neq \vec{0}$

We now move on to analyze the states with non-maximally mixed marginals. In this case, the state prepared by the protocol is $\vec{r} = E^T \hat{m} + \left(\vec{b} - E^T \hat{m} \right) \cdot \hat{\beta} \, \hat{\beta}$. Since the state to be transferred is orthogonal to $\hat{\beta}$, $\hat{n} \cdot \vec{r} = \hat{n}E\hat{m}^T$ and therefore the performance is still given by equation (11) and A can maximize it (12) by performing a measurement defined by the same observable $\hat{m} = \hat{n}^E = \hat{n}E/|\hat{n}E|$. The protocol therefore relies on the correlations of the MMMS, which can be obtained by setting $\vec{a} = \vec{0}, \vec{b} = \vec{0}$, i.e. $\rho_{AB}(\vec{a} = \vec{0}, \vec{b} = \vec{0})$. Therefore, the condition that leads to the choice of the optimal measurement $\hat{m} = \hat{n}^E$ is equivalent to maximizing the correlations between $\hat{m}$ and $\hat{n}$, which are present in $\rho_{AB}(\vec{a} = \vec{0}, \vec{b} = \vec{0})$ rather than in ρ_{AB}.

As for the evaluation of the gain, for non-MMMS states, one is led to compare two different situations. In the first case, the procedure making use of the correlations is the same as the one described for MMMS, and we refer to it as $\mathcal{P}^U_{\vec{b}}$; correspondingly the figure-of-merit in the optimal case is again (12). In the second case, in which correlations are not used, one can implement a procedure that is based on the polarization properties of ρ_B. This procedure, which we call $\mathcal{P}^{UN}_{\vec{b}}$ for a reason that will shortly be clear, can be implemented as follows: if $\hat{n} \cdot \vec{b} > 0$ ($\hat{n} \cdot \vec{b} < 0$), A always sends the bit 0(1) so that B never (always) rotates its state, and the post measurement state is correspondingly $\vec{b} \left(-\vec{b} \right)$. With this procedure, the probability of measuring $\hat{n}$ on $\vec{b} (-\vec{b})$ is $p_{\pm}(\vec{b}) = (1 \pm |\hat{n} \cdot \vec{b}|)/2$. Therefore, for $\mathcal{P}^{UN}_{\vec{b}}$, the figure-of-merit $\mathcal{F}^{UN} = \mathcal{F}^{UN}(\hat{n}, \vec{b})$ can be derived as in (11) and it reads

$$\mathcal{F}^{UN} = 1 - \log_2(1 + |\hat{n} \cdot \vec{b}|). \tag{19}$$

Introducing the procedure $\mathcal{P}_{\vec{b}}^{UN}$ allows us to devise the following optimized protocol, $\mathcal{P}_{\vec{b}}^{\text{opt}}$, which has a higher efficiency than the original RSP. Indeed, what A must now do for any given $\hat{n}$ is to choose whether or not to use the correlations present in the state—i.e. whether to use the procedure $\mathcal{P}_{\vec{b}}^{U}$ or $\mathcal{P}_{\vec{b}}^{UN}$. To this end, A must compare the figures-of-merit of the two procedures: whenever $\mathcal{F}^{U}(\hat{n}) < \mathcal{F}^{UN}(\hat{n})$, i.e whenever $|\hat{n}E| > |\hat{n} \cdot \vec{b}|$, A uses the state's correlations; otherwise A does not use them and enacts $\mathcal{P}_{\vec{b}}^{UN}$. Thus, depending on the desired output state, correlations can be *useful* or *unuseful* for optimizing the overall RSP performance. This fact leads us to identify the resources needed for RSP as correlations that are both relevant and useful. Given κ and $\vec{b}$, the set of 'relevant and useful observables'—i.e. that which provides the relevant and useful correlations—is $\Omega_{\kappa,b}^{U} = \left\{ (\hat{n}^{E}, \hat{n}) |\ |\hat{n}E| > |\hat{n} \cdot \vec{b}| \right\}$. The set of relevant observables is therefore given by the disjoint union $\Omega_{\text{RO}} = \Omega_{\kappa,b}^{U} \bigcup \Omega_{\kappa,b}^{UN}$, where $\Omega_{\kappa,b}^{UN} = \left\{ (\hat{n}^{E}, \hat{n}) |\ |\hat{n}E| < |\hat{n} \cdot \vec{b}| \right\}$ is a set of relevant but 'unuseful' observables, since $(\hat{n}^{E}, \hat{n}) \in \Omega_{\kappa,b}^{UN}$, $\mathcal{F}^{U}(\hat{n}) > \mathcal{F}^{UN}(\hat{n})$. The overall figure-of-merit of our optimized protocol $\mathcal{P}_{\vec{b}}^{\text{opt}}$ can then be written as:

$$\mathcal{F}^{\text{opt}} = \mathcal{F}^{U}(\hat{n}) \, \chi_{\Omega_{\kappa,b}^{U}} + \mathcal{F}^{UN}(\hat{n}) \, \chi_{\Omega_{\kappa,b}^{UN}} \tag{20}$$

where $\chi_{\Omega_{\kappa,b}^{U}} \left(\chi_{\Omega_{\kappa,b}^{UN}} \right)$ is the indicator function that identifies the set of useful (unuseful) observables for a given $\kappa, \vec{b}$. We notice that $\mathcal{F}^{\text{opt}}$ correctly takes into account the asymmetry of the RSP with respect to the exchange of the role of A and B and that is manifest for non-MMMS whenever $\vec{a} \neq \vec{b}$. In order to better understand which of the relevant correlations are useful, one can simply note that the condition $|\hat{n}E| > |\hat{n} \cdot \vec{b}|$ is equivalent to requiring the post measurement states $\vec{r}_{+}, \vec{r}_{-}$ defined in (10) to satisfy

$$(\hat{n} \cdot \vec{r}_{+})(\hat{n} \cdot \vec{r}_{-}) \leqslant 0. \tag{21}$$

In other words, the components of the vectors $\vec{r}_{+}$ and $\vec{r}_{-}$ along the direction defined by $+\hat{n}$ should be opposite in verse. Indeed, suppose both components have the same verse of $+\hat{n}$, for example if $(\hat{n} \cdot \vec{r}_{+}) > 0, (\hat{n} \cdot \vec{r}_{-}) > 0$; then $R_{\beta}^{\pi} \vec{r}_{-}$ contributes to the final output state $\vec{r}$ (9) with a component parallel to $-\hat{n}$, which is orthogonal to the desired output state $+\hat{n}$. Therefore, the rotation of $\vec{r}_{-}$ around the $\hat{\beta}$ axis required by the standard RSP protocol is detrimental to the performance. With our modified protocol, the latter is measured by $\langle \mathcal{F}^{\text{opt}} \rangle_{\Omega_{\text{RO}}}$, which now has two contributions $\left\langle \mathcal{F}^{U}(\hat{n}) \, \chi_{\Omega_{\kappa,b}^{U}} \right\rangle_{\Omega_{\text{RO}}}$, and $\left\langle \mathcal{F}^{UN}(\hat{n}) \, \chi_{\Omega_{\kappa,b}^{UN}} \right\rangle_{\Omega_{\text{RO}}}$. As for the properties of $\mathcal{F}^{\text{opt}}$ and $\langle \mathcal{F}^{\text{opt}} \rangle_{\Omega_{\text{RO}}}$ one has:

Proposition 7. (*i*) *For a fixed* $\vec{b}$, $\mathcal{F}^{\text{opt}}$ *and* $\langle \mathcal{F}^{\text{opt}} \rangle_{\Omega_{\text{RO}}}$ *are decreasing functions of* κ; (*ii*) *for a given* $\kappa, \vec{b}$, *states that are obtained by the transformations that connect the unit vectors belonging to a given class* $\mathcal{LU}_{\hat{c}}^{\text{eq}}$ *have the same value of* $\langle \mathcal{F}^{\text{opt}} \rangle_{\Omega_{\text{RO}}}$.

The proof of proposition 7 can be found in appendix D. The above considerations demonstrate that our modified protocol $\mathcal{P}_{\vec{b}}^{\text{opt}}$, which distinguishes between useful and unuseful correlations, can in general give a better performance than the standard RSP.

We now turn to the definition of the gain function for non-MMMS states. The procedure is analogous to the one seen for MMMS, with two main differences. On the one hand, the two probability distributions we want to compare are now: $p_{\pm}(\vec{r}_{\text{opt}}) = (1 \pm |\hat{n}E|)/2$, i.e. the probability of measuring $\pm\hat{n}$ on $\vec{r}_{\text{opt}}$, and $p_{\pm}(\vec{b}) = (1 \pm |\hat{n} \cdot \vec{b}|)/2$, i.e. the probability of measuring $\pm\hat{n}$ on $\vec{r} = \vec{b}(-\vec{b})$—the latter being the same probability used for the definition of $\mathcal{F}^{UN}$. On the

other hand, we want to restrict the evaluation of the gain to the set of useful observables $\Omega_{\kappa,b}^U$, i.e. for the part $\mathcal{P}_{\vec{b}}^U$ of the protocol that effectively makes use of the correlations. We therefore have for $\left(\hat{n}^E, \hat{n}\right) \in \Omega_{\kappa,b}^U$, and after some manipulations

$$\mathcal{D}(\vec{r}^{\,\text{opt}}, \vec{b}) = \sum_{i=\pm} p_i(\vec{r}_{\text{opt}}) \log_2 \frac{p_i(\vec{r}_{\text{opt}})}{p_i(\vec{b})}$$

$$= \mathcal{I}(\hat{n}^E, \hat{n})_{(\vec{a}=\vec{0}, \vec{b}=\vec{0})} + \frac{1}{2}(1 + |\hat{n}E|) \log(1 + |\hat{n} \cdot \vec{b}|) + \frac{1}{2}(1 - |\hat{n}E|) \log(1 - |\hat{n} \cdot \vec{b}|).$$

The gain $\mathcal{G}^U \equiv \mathcal{D}(\vec{r}^{\,\text{opt}}, \vec{b})$ explicitly depends on the correlations $\mathcal{I}(\hat{n}^E, \hat{n})_{(\hat{a}=\vec{0}, \hat{b}=\vec{0})}$ between the relevant observables for the corresponding MMMS $\rho_{AB}(\vec{a} = \vec{0}, \vec{b} = \vec{0})$. Therefore, the desired measure of correlations for the modified protocol is simply given by the mutual information $\mathcal{I}(\hat{n}^E, \hat{n})_{(\hat{a}=\vec{0}, \hat{b}=\vec{0})}$. This implies that the correlation properties of $\rho_{AB}(\vec{a} = \vec{0}, \vec{b} = \vec{0})$ rather than ρ_{AB} are those that matter for the protocol. This shift of attention from ρ_{AB} to $\rho_{AB}(\vec{a} = \vec{0}, \vec{b} = \vec{0})$ is a direct result of our approach. A simple study reveals that $\mathcal{G}^U$ is a growing function of κ and a decreasing function of $b = |\vec{b}|$. These properties can be understood by first analyzing the case in which $\Omega_{\kappa,b}^U = \Omega_{\text{RO}}$, i.e. all relevant correlations are useful, and by considering the difference $\Delta \mathcal{F} = \left(\mathcal{F}^{UN} - \mathcal{F}^U\right)$. When κ grows $\mathcal{F}^U$ decreases and thus $\Delta \mathcal{F}$, i.e. the gap between the performance of the two protocols grows, and it becomes even more convenient to use the correlations in the protocol. On the other hand, if b grows the opposite happens: it is $\mathcal{F}^{UN}$ that decreases and thus $\Delta \mathcal{F}$ becomes smaller. The behavior of $\mathcal{G}^U$ correctly reproduces these features with respect to the variations of κ and b. As for the average gain, one defines $\left\langle \mathcal{G}^U \right\rangle = \left\langle \mathcal{D}(\hat{n}^E, \vec{b}) \chi_{\Omega_{\kappa,b}^U} \right\rangle_{\Omega_{\text{RO}}}$. The average is taken over the whole set of relevant observables $\Omega_{\text{RO}} \sim S^2$ and the integrand is different from zero over the set $\chi_{\Omega_{\kappa,b}^U}$ and zero otherwise. When b increases, $\left\langle \mathcal{G}^U \right\rangle$ decreases, not only due to its functional dependence on b, but also because of the restriction of the domain $\Omega_{\kappa,b}^U$ over which it is evaluated. The proper average measure of correlations for the modified protocol is simply given by the average of the mutual information $\mathcal{I}(\hat{n}^E, \hat{n})_{(\hat{a}=\vec{0}, \hat{b}=\vec{0})}$ over the set of useful correlations, i.e. $\left\langle \mathcal{I}^U \right\rangle = \left\langle \mathcal{I}(\hat{n}^E, \hat{n})_{(\hat{a}=\vec{0}, \hat{b}=\vec{0})} \chi_{\Omega_{\kappa,b}^U} \right\rangle_{\Omega_{\text{RO}}}$.

We conclude this section by analyzing the properties of $\mathcal{G}^U$ and $\mathcal{F}^{\text{opt}}$ for some relevant classes of non-MMMS.

3.3.1. Example: pure states. Thanks to the Schmidt decomposition, the pure states can be written as $\lambda |00\rangle + \sqrt{1 - \lambda^2}|11\rangle$ for some choice of local bases. Therefore, their correlation matrix can be expressed as $E = \text{diag}(2\lambda\sqrt{1 - \lambda^2}, -2\lambda\sqrt{1 - \lambda^2}, 1)$ and their local Bloch vectors as $\vec{a} = \vec{b} = (0, 0, 2\lambda^2 - 1)$, in terms of the single parameter λ. It is then easy to check that for pure states $\Omega_{\kappa,b}^U = \Omega_{\text{RO}}$, i.e. all relevant observables are useful. In figure 3(a) we plot $\left\langle \mathcal{G}^U \right\rangle$ and $\left\langle \mathcal{F} \right\rangle_{\Omega_{\text{RO}}}$; the latter are respectively maximal and minimal for the pure Bell states, i.e. given the fixed purity for states that are maximally isotropic.

3.3.2. Example: isotropic case. As for the isotropic case, one can first evaluate $\left\langle \mathcal{G}_{3\text{iso}}^U \right\rangle$ when κ and $|\vec{b}|$ are such that $\Omega_{\text{RO}} \equiv \Omega_{\kappa,b}^U$, i.e. when $\kappa/\sqrt{3} > |\vec{b} \cdot \hat{n}|$, $\forall \hat{n}$ and all relevant correlations are useful. In this case the gain reads

$$\left\langle \mathcal{G}_{3\text{iso}}^U \right\rangle = \left\langle \mathcal{G}_{3\text{iso}} \right\rangle_{\Omega_{\text{RO}}} + \left(1 - \frac{f(1) - f(-1)}{6b}\right) / \ln 2 \tag{22}$$

where $\langle \mathcal{G}_{3\mathrm{iso}} \rangle_{\Omega_{\mathrm{RO}}} = \langle \mathcal{I}_{3\mathrm{iso}} \rangle_{\Omega_{\mathrm{RO}}}$ is given by (16), i.e. the result obtained for $|\vec{b}| = 0$, while the average of the part depending on $\vec{b}$ can be written in terms of $f(\pm 1) = (1 \pm b)\left(3 \pm \kappa\sqrt{3}\right)\ln(1 \pm b)$ and the result depends on $b = |\vec{b}|$ only. In this case, $\langle \mathcal{F}_{3\mathrm{iso}}^{\mathrm{opt}} \rangle = \langle \mathcal{F}_{3\mathrm{iso}}^{U} \rangle_{\Omega_{\mathrm{RO}}}$ and it is given by (15). If now $\kappa/\sqrt{3} < |\vec{b}|$ and $\Omega_{\kappa,b}^{U} \subset \Omega_{\mathrm{RO}}$ one has to properly adjust the limits of the integrations in order to implement both for $\mathcal{G}^{U}$ and $\mathcal{F}^{\mathrm{opt}}$, the $\chi_{\Omega_{\kappa,b}^{U}}$ and $\chi_{\Omega_{\kappa,b}^{UN}}$. The integrations can be carried out analytically and the result is plotted for the whole set of parameters κ, b for which the state is positive in figure 3(b). In the figure we show $\langle \mathcal{G}_{3\mathrm{iso}}^{U} \rangle$ and $\langle \mathcal{F}_{3\mathrm{iso}}^{\mathrm{opt}} \rangle$; they both attain their optimal value (1 and 0 respectively) for $\kappa = 1$. The benefit in using our modified protocol can be appreciated in figure 4 where we have plotted the difference between the average figure-of-merit pertaining to the usual RSP, given by equation (15) and $\langle \mathcal{F}_{3\mathrm{iso}}^{\mathrm{opt}} \rangle$ for the optimized protocol $\mathcal{P}_{\vec{b}}^{\mathrm{opt}}$. When $\kappa/\sqrt{3} > |\vec{b}|$, one has $\Omega_{\mathrm{RO}} = \Omega_{\kappa,b}^{U}$, the two protocols coincide and they have the same efficiency such that $\Delta \langle \mathcal{F} \rangle_{\Omega_{\mathrm{RO}}} = 0$; when $\kappa/\sqrt{3} < |\vec{b}|$ the optimized protocol performs better, and $\Delta \langle \mathcal{F} \rangle_{\Omega_{\mathrm{RO}}} > 0$.

The results discussed in this section concern a simple yet paradigmatic example of the quantum communication protocol, RSP. They show how the approach introduced allows proper protocol-tailored measures of correlations for both MMMS and non-MMMS states to be defined. Furthermore, the new perspective allows, in general, the role of symmetry in the states' correlation distribution (e.g. proposition 6) to be highlighted, and allows new optimized protocols to be devised that may have better efficiencies. The role of symmetry is further analyzed in the following section.

4. RSP and symmetry

The main theme of our discussion is the interplay between the two main resources that characterize the performance of a given quantum protocol: state purity and correlation symmetry. In particular, we have emphasized the importance of the way the relevant correlations are distributed in a given state, and how this property determines the performance of a given protocol. In this section we discuss, in a simplified situation, how the specific kind of symmetry of a given state ρ_{AB} determines the conditions for the implementation of the RSP. The original protocol is based on:

- the set-up of a communication channel, which is realized when A sends part of her state to B;
- the ability to realize local measurements along an arbitrary axis on the A side (which is equivalent to the ability of realizing an arbitrary $SU(2)$ rotation and a measurement along a given fixed axis);
- the ability to locally realize π rotations around an arbitrary axis $\hat{\beta}$ on the B side.

The basic RSP first requires the communication channel to be set up, then, after the measurement of the A side and the communication of the result to B, a π rotation around a given axis $\hat{\beta}$. In the following, we analyze the protocol in terms of the resources needed, in terms of the symmetry of the state and in terms of the characteristic times of the protocol: t_{ch}, $t_{\hat{\beta}}$, $t_{\hat{n}}$. We have that t_{ch} is the time in which the channel between A and B is set up; $t_{\hat{\beta}}$ is the time in which the decision about the axis $\hat{\beta}$ is taken by A and B, while $t_{\hat{n}}$ is the time when A gets to know what the state $\hat{n}$ to be transferred is. The goal of our game is to obtain the same average value of $\mathcal{F}$ (12) for states with different symmetries; this is in general possible but it requires the
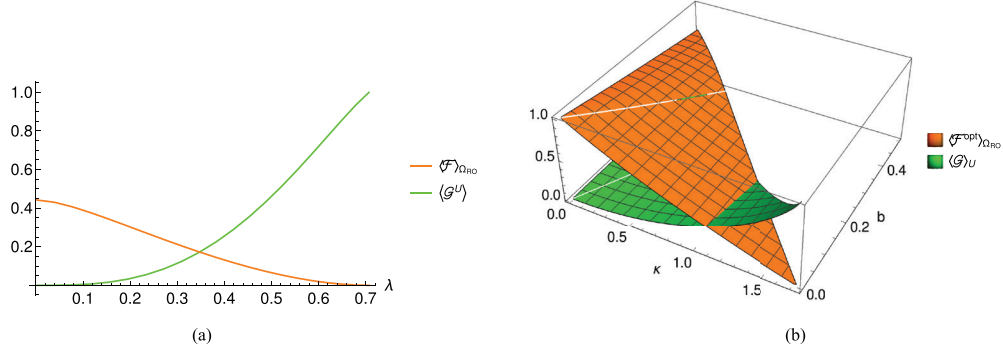
Figure 3. (a) The average figure-of-merit $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ and gain $\langle \mathcal{G}^U \rangle$ for pure states as a function of the Schmidt coefficient λ; (b) the $\langle \mathcal{F}^{opt} \rangle_{\Omega_{RO}}$ and gain $\langle \mathcal{G}^U \rangle$ for isotropic states as a function of κ and b. The protocol only uses useful correlations to the left of the cuts in the plots. (The domain of the plot is given by the values of κ and b for which the state is defined.)

basic protocol to be modified, and some constraints to be added to the relations among t_{ch}, $t_{\hat{\beta}}$, and $t_{\hat{n}}$. The simplification we adopt is the following: A sends to B part of her state ρ_{AB} through a channel that does not change state (perfect channel). This is quite a strong restriction, indeed if the channel is perfect, A could choose to send the state $|\hat{n}\rangle$ directly to B. But since we deal with the relation between the performance of the protocol and the correlations present in a state, the example allows us to discuss the relation between RSP and symmetry. We focus on MMMS belonging to different classes, and each state will have the maximum purity allowed by its class, i.e. $\kappa = \max_{\hat{c} \in \mathcal{L}\mathcal{U}_{eq}} k_{Max}(\hat{c})$.

Suppose now ρ_{AB} belongs to the class ρ_{3iso}, then $\kappa = \sqrt{3}$ and ρ_{AB} is a pure Bell state. A and B can then proceed with the usual protocol, and they are free to choose three times such that $t_{ch} < t_{\hat{\beta}}$, $t_{\hat{n}}$, i.e. A can set up the channel before knowing $\hat{\beta}$ and $\hat{n}$. The figure-of-merit of the protocol and the gain are $\mathcal{F}_{3iso}(\hat{n}) = 0, \mathcal{G}_{3iso} = 1$ for all $\hat{n}$ and hence also on average.

Suppose now ρ_{AB} is such that $\hat{c} = (1/\sqrt{2}, 1/\sqrt{2}, 0)$ and $\kappa = 1/\sqrt{2}$; the state belongs to the class ρ_{2iso}^{ϵ}, with $\epsilon = 1/\sqrt{2}$, it is separable and its discord is different from zero. In this case, A can do the following: *before* setting up the channel and *after* she gets to know $\hat{\beta}$, A rotates B's qubit with a single rotation $U_{\hat{\beta}}$ that implements the rotation $\hat{z} \to \hat{\beta}$ on the corresponding Bloch sphere; then A sends the qubit to B. When she knows the desired $\hat{n}$, by a proper rotation U_{xy} she rotates her measuring axes that will lie in the xy plane of her Bloch sphere. The rest of the protocol is the usual one. It turns out that $\mathcal{F}_{2iso}^{1/\sqrt{2}}(\hat{n}) = \mathcal{F}_{3iso}^{\kappa}(\hat{n}) > 0$ and $\mathcal{G}_{2iso}^{0} = \mathcal{G}_{3iso}^{\kappa} < 1$ with $\kappa = \sqrt{3}/2$. Again, the resources used in terms of local rotations, i.e. $U_{\hat{\beta}}, U_{xy} \sim SU(2)$ are the same as before, since in general $U_{\hat{\beta}}$ is determined by two real parameters and U_{xy} by a single real parameter (the angle on the xy circumference). However, in this case it must be $t_{\hat{\beta}} < t_{ch} < t_{\hat{n}}$. Once again by using the same resources and a mixed state one can obtain the same performance of an isotropic state, which for $\kappa = \sqrt{3}/2$ is purer than the state $\rho_{2iso}^{1/\sqrt{2}}$, and is both entangled and discordant. However, symmetry in this case only allows A to set up the channel before knowing $\hat{n}$, but after she gets to know $\hat{\beta}$.

Suppose now A is allowed to use the state $\sigma = (|00\rangle\langle00| + |11\rangle\langle11|)/2$—the state belongs to the class ρ_{2iso}^{0}, $\kappa = 1$ and it is called 'classical' in some parts of the literature [8]— in particular, σ has zero entanglement and zero discord. A can modify the protocol as follows: instead of using the $SU(2)$ rotations for measuring along different axes, after A gets
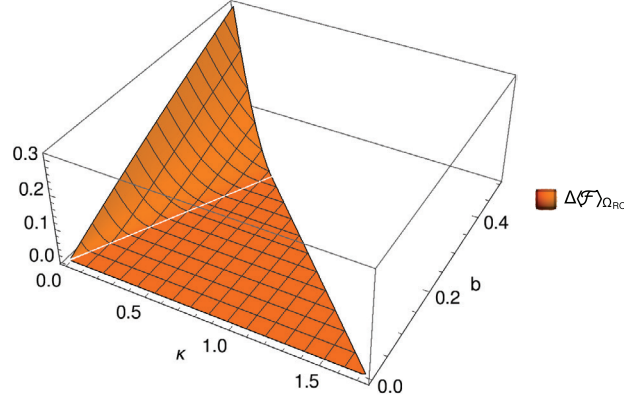
Figure 4. $\Delta \langle \mathcal{F} \rangle_{\Omega_{RO}}$: the difference between the average figure-of-merit $\langle \mathcal{F} \rangle_{\Omega_{RO}}$ evaluated for the usual RSP, which always uses the relevant correlations (equation (15)), and our modified protocol based on useful correlations ($\langle \mathcal{F}_{3iso}^{opt} \rangle$ in the text, based on equation (20)); when $\kappa/\sqrt{3} > |\vec{b}|$ one has $\Omega_{RO} \equiv \Omega_{\kappa,b}^{U}$, the two protocols coincide and $\Delta \langle \mathcal{F} \rangle_{\Omega_{RO}} = 0$; when $\kappa/\sqrt{3} < |\vec{b}|$ the performance of the modified protocol is better, i.e. $\Delta \langle \mathcal{F} \rangle_{\Omega_{RO}} > 0$ (the domain of the plot is given by the values of κ and b for which the state is defined).

to know both $\hat{\beta}, \hat{n}$, and before building the channel, she applies the rotation on the B part of the state such that $\rho \rightarrow \rho_{\hat{n}} = (|0\hat{n}\rangle \langle 0\hat{n}| + |1, -\hat{n}\rangle \langle 1, -\hat{n}|)/2$; A then sends the second qubit to B, implementing measurements along the $\hat{z}$ axis on her qubit, and the protocol proceeds as usual. One has that $\mathcal{F}_{2iso}^{0}(\hat{n}) = \mathcal{F}_{3iso}(\hat{n}) = 0$, and $\mathcal{G}_{1iso} = \mathcal{G}_{3iso} = 1$ for all $\hat{n}$ and on average. The resources used in this case are the same as in the previous ones ($SU(2)$ rotations on the A side, $R_{\pi}(\hat{\beta})$ rotations on the B side). Therefore, by using the same resources and a so-called classical mixed state (zero discord and entanglement) one can obtain the same performance one gets with a pure Bell state. The main and relevant difference is that now $t_{\hat{\beta}}$, $t_{\hat{n}} < t_{ch}$, i.e. A has to set up the channel after she gets to know both $\hat{\beta}$ and $\hat{n}$.

The bottom line of the above discussion is that in the described set-up (perfect channel), it is the way the correlations are distributed among the relevant observables that matters in defining: (i) which kind of freedom one has in realizing the different steps of the protocol, and (ii) in which way one has to use the same $SU(2)$ rotations. The modified protocols for the states $\rho_{2iso}^{1/\sqrt{2}}, \rho_{2iso}^{0}$ do not change their correlation content; they make use of the same ability to perform $SU(2)$ rotations as in the original protocol. The rotations are now used in a way that compensates for the lack of symmetry in the states, in order to reorient the correlation distribution among the different observables, such that the protocol—as dummy as it may appear—is as efficient as possible with the given purity. In particular, in the case of the state ρ_{2iso}^{0}, the protocol is as efficient as the one that makes use of pure Bell states. The above results seem to depend on the different symmetries of the states, rather than their supposed 'quantumness' or 'classicality'. Indeed, the freedom in the choice of t_{ch} is guaranteed by the symmetry of the distribution of correlations between the relevant observables (the ones that are perfectly correlated or anti-correlated). The states with isotropic correlations allow a total freedom for all values of purity, even in the absence of entanglement. These states are always discordant, but here the presence of discord simply records the presence of a sufficient amount of the 'right' symmetry.

We finally note that, in principle, it depends on A's will or needs (and on her specific experimental constraints) to decide when to set up the channel. Once the kind of channel to be used is fixed, the performance of the protocol only depends on the ability to create a state with the highest possible purity and to properly implement the rotations and measurements needed.

Having identified the relevant correlations and their symmetry as those that determine the performance of RSP, if one relaxes the hypothesis of a perfect channel, one may argue that the noisy channels that are optimal are not in general those that preserve entanglement or discord. On the contrary, they are those that preserve the amount of relevant correlations and the symmetry (isotropy) of the state.

5. Conclusions

In this paper we have introduced a new measure of correlations based on the average classical mutual information $\langle \mathcal{I} \rangle$ between the local von Neumann observables. We have illustrated our measure focusing on the case of two-qubit systems. To analyze its properties we have defined classes of maximally mixed marginal two-qubit states (MMMS) with different continuous symmetries. At fixed purity, the states belonging to each class have the same value of $\langle \mathcal{I} \rangle$, and their distributions of $\mathcal{I}(\hat{n}, \hat{m})$ among the various observables are isomorphic. At fixed purity, the states that give the minimum value of $\langle \mathcal{I} \rangle$ are isotropic states, while those that attain the maximum are those with a single non-zero singular value in their correlation tensor (the so-called 'classical states'). Any pair of local observables $(\hat{n}, \hat{m})$ defines a product basis $\mathcal{B}_{(\hat{n},\hat{m})}$, and we showed for MMMS that the higher the $\mathcal{I}(\hat{n}, \hat{m})$, the lower the coherence $\mathrm{Coh}_{\mathcal{B}_{(\hat{n},\hat{m})}}$ of the corresponding basis. In other words, the (average) correlations of MMMS and their (average) coherence are complementary resources: protocols that require the maximization of $\mathcal{I}(\hat{n}, \hat{m})$, correspondingly require a minimization of $\mathrm{Coh}_{\mathcal{B}_{(\hat{n},\hat{m})}}$. We conjecture that such a distinction may have a general character and that correlations and coherence may play a complementary role in the quantum information protocols, in the sense that some of them (or some parts of them) should be based on the maximal amount of correlations between the relevant observables, and they correspondingly require the least amount of coherence, while in contrast others should be based on the coherence properties of the relevant observables.

In the rest of the paper, we introduced a general standard scheme for identifying the proper measures of correlations for protocols whose figure-of-merit $\mathcal{F}(\hat{n}, \hat{m})$ explicitly depends on a given set Ω_{RO} of pairs of observables $(\hat{n}, \hat{m})$, i.e. the set of observables relevant for the protocol. The measure of correlations is obtained by defining a gain function $\mathcal{G}$ that expresses the benefit in using the correlations present in the state ρ_{AB} employed in the protocol versus not using them. This perspective has a series of consequences. Indeed, on the one hand the measure of correlations becomes protocol-dependent; on the other hand the described procedure allows one to derive 'proper' measures of correlations in a standard way for each protocol. Ultimately, the condition of being 'proper' stems from the explicit connection one is able to make between the measure of correlations and the figure-of-merit $\mathcal{F}$. Furthermore, we notice that when a state is sent through a noisy channel the overall properties of the state are, in general, corrupted, while depending on the specific kind of noise, the relevant correlations may well be preserved.

We illustrated our scheme by specializing it to an example of a quantum communication task—remote state preparation (RSP)—for which neither discord nor entanglement are able to capture the relevant features that allow the performance to be maximized. In the case of MMMS, we introduced a specific figure-of-merit $\mathcal{F}(\hat{n}, \hat{m})$, defined the set Ω_{RO} and showed that $\mathcal{G} = \mathcal{I}(\hat{n}, \hat{m})$ for $(\hat{n}, \hat{m}) \in \Omega_{\mathrm{RO}}$; therefore the measure of correlations pertaining to the

protocol is just $\langle\mathcal{G}\rangle_{\Omega_{RO}} = \langle\mathcal{I}(\hat{n},\hat{m})\rangle_{\Omega_{RO}}$, i.e. the average mutual information between the relevant observables. The resources involved in the process are the purity of the state and the symmetry of the correlations. We found that the extremal states are the isotropic ones: at fixed purity they allow the optimal value of $\langle\mathcal{F}\rangle_{\Omega_{RO}}$ to be obtained with the least amount of $\langle\mathcal{G}\rangle_{\Omega_{RO}}$, i.e. with the least amount of resources (correlations) used. We then extended our scheme to general (non-MMMS) two-qubit states. The definition of $\langle\mathcal{F}\rangle_{\Omega_{RO}}, \langle\mathcal{G}\rangle_{\Omega_{RO}}$ parallels that for MMMS, and it shows that the relevant observables and correlations are those pertaining to the state $\rho_{AB}(\vec{a} = \vec{b} = \vec{0})$, i.e. the MMMS obtained from ρ_{AB} by setting the local vectors $\vec{a}, \vec{b}$ to zero. One has that $\langle\mathcal{G}\rangle_{\Omega_{RO}}$ is a function of $\langle\mathcal{I}(\hat{n},\hat{m})\rangle_{\Omega_{RO}}^{\vec{a}=\vec{b}=\vec{0}}$, i.e. the average mutual correlation between the relevant observables evaluated for the state $\rho_{AB}(\vec{a} = \vec{b} = \vec{0})$. Therefore, $\langle\mathcal{I}(\hat{n},\hat{m})\rangle_{\Omega_{RO}}^{\vec{a}=\vec{b}=\vec{0}}$ is the desired measure of correlations. Furthermore, for non-MMMS the study of $\mathcal{F}$ allows one to identify among the relevant observables the set of those that are indeed useful $\Omega_U \subset \Omega_{RO}$, and correspondingly to define the $\langle\mathcal{F}\rangle_{\Omega_U}, \langle\mathcal{G}\rangle_{\Omega_U}$. We have shown how to use our approach to devise an optimized protocol that attains better values of $\mathcal{F}$ on average in a given range of parameters defining the state ρ_{AB}. Our treatment of RSP allows a proper measure of correlations that applies to all states to be found, identifying classes of states that have the same performance and discriminating those classes that allow the best performance to be obtained at fixed purity. The optimality of isotropic states has a general character: the average performance $\langle\mathcal{F}\rangle_{\Omega_U}$ of the protocol is determined by the purity of the state and by the way (symmetry) in which the useful correlations are distributed.

The idea of analyzing and classifying correlations in terms of classical mutual information, its average over observables and its symmetries does not depend on the structure of the set of two-qubit states or observables. As such, one could extend it to the cases of two-qudit systems or to the case in which POVMs [36, 37] are considered, with the aim of providing insights into the general structure of quantum correlations [34]. As for the task of applying our scheme to derive protocol-dependent measures of correlations, in general one should first try to pick out the relevant observables involved in the protocol, and to relate the presence (absence) of a given symmetry in the used initial state to the presence (absence) of the relevant correlations. The extension to other protocols may prove difficult in general, and in this case one may also need to enlarge the set of measurements allowed for general POVMs (generalized observables) [35]. Possible ways to achieve such generalizations could, in principle, take advantage of the representation of the states involved in terms of their generalized Bloch vectors [38]. Moreover, one could resort to classifications of the symmetries of the states, such as those given by the local unitary stabilizer formalism [29], and start to apply our scheme to simple classes of states with continuous symmetries. We leave such generalizations for future research.

Acknowledgments

Appendix A

Given each of the directions $\hat{d} \in \mathcal{LU}_{\hat{c}}^{\text{eq}}$, there is always a unique transformation that maps $\hat{c}$ into $\hat{d}$. These transformations can be seen as orthogonal transformations in the $\mathbb{R}^3$ space of the correlation vectors. They thus form a discrete subgroup of $O(3)$ that is isomorphic to $G \sim S_3 \otimes E_8$, where S_3 is the symmetric group of order three, corresponding to the permutations of three indices, and E_8 is the elementary Abelian group of order eight that realizes the changes of signs s_i in equation (2). This group can also be written as $G \sim S_4 \otimes Z_2$, where S_4 is the symmetric group of order four and Z_2 is the cyclic group of order two. The role of the two tensor factors S_4 and Z_2 is best explained by considering the action of G in the Hilbert space. In the Hilbert space representation, the transformations of G can be implemented by a combination of local unitary rotations and local spin-flips acting on the two-qubit state. In particular, we have $O_A = S_A \tilde{O}_A$ and $O_B = S_B \tilde{O}_B$, where $\tilde{O}_A, \tilde{O}_B \in SO(3)$ and $S_A, S_B \in \{\mathbb{I}_3, -\mathbb{I}_3\}$. The local change of coordinates corresponding to $\tilde{O}_A, \tilde{O}_B$ can always be implemented by means of the local unitary operations $U_A \otimes U_B$ acting on the state. Indeed, it is well known [15] that for any unitary transformation $U \in SU(2)$ there exists a (unique) rotation $\tilde{O} \in SO(3)$ such that $U\hat{n} \cdot \vec{\sigma} U^\dagger = (\tilde{O}\hat{n}) \cdot \vec{\sigma}$. Transformations corresponding to $\tilde{O}_A, \tilde{O}_B$ cannot change $\det(E) = c_1 c_2 c_3$; therefore, acting on $\text{diag}(c_1, c_2, c_3)$ they result in permutations of the $c_i's$ and changes of signs of either zero or two s_i. These transformations form the subgroup S_4 of G, that can also be interpreted as the symmetry group of the tetrahedron $\mathcal{T}$, i.e. the group of permutations of the vertices of $\mathcal{T}$. The other tensor factor group can be realized as $Z_2 = \{\mathbb{I}_3, -\mathbb{I}_3\}$, where the element $-\mathbb{I}_3$ realizes the inversion $\hat{c} \to -\hat{c}$. The operation represented by the matrix $-\mathbb{I}_3$ realizes a reflection of one of the two Bloch spheres of the qubit around the origin, i.e. a local spin-flip of one of the qubits. The spin-flip cannot be implemented with a unitary operation: in fact, it is an anti-unitary operation [28]. If for a given κ the vector $\vec{c} = \kappa\hat{c}$ is admissible (i.e. together with $\vec{a}, \vec{b}$ it yields a positive state, then all transformations in S_4, which can be realized as local unitaries, yield the admissible vectors $\vec{d} = \kappa\hat{d}$. However, the spin-flip $-\mathbb{I}$ is a positive-but-not-completely-positive operation, and as such it can map entangled states into non-positive states. Thus, it may map an admissible $\vec{c}$ into a non-admissible $\vec{d}$. As proved in [15], the spin-flip is a positive only state such that $\vec{c} \in \mathcal{T} \cap -\mathcal{T}$.

Appendix B

Proof of proposition 1. Since we do not have a general analytical formula for $\langle \mathcal{I} \rangle_{(\hat{n},\hat{m})} (\hat{c})$, we analyze $\left\langle \partial_\alpha \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m}) \right\rangle$ and $\left\langle \hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m}) \right\rangle$ with $\hat{\partial}_\beta = \partial_\beta / \sin\alpha$, i.e. we analyze the gradient of $\langle \mathcal{I} \rangle_{\hat{n}} (\hat{m})$ in spherical coordinates, where $\hat{c} = (\sin\alpha\cos\beta, \sin\alpha\sin\beta, \cos\beta)$. One has that

$$\hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m}) = \kappa^2 \left(m_2^2 - m_1^2\right) \sin\alpha \sin\beta \partial_R \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m})$$

and that $\partial_R \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m})$ is a positive $\forall R$. Therefore, the critical values for $\langle \mathcal{I} \rangle_{(\hat{n},\hat{m})} (\hat{c})$ are those given by $\partial_\alpha R = \partial_\beta R / \sin\alpha = 0$ in the first place. It turns out that for $\hat{c} \in \{\pm\hat{x}, \pm\hat{y}, \pm\hat{z}\}$, i.e. the $\rho_{2\text{iso}}^0$ state, both derivatives are zero and such is their average over $\hat{m}$. Furthermore, if one evaluates the derivatives in correspondence with the isotropic states, i.e. $\rho_{3\text{iso}}$, one has that $\partial_R \langle \mathcal{I} \rangle_{\hat{n}} (\hat{m})$ is constant with $\hat{m}$ and $\langle \partial_\alpha R \rangle = \left\langle -\sqrt{2}\kappa^2(m_1^2 + m_2^2 - 2m_3^2)/3 \right\rangle = 0$ and $\left\langle \hat{\partial}_\beta R \right\rangle = \left\langle \kappa^2(m_2^2 - m_1^2) \right\rangle = 0$. The evaluation of the average of the Hessian matrix shows that

isotropic states attain a minimum, and states with single $c_i \neq 0$ a maximum. The $\rho^0_{2\text{iso}}$ and $\rho_{3\text{iso}}$ states constitute the only extremal point for $\langle \mathcal{I} \rangle_{(\hat{n},\hat{m})}(\hat{c})$ and therefore they constitute global maxima and minima. Indeed, the only other critical points are given by the two equal states c_i and the remaining $c_j = 0$, i.e. the class of states $\rho^\epsilon_{2\text{iso}}$ with $\epsilon = 1/\sqrt{2}$. In order to show that these are the only other critical points we focus on the states with $\alpha = \pi/2, \beta = \pi/4 + j\pi, j \in \mathbb{Z}$, since the symmetry allows the results to be extended to the other elements of the class $\rho^\epsilon_{2\text{iso}}$. For the proof, it is first sufficient to show that when $\hat{c} \notin \{\pm\hat{x}, \pm\hat{y}, \pm\hat{z}\}$ and for non-isotropic states $\hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m})$ has a constant sign for all $\hat{m}$, and therefore $\left\langle \hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m}) \right\rangle$ cannot be zero, except for the $\rho^{1/\sqrt{2}}_{2\text{iso}}$ states. To this end we express $\hat{m} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$; at fixed $\hat{c}$, one has that

$$\sin\theta\hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m})\mathrm{d}\theta\mathrm{d}\phi \propto -\sin^3\theta\cos(2\phi)\, \partial_R \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m})\mathrm{d}\theta\mathrm{d}\phi$$

and therefore the integrand has a constant sign in the integration over θ. Furthermore, both $\cos(2\phi)$ and $\partial_R \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m}) \doteq \mathcal{I}^R(\phi)$ has period π as a function of ϕ. The integration for $\phi \in [0, \pi]$ can be replaced by twice the integration for $\phi \in [-\pi/4, 3\pi/4]$ and one can show that

$$\int_{-\pi/4}^{3\pi/4} \cos(2\phi)\, \mathcal{I}^R(\phi) = \int_{-\pi/4}^{\pi/4} \cos(2\phi)\left(\mathcal{I}^R(\phi) - \mathcal{I}^R(\phi - \pi/2)\right).$$

Since for $\phi \in [-\pi/4, \pi/4]$ the difference $\mathcal{I}^R(\phi) - \mathcal{I}^R(\phi - \pi/2)$ has a constant sign (that depends on the sign of $c_1^2 - c_2^2$. Therefore, $\hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m})$ has a constant sign on the domain of the integration and $\left\langle \hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m}) \right\rangle \neq 0$. The only points at which $\left\langle \hat{\partial}_\beta \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m}) \right\rangle = 0$ is when $c_1^2 - c_2^2 = 0$, i.e. $\beta = \pi/4$. Upon evaluating $\left\langle \partial_\alpha \langle \mathcal{I} \rangle_{\hat{n}}(\hat{m}) \right\rangle$ one finds that it is zero, iff $\alpha = \pi/2$. By studying the relative average of the Hessian, one sees that these points are saddle points. By permutation of the coordinate axes and symmetry arguments, one can extend the result to the whole set of states $\rho^{1/\sqrt{2}}_{2\text{iso}}$. Since the above arguments are independent on κ, therefore, when $\kappa > 1$ the domain of $\hat{c}$ shrinks, since some of the directions define a non-positive state, and while the minima of $\langle \mathcal{I} \rangle_{(\hat{n},\hat{m})}(\hat{c})$ remains in correspondence with the $\rho_{3\text{iso}}$ states, the maxima are found at the borders of the domain, i.e. at the intersection between the sphere of radius κ and the tetrahedron $\mathcal{T}$. $\qquad\square$

Appendix C

Proof of proposition 6.   In order to prove the extremality of $\rho^0_{2\text{iso}}$ and $\rho_{3\text{iso}}$ for both $\langle \mathcal{F} \rangle_{\Omega_{\text{RO}}}$ and $\langle \mathcal{G} \rangle_{\Omega_{\text{RO}}}$ we use the same arguments used in appendix B to prove proposition 1. Indeed, one can see that since both $\mathcal{F}$ and $\mathcal{G}$ are monotonically dependent on $|E\hat{n}|$, (i) they are monotonically dependent on κ, and (ii) since we do not have an analytical formula for general $\hat{c}$, we find the critical points by analyzing $\langle \partial_\alpha(R) \rangle = \langle \partial_\beta(R)/\sin\alpha \rangle = 0$, now with $R = |E\hat{n}|^2 = (c_1^2 n_1^2 + c_2^2 n_2^2 + c_3^2 n_3^2)$. Just as in appendix B, we find that both $\partial_R \mathcal{F}$ and $\partial_R \mathcal{G}$ are monotonic functions of R, and therefore the proof goes along the same line as appendix B. $\qquad\square$

Appendix D

Proof. Property (i) immediately follows from the following facts: if $\kappa < \kappa'$ and $\Omega^U_{\kappa,b} \subset \Omega^U_{\kappa',b}$, $\mathcal{F}^U$ for $(\hat{n}, \hat{n}^E) \in \Omega^U_{\kappa,b} \cap \Omega^U_{\kappa',b}$ decreases; $\mathcal{F}^U < \mathcal{F}^{UN}$ for $(\hat{n}, \hat{n}^E) \in \Omega^U_{\kappa',b} \backslash \Omega^U_{\kappa,b}$. Property (ii) follows from the following facts: for all transformations O_A, O_B that map $\hat{c} \to \hat{d}$ with $\hat{c}, \hat{d} \in \mathcal{LU}^{eq}_{\hat{c}}$, the sets $\Omega^U_{\kappa,b}, \Omega^{UN}_{\kappa,b}$ are mapped into the sets $\Omega^U_{\kappa,b'}, \Omega^{UN}_{\kappa,b'}$, where $\vec{b'} = O_B\vec{b}$; the result follows from the fact that such transformations leave the Haar measure invariant.

$\square$

References

[1] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Mod. Phys.* **81** 865
[2] Werner R F 1989 *Phys. Rev.* A **40** 4277
[3] Jozsa R and Linden N 2003 *Proc. R. Soc.* A **459** 2036
[4] Bennett C H *et al* 1993 *Phys. Rev. Lett.* **70** 1895
[5] Horodecki M and Piani M 2012 *J. Phys. A: Math. Theor.* **45** 105306
[6] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[7] Giovannetti V, Lloyd S and Maccone L 2003 *Science* **306** 1330
[8] Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 *Rev. Mod. Phys.* **84** 1655
[9] Ollivier H and Zurek W H 2001 *Phys. Rev. Lett.* **88** 017901
[10] Henderson L and Vedral V 2001 *J. Phys. A: Math. Gen.* **34** 6899
[11] Datta A, Shaji A and Caves C M 2008 *Phys. Rev. Lett.* **100** 050502
[12] Pirandola S 2014 *Sci. Rep.* **4** 6956
[13] Gu M *et al* 2012 *Nat. Phys.* **8** 671
[14] Vedral V 2010 *Found. Phys.* **40** 1141
[15] Horodecki R and Horodecki M 1996 *Phys. Rev.* A **54** 1838
[16] Peres A 1995 *Quantum Theory: Concepts and Methods* (New York: Springer) (https://doi.org/10.1007/0-306-47120-5)
[17] Griffiths R B 2003 *Consistent Quantum Theory* (Cambridge: Cambridge University Press) (https://doi.org/10.1017/CBO9780511606052)
[18] Omnes R 1992 *Rev. Mod. Phys.* **64** 339
[19] Paulraj A, Nabar R and Gore D 2003 *Introduction to Space-time Wireless Communications* (Cambridge: Cambridge University Press)
[20] Pati A K 2001 *Phys. Rev.* A **63** 014302
[21] Bennett C H, DiVincenzo D P, Shor P W, Smolin J A, Terhal B M and Wootters W K 2001 *Phys. Rev. Lett.* **87** 077902
   Bennett C H, DiVincenzo D P, Shor P W, Smolin J A, Terhal B M and Wootters W K 2002 *Phys. Rev. Lett.* **88** 099902
[22] Bennett C H, Hayden P, Leung D W, Shor P W and Winter A 2005 *IEEE Trans. Inf. Theory* **51** 56
[23] Ye M Y, Zhang Y S and Guo G C 2004 *Phys. Rev.* A **69** 022310
[24] Dakić B *et al* 2012 *Nat. Phys.* **8** 666
[25] Giorgi G L 2013 *Phys. Rev.* A **88** 022315
[26] Horodecki P, Tuziemski J, Mazurek P and Horodecki R 2014 *Phys. Rev. Lett.* **112** 140507
[27] Tran M C, Dakic B, Arnault F, Laskowski W and Paterek T 2015 *Phys. Rev.* A **92** 050301
   Tran M C, Dakic B, Laskowski W and Paterek T 2016 *Phys. Rev.* A **94** 042302
[28] Buzek V, Hillery M and Werner R F 1999 *Phys. Rev.* A **60** 2626
[29] Lyons D W and Walck S N 2012 *Phys. Rev.* A **84** 042340
[30] Baumgratz T, Cramer M and Plenio M B 2014 *Phys. Rev. Lett.* **113** 140401
[31] Chaves R and de Melo F 2011 *Phys. Rev.* A **84** 022324
[32] Allegra M, Giorda P and Lloyd S 2016 *Phys. Rev.* A **93** 042312
[33] Giorda P and Allegra M 2016 arXiv:1611.02519
[34] Maccone L, Bruss D and Macchiavello C 2015 *Phys. Rev. Lett.* **114** 130401
[35] Mor T and Horodecki P 1999 arXiv:quant-ph/9906039
[36] D'Ariano G M, Lo Presti P and Perinotti P 2005 *J. Phys. A: Math. Gen.* **38** 5979
[37] Dall'Arno M, D'Ariano G M and Sacchi G F 2011 *Phys. Rev.* A **83** 062304
[38] Bertlmann R A and Krammer P 2008 *J. Phys. A: Math. Theor.* **41** 235303