

# Private Quantum Decoupling and Secure Disposal of Information

**Francesco Buscemi**

Institute for Advanced Research, Nagoya University, Japan

E-mail: [buscemi@iar.nagoya-u.ac.jp](mailto:buscemi@iar.nagoya-u.ac.jp)

**Abstract.**

Given a bipartite system, correlations between its subsystems can be understood as information that each one carries about the other. In order to give a model-independent description of secure information disposal, we propose the paradigm of *private quantum decoupling*, corresponding to locally reducing correlations in a given bipartite quantum state without transferring them to the environment. In this framework, the concept of *private local randomness* naturally arises as a resource, and total correlations get divided into eliminable and ineliminable ones. We prove upper and lower bounds on the amount of ineliminable correlations present in an arbitrary bipartite state, and show that, in tripartite pure states, ineliminable correlations satisfy a monogamy constraint, making apparent their quantum nature. A relation with entanglement theory is provided by showing that ineliminable correlations constitute an entanglement parameter. In the limit of infinitely many copies of the initial state provided, we compute the regularized ineliminable correlations to be measured by the coherent information, which is thus equipped with a new operational interpretation. In particular, our results imply that two subsystems can be privately decoupled if their joint state is separable.

## 1. Introduction

Let us suppose we are given a medium containing sensitive information which, for some reason, we want to dispose of in a secure way, i. e. in such a way that neither we nor anyone else can have access to—or be deemed to possess—that information anymore. In many everyday situations, particular precautions have to be taken in advance in order to counter unwanted *data remanence*, i. e. the persistence of data that were nominally erased or removed.

When dealing with macroscopic objects, the irreversibility of dissipative processes is generally enough to provide a *practically secure* erasure of data (think of e. g. shredding the medium). However, such a conclusion is *in-principle* completely inadequate. Let us suppose in fact that the medium carrying the information is represented by the state of a microscopic object obeying the laws of Quantum Mechanics. Since quantum evolutions are globally reversible, also information has to be globally preserved, and any sort of *true* information erasure is thus forbidden [1]. Even so, information could be, if not erased, *hidden* or encoded in such a way to achieve what a secure disposal of information is meant to achieve. Our aim here is to introduce and analyze a model-independent paradigm of secure information disposal, suitable to describe both classical and quantum information disposal, and naturally encompassing the ideal situation in which the only limitations to data processing are those imposed by the laws of Quantum Mechanics.

In order to do so, let us consider the following protocol: let  $\varrho_{RA}$  denote the initial bipartite state shared between two parties—the active player (or *receiver*)  $A$  and the passive and inaccessible reference system (or *remote sender*)  $R$ . According to a common understanding, the amount of correlations existing in  $\varrho_{RA}$  between subsystems  $A$  and  $R$  can be interpreted as the amount of information that  $A$  carries or possesses *about*  $R$ . Since the content of the message is assumed to be private (otherwise there is no reason to require security in its disposal), we suppose that the state  $\varrho_{RA}$  is decoupled from other accessible quantum systems, in particular from the local environment—i. e. the ‘trash’ system—of  $A$ . The goal for  $A$  is to securely dispose of the information she has about  $R$ . By identifying information with correlations, this means that she has to reduce her correlations with  $R$  by applying local operations on her share only (as  $R$  is not accessible), *and* without transferring any of these correlations into her local environment (as this is assumed to be accessible to adversaries). We name this protocol (*local*) *private quantum decoupling* (PQD).

PQD constitutes a novel instance of the general task of producing, under various constraints, an uncorrelated (or, equivalently, ‘factorized’) state out of a correlated one. The importance of studying decoupling protocols lies in the fact that, with appropriate constraints, it is possible to quantitatively characterize diverse properties of quantum correlations with respect to their robustness *against* decoupling. Such an approach has been introduced independently in Refs. [2] and [3], and contributed in recognizing the central role that decoupling plays in quantum information processing: for example, the primitives of state merging [11], state redistribution [12], and the ‘mother’ protocol [13], are all based on decoupling arguments, and decoupling procedures form the building blocks of many recently constructed coding theorems achieving quantum capacity [14, 15]. Hence, PQD offers a new point of view on the study of quantum correlations, with possible implications in entanglement theory and quantum cryptography.

The structure of the paper is as follows: in Section 2, previous approaches

to quantum decoupling are described and the new paradigm of PQD is motivated through simple examples. The rigorous definition of PQD is given in Section 3 by defining eliminable and ineliminable correlations, and the concept of private local randomness as a resource is introduced. In Section 4 we prove general bounds on PQD when acting on an arbitrary mixed state, and show that ineliminable correlations are in fact monogamous correlations, in the sense that they cannot be freely shared. This is a feature common to many distinctively quantum correlations, like e. g. entanglement (when suitably measured). Section 5 deals with the asymptotic limit where infinitely many identical and independent copies of a given state are available: in this case, the optimal rate for PQD is explicitly calculated as being expressed by the coherent information. In Section 6 we discuss some examples for which PQD assumes a particularly simple form. A connection between PQD and random-unitary channels is exhibited, together with an open question concerning the latter. Finally, Section 7 describes the relations existing between ineliminable correlations, quantum entanglement, and other ‘quantum’ correlations present in an arbitrary bipartite quantum state. Here we show that ineliminable correlations represent an entanglement parameter, in the sense given by [27]. Section 8 concludes the paper with a brief summary of the results obtained and possible directions to investigate in future.

### 1.1. Notation and basic concepts

All quantum systems considered in the following are finite dimensional, in the sense that their attached Hilbert spaces  $\mathcal{H}$  are finite dimensional. We use Greek letters like  $\psi, \Psi, \dots$  for pure quantum states, while letters like  $\varrho, \varsigma, \tau, \dots$  are reserved for mixed states. The usual ket-bra notation  $|\psi\rangle\langle\psi|$  denoting the rank-one projector onto the state  $|\psi\rangle$  is generally abbreviated simply as  $\psi$ . Roman letters label the systems sharing a quantum state: for example,  $\varrho_{RA}$  is a mixed state defined on the composite system  $RA$ , carrying the Hilbert space  $\mathcal{H}_R \otimes \mathcal{H}_A$ . Where no confusion arises (or it is not differently specified), omission of a letter in the label indicates a partial trace, namely,  $\varrho_A := \text{Tr}_R[\varrho_{RA}]$ .

In classical information theory, given two random variables  $\mathbf{X}$  and  $\mathbf{Y}$  distributed according to a joint probability distribution  $p(x, y)$ , the *mutual information*  $I(\mathbf{X} : \mathbf{Y}) := H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{XY})$ , where  $H(\mathbf{X}) := -\sum_x p(x) \log_2 p(x)$  is the Shannon entropy, is known to measure both the degree of correlation existing between  $\mathbf{X}$  and  $\mathbf{Y}$  †, as well as “the reduction in the uncertainty of  $\mathbf{X}$  due to the knowledge of  $\mathbf{Y}$ ” (see Ref. [16] p.20). We hence say that  $\mathbf{Y}$  carries a total of  $I(\mathbf{X} : \mathbf{Y})$  bits of information about  $\mathbf{X}$ .

The classical arguments given above can be straightforwardly generalized to the quantum case as follows. According to Refs. [2, 3], given a bipartite quantum state  $\varrho_{RA}$ , the *quantum mutual information* (QMI) [4] defined as  $I^{R:A}(\varrho_{RA}) := S(\varrho_R) + S(\varrho_A) - S(\varrho_{RA})$ , where  $S(\sigma) := -\text{Tr}\sigma \log_2 \sigma$  is the von Neumann entropy of a state  $\sigma$  and  $\varrho_{R(A)} := \text{Tr}_{A(R)}[\varrho_{RA}]$ , provides a sound and operationally meaningful measure of the total amount of correlations present in  $\varrho_{RA}$  ‡. It is known that  $I^{R:A}(\varrho_{RA}) = 0$  if and only if  $\varrho_{RA} = \varrho_R \otimes \varrho_A$ , while  $I^{R:A}(\varrho_{RA}) = 2S(\varrho_R)$  if and only if  $\varrho_R$  is purified by  $A$ . Moreover, when systems  $R$  and  $A$  are classical, QMI coincides with its classical counterpart. It makes sense then to say that the system  $A$

† Since  $I(\mathbf{X} : \mathbf{Y}) = 0$  iff  $p(x, y) = p(x)p(y)$  and  $I(\mathbf{X} : \mathbf{Y}) = H(\mathbf{X})$  iff  $p(x, y) = p(y)\delta(x, f(y))$ , namely,  $\mathbf{X}$  is a function of  $\mathbf{Y}$ . See Ref. [16].

‡ This means that also correlations, as information, are measured here in (quantum) bits.

carries a total of  $I^{R:A}(\varrho_{RA})$  (quantum) bits of information about  $R$ . Notice that the information content, as we defined it, turns out to be positive and symmetric, that is, the amount of information  $A$  carries about  $R$  equals the amount of information  $R$  carries about  $A$ , since  $I^{R:A}(\varrho_{RA}) = I^{A:R}(\varrho_{RA})$ . When the state  $\varrho_{RA}$  is clear from the context, we will simply write  $I(R:A)$  to indicate  $I^{R:A}(\varrho_{RA})$ , and, in case the state is multipartite like, for example,  $\varsigma_{RBE}$ , we will denote  $I^{R:B}(\text{Tr}_E[\varsigma_{RBE}])$  simply by  $I^{R:B}(\varsigma_{RBE})$  or even by  $I(R:B)$ .

We finally recall here also the notion of *coherent information* [5] which is well-known in the literature to play a fundamental role in entanglement theory and quantum Shannon theory and is defined as  $I_c^{A \rightarrow R}(\varrho_{RA}) := S(\varrho_R) - S(\varrho_{RA})$ . Contrarily to QMI, coherent information can be negative and it is not symmetric as there is a preferred directionality in its definition.

## 2. Quantum decoupling: previous definitions and new motivations

Suppose two players, Alice ( $A$ ) and a Referee ( $R$ ), share a bipartite quantum state  $\varrho_{RA}$ . We say that they are *decoupled* if and only if  $\varrho_{RA} = \varrho_R \otimes \varrho_A$ . If the initial state is not decoupled, a decoupling procedure aims at transforming the initial state  $\varrho_{RA}$  into (something close to) a factorized state. It is clear that, without imposing any constraint on the decoupling procedure, the whole task is trivial: one can always *prepare*, even *locally*, an exactly decoupled state after having discharged the input into the environment. If we want to probe some property of quantum correlations using decoupling, the main point is then to choose appropriate constraints making the best decoupling strategy non-trivial. In the following, before presenting our decoupling task, we will review two different types of decoupling tasks adopted in the literature.

A first decoupling task is introduced through information-theoretical arguments. Refs. [2, 3], with analogous though inequivalent arguments, prove that quantum mutual information  $I^{R:A}(\varrho_{RA})$  provides an *operational* measure of total (both classical and quantum) correlations shared between  $A$  and  $B$ , in that  $I^{R:A}(\varrho_{RA})$  quantifies the cost of erasing initial correlations. In particular, the decoupling protocol adopted in Ref. [2] is related with the theory of *private quantum channels* [6] and aims at constructing a local map  $A \rightarrow B$  of the form

$$\mathcal{D} : \sigma \mapsto \frac{1}{N} \sum_{i=1}^N U_i \sigma U_i^\dagger, \quad (1)$$

such that  $(\text{id}_R \otimes \mathcal{D}_A)(\varrho_{RA})$  is close to some factorized state  $\varrho_R \otimes \omega_B$ . The additional requirement posed in [2] is to use in (1) the smallest possible number  $N$  of unitary operators (indeed, the average over the whole special unitary group  $\mathbb{S}\mathbb{U}(d)$  achieves perfect decoupling, but it requires an infinite amount of randomness to be added). Clearly, the number  $N$  can in general depend both on the input state  $\varrho_{RA}$  and on the degree of approximation required of the decoupling. Ref. [2] proves that, in the i.i.d. asymptotic limit, exact decoupling can be achieved for values of  $N$  as small as  $2^{nI(R:A)}$ , where  $n$  is the (large) number of copies of  $\varrho_{RA}$  provided. Following Landauer's principle, quantum mutual information is then interpreted as the total amount of correlations *per copy*, being the minimum cost (measured in bits of extra-randomness borrowed from a randomness reservoir) needed in the i.i.d. limit to achieve exact decoupling. A similar, though not equivalent, conclusion can be drawn as a special case of the general setting introduced in Ref. [3], where a class of transformations

different from (1) is considered (in particular, classical communication between the two parties is taken into account in an essential way). Ref. [3] interprets quantum mutual information as a particular type of *quantum deficit*, being the minimum cost, measured in bits of entropy production, required by a decoupling process consisting of local unitaries and local orthogonal measurements only.

A second, quite different, definition of decoupling task is adopted in Ref. [7]: here the input state  $\varrho_{RA}$  is drawn from a non-trivial set of possible input states (constructed as the orbit of different seed states under the action of a unitary representation of a group), while the decoupling map can act *globally* and is required to achieve exact decoupling *always* (there is no approximation here). It is then shown that some seed states induce orbits for which the optimal decoupling map cannot be different from the completely depolarizing channel which transforms every state into the maximally mixed one. Correspondingly, such correlations are called *unerasable*, as opposed to *erasable* correlations, which are those that can be decoupled by a non-trivial map. Such a distinction hence arises as an algebraic/geometrical property of the set of quantum states analyzed, depending on the seed state and the group acting on it.

The decoupling task we propose here is independent of both previously mentioned approaches. In fact, as anticipated in the Introduction, when performing PQD, we monitor not only the decrease of correlations between  $R$  and  $A$ , but also the corresponding *increase* of correlations between  $R$  and the environment (causing the decoupling ||). In fact, it is not difficult to see that the group-averaging channel  $A \rightarrow B$  of the form

$$\mathcal{R} : \sigma \mapsto \int_{\text{SU}(d)} dg U_g \sigma U_g^\dagger = \frac{\mathbb{1}}{d}, \quad \forall \sigma, \quad (2)$$

of which Eq. (1) aims at being a faithful approximation, when applied on  $A$ , does not *truly destroy* correlations between  $A$  and  $R$ , but simply *transfers* them to the environment, so that  $R$  is no more correlated with  $A$ , but is correlated with the environment. This can be explicitly seen by writing the Stinespring purification [17] of the channel  $\mathcal{R}_A$  as an (essentially uniquely defined) isometry  $V_A : A \rightarrow BE_1E_2$ , with  $V_A^\dagger V_A = \mathbb{1}_A$ , acting as

$$V_A |\psi_A\rangle = |\Psi_{BE_1}^+\rangle \otimes |\psi_{E_2}\rangle, \quad \forall \psi, \quad (3)$$

where  $\Psi^+$  is a maximally entangled state. One can check that indeed it holds

$$\mathcal{R}(\sigma_A) = \text{Tr}_{E_1E_2}[V_A \sigma_A V_A^\dagger], \quad \forall \sigma. \quad (4)$$

On the other hand,

$$\text{Tr}_B[V_A \sigma_A V_A^\dagger] = \frac{\mathbb{1}_{E_1}}{d} \otimes \sigma_{E_2}, \quad \forall \sigma. \quad (5)$$

In other words, the induced channel  $A \rightarrow E_2$  is *noiseless*: all correlations initially shared with  $R$  are now *perfectly* transferred to the environment subsystem  $E_2$ . (In fact, the same phenomenon happens with all channels preparing some fixed state regardless of the input.) We conclude that the approach adopted in Ref. [2] constitutes the opposite of what we want to achieve with PQD: in defining the latter, in fact, we will impose an upper bound on the amount of correlations transferred into the environment as a consequence of the decoupling process.

|| It should be clear that non-trivial decoupling processes are possible only in presence of an environment interacting with the system. A closed evolution, in fact, does not induce any change in the correlations.

At this point, the natural question arises—is the constraint we are going to impose well balanced? In other words, does it induce some non-trivial situations where we can truly eliminate correlations, without merely ‘jettisoning’ them into the environment, and some non-trivial situations where we cannot? As a first motivating example, let us consider the extreme case where the initial shared state is a pure state  $|\Psi_{RA}\rangle$ . Again, due to Stinespring’s theorem [17], whatever deterministic transformation Alice could engineer can always be represented by an isometry  $V_A : A \rightarrow BE$ , with  $V_A^\dagger V_A = \mathbb{1}_A$ , the share  $B$  being Alice’s output, the share  $E$  being the environment. In other words, the initial bipartite pure state  $|\Psi_{RA}\rangle$  gets transformed into the tripartite pure state

$$|\Phi_{RBE}\rangle := (\mathbb{1}_R \otimes V_A)|\Psi_{RA}\rangle. \quad (6)$$

Thanks to the identity [8]

$$I^{X:Y}(\psi_{XYZ}) + I^{X:Z}(\psi_{XYZ}) = 2S^X(\psi_{XYZ}), \quad (7)$$

where  $\psi_{XYZ}$  is a tripartite pure state, we see that

$$I^{R:B}(\Phi_{RBE}) + I^{R:E}(\Phi_{RBE}) = 2S^R(\Phi_{RBE}) \quad (8)$$

$$= I^{R:A}(\Psi_{RA}), \quad (9)$$

that shows that, if the initial state is pure, total correlations cannot be eliminated but only moved from one system to another: pure state correlations constitute a *conserved quantity*.

As a second motivating example, for which correlations are instead truly eliminable, let us consider the classically  $A \rightarrow B$  correlated state [3]

$$\varrho_{RA} = \sum_i p_i \varrho_R^i \otimes |i\rangle\langle i|_A, \quad (10)$$

where vectors  $|i\rangle$ ’s are orthonormal. Then, by applying on  $A$  the Stinespring’s isometry

$$M_A := \sum_i |e_B^i\rangle\langle e_A^i| \otimes |e_E^i\rangle, \quad (11)$$

where  $B \cong E \cong A$  ( $\dim \mathcal{H}_A = d$ ) and the vectors  $|e^i\rangle$ ’s are orthonormal vectors such that  $|\langle e^i|j\rangle|^2 = 1/d$  for all  $i, j$ , the resulting tripartite output state

$$\varsigma_{RBE} := (\mathbb{1}_R \otimes M_A)\varrho_{RA}(\mathbb{1}_R \otimes M_A^\dagger) \quad (12)$$

satisfies

$$\varsigma_{RB(E)} = \varrho_R \otimes \frac{\mathbb{1}_{B(E)}}{d}. \quad (13)$$

In other words, by applying  $M_A$ , we obtained perfect decoupling between  $B$  and  $R$  (since the state  $\varsigma_{RB}$  is factorized), however without correlating  $R$  with  $E$  (since also the state  $\varsigma_{RE}$  is factorized). In this case, we say that the initial correlations in  $\varrho_{RA}$  have been *perfectly eliminated*.

In the rest of the paper we will study what happens when initial correlations belong to a general bipartite quantum state. The general situation will turn out to lie in between the two preceding examples, in the sense that we will be able to divide total correlations into those which are *eliminable* and those which are *ineliminable*, the latter representing some sort of conserved quantity behaving like the correlations present in pure bipartite states.

### 3. Private quantum decoupling: mathematical definition

#### 3.1. Ineliminable correlations

According to the fact that in our scenario  $R$  acts as the passive reference system with respect to which information is measured, the goal of approximate PQD is to minimize correlations with  $R$  by acting with a channel (i. e. with a completely positive, trace-preserving map) only on subsystem  $A$  of  $\varrho_{RA}$ , in such a way that the amount of correlations transferred to the environment during the decoupling process is upper bounded by a privacy parameter  $\varepsilon \geq 0$ . We call this task  $\varepsilon$ -PQD. The appropriate tool to analyze such a task is provided by the Stinespring dilation of a channel [17]: given an input Hilbert space  $\mathcal{H}_A$  (of finite dimension  $d_A$ ), a channel  $\mathcal{D}$ , and an output Hilbert space  $\mathcal{H}_B$  (of finite dimension  $d_B$ ), there always exists a finite dimensional auxiliary Hilbert space  $\mathcal{H}_E$  (of dimension  $d_E \leq d_A d_B$ ) and an isometry  $V_{\mathcal{D}} : \mathcal{H}_A \mapsto \mathcal{H}_B \otimes \mathcal{H}_E$ ,  $V_{\mathcal{D}}^\dagger V_{\mathcal{D}} = \mathbb{1}_A$ , such that  $\mathcal{D}(\sigma) = \text{Tr}_E[V_{\mathcal{D}}\sigma V_{\mathcal{D}}^\dagger]$ , for all states  $\sigma$  on  $\mathcal{H}_A$ . Such an isometric extension  $V_{\mathcal{D}}$  is unique up to local unitary transformations on  $\mathcal{H}_E$ , which represents the environment interacting with the system during the open evolution described by  $\mathcal{D}$ . Before proceeding we shall notice that since everything here is finite-dimensional, minima and maxima appearing in the following are all achievable.

In practise,  $A$  applies the isometry  $V_{\mathcal{D}}$  on her share, keeps the  $B$  part and discards  $E$ . Accordingly,  $\varepsilon$ -PQD is mathematically characterized by the following quantity:

$$\Xi_A(\varrho_{RA}; \varepsilon) := \min_{V_A \in \mathcal{V}_\varepsilon(\varrho_{RA})} I^{R:B}(\varsigma_{RBE}), \quad (14)$$

where  $\varsigma_{RBE} := (\mathbb{1}_R \otimes V_A)\varrho_{RA}(\mathbb{1}_R \otimes V_A^\dagger)$ , and  $\mathcal{V}_\varepsilon(\varrho_{RA})$  is the set of isometries  $V_A : \mathcal{H}_A \mapsto \mathcal{H}_B \otimes \mathcal{H}_E$  such that  $I^{R:E}(\varsigma_{RBE}) \leq \varepsilon$  and, without loss of generality since the roles of output subsystems  $B$  and  $E$  in the definition (14) can be exchanged,  $I^{R:E}(\varsigma_{RBE}) \leq I^{R:B}(\varsigma_{RBE})$ . In formula,

$$\mathcal{V}_\varepsilon(\varrho_{RA}) := \left\{ V_A : \mathcal{H}_A \mapsto \mathcal{H}_B \otimes \mathcal{H}_E \left| \begin{array}{l} I^{R:E}(\varsigma_{RBE}) \leq \varepsilon \\ \& I^{R:E}(\varsigma_{RBE}) \leq I^{R:B}(\varsigma_{RBE}) \end{array} \right. \right\}.$$

The non-negative quantity  $\Xi_A(\varrho_{RA}; \varepsilon)$ , which we call  $\varepsilon$ -*ineliminable information* (or, equivalently,  $\varepsilon$ -*ineliminable correlations*), measures the amount of correlations with the Referee that Alice cannot eliminate, without discharging into the environment more than  $\varepsilon$  bits of them. We will refer to the parameter  $\varepsilon$  as the *privacy level parameter*: the two extreme cases, that is,  $\varepsilon = 0$  and  $\varepsilon = \infty$ , correspond to *perfect* PQD and to *advantage preserving* PQD, respectively. In the following, for sake of clarity, we will denote  $\Xi_A(\varrho_{RA}; \infty)$  simply as  $\Xi_A(\varrho_{RA})$ . Notice that  $\Xi_A(\varrho_{RA}; \varepsilon) = 0$  if and only if  $\Xi_A(\varrho_{RA}) = 0$ .

#### 3.2. Few properties at a glance

Already from the definition (14), we can see that  $\Xi_A(\varrho_{RA}; \varepsilon)$  is invariant under local unitary operations, that is

$$\Xi_A \left( (U_R \otimes W_A)\varrho_{RA}(U_R^\dagger \otimes W_A^\dagger); \varepsilon \right) = \Xi_A(\varrho_{RA}; \varepsilon). \quad (15)$$

Moreover, for all  $\varepsilon_1 \geq \varepsilon_2$ ,

$$0 \leq \Xi_A(\varrho_{RA}; \varepsilon_1) \leq \Xi_A(\varrho_{RA}; \varepsilon_2) \leq I^{R:A}(\varrho_{RA}), \quad (16)$$

since all the values of  $I^{R:B}(\varsigma_{RBE})$  that are achievable with the constraint  $I^{R:E}(\varsigma_{RBE}) \leq \varepsilon_2$  are also achievable with the looser constraint  $I^{R:E}(\varsigma_{RBE}) \leq \varepsilon_1$ , but not viceversa, while the upper bound  $I^{R:A}(\varrho_{RA})$  is trivially achieved when Alice does nothing at all, in such a way that  $I^{R:E}(\varsigma_{RBE}) = 0$ .

### 3.3. Private local randomness is a resource

Implicitly, by giving Alice the possibility of performing local isometric embeddings, we are providing her with free access to local pure states: indeed, an isometric embedding is nothing but a unitary interaction of the system with some pure ancillary state.

On the contrary, let us think for a while to the opposite situation, like the one considered in Ref. [3, 9] in the context of local purity distillation, where Alice is granted unlimited access to local randomness, that is, she can freely create maximally mixed states. In particular, let us consider such a local randomness as being *private*, i. e. factorized from all other parties taking part—either actively or passively—into the protocol (including the adversary Eve). Within this alternative scenario, suppose that Alice and the Referee initially share some bipartite two-qubits state  $\varrho_{RA}$ . Since we allow local private randomness for free, we can actually consider the state

$$\varrho_{RA\tilde{A}} := \varrho_{RA} \otimes \frac{\mathbb{1}_{\tilde{A}}}{4}, \quad (17)$$

where  $\tilde{A} \cong \mathbb{C}^4$  belongs to Alice, namely, Alice happens to be provided with two extra-bits of private randomness. The idea is now simple: Alice can use these two extra-bits in order to securely decouple  $A$  from  $R$ . The decoupling isometry  $V_{A\tilde{A}} : A\tilde{A} \rightarrow A\tilde{A}$  Alice has to perform is given by

$$V_{A\tilde{A}} := \sum_{i=0}^3 \sigma_A^i \otimes |i\rangle\langle i|_{\tilde{A}}, \quad (18)$$

where the  $\{\sigma^i\}_i$  correspond to the Pauli's matrices  $\{\mathbb{1}, \sigma^x, \sigma^y, \sigma^z\}$ . Written  $\varsigma_{RA\tilde{A}} := (\mathbb{1}_R \otimes V_{A\tilde{A}})\varrho_{RA\tilde{A}}(\mathbb{1}_R \otimes V_{A\tilde{A}}^\dagger)$ , it is easy to check that

$$\varsigma_{R\tilde{A}} = \varrho_R \otimes \frac{\mathbb{1}_{\tilde{A}}}{4} \quad \& \quad \varsigma_{RA} = \varrho_R \otimes \frac{\mathbb{1}_A}{2}, \quad (19)$$

that implies  $\Xi_{A\tilde{A}}(\varrho_{RA\tilde{A}}; \varepsilon) = 0$ , for all  $\varepsilon$ . Then, two extra-bits of private randomness in  $\tilde{A}$  suffice to securely decouple any two-qubit state  $\varrho_{RA}$  shared between  $R$  and  $A$ , no matter how correlated is the state  $\varrho_{RA}$ . Notice that this is in agreement with Ref. [2]. It is important at this point to stress that, in order to eliminate correlations, the randomness in  $\tilde{A}$  has to lose its privacy, since in general  $\tilde{A}$  has to get correlated with  $A$ —in fact,  $\varsigma_{A\tilde{A}} = (1/4) \sum_i \sigma_A^i \rho_A \sigma_A^i \otimes |i\rangle\langle i|_{\tilde{A}}$ . This means that, even if the reduced state of  $\tilde{A}$  still looks maximally mixed after the decoupling process, it does not represent anymore a fresh source of *private* randomness: in other words, there is no *catalysis* occurring here.

We can conclude saying that, if private local randomness is provided for free, correlations can always be perfectly eliminated: in this sense, the framework of PQD implicitly assumes that local private randomness has to be considered as a *resource*.

One final remark: from the preceding example, one should not jump to the conclusion that, in order to perfectly eliminate  $n$  bits of total correlations, at least  $n$  bits of extra-randomness are *always* needed. It is indeed possible to securely decouple a maximally pure state of two qubits, hence carrying *two bits* of total correlations, using only *one bit* of extra randomness. See Subsection 6.4 for details.



#### 4. General bounds and a monogamy relation

We now face the general problem of quantifying the amount of ineliminable correlations present in a given state  $\varrho_{RA}$  which is neither pure nor simply classically correlated. The following Proposition exhibits a useful lower bound on ineliminable correlations:

**Proposition 1** *For any given state  $\varrho_{RA}$ , it holds that*

$$\Xi_A(\varrho_{RA}; \varepsilon) \geq \max\{2I_c^{A \rightarrow R}(\varrho_{RA}) - \varepsilon, I_c^{A \rightarrow R}(\varrho_{RA}), 0\}, \quad (20)$$

and

$$\Xi_A(\varrho_{RA}) \geq \max\{I_c^{A \rightarrow R}(\varrho_{RA}), 0\}. \quad \square \quad (21)$$

**Proof.** We introduce a purification  $|\Psi_{SRA}\rangle$  of  $\varrho_{RA}$ . Then, any isometry  $V_A : \mathcal{H}_A \mapsto \mathcal{H}_B \otimes \mathcal{H}_E$  produces a four-partite pure state  $|\Upsilon_{SRBE}\rangle := (\mathbb{1}_{SR} \otimes V_A)|\Psi_{SRA}\rangle$ . Since both  $\Psi_{SRA}$  and  $\Upsilon_{SRBE}$  are purifications of the same state  $\varrho_R$ , it is easy to check (by direct inspection) that:

$$I(R:A) + I(R:S) = I(R:B) + I(R:SE). \quad (22)$$

Notice that the notation  $I(R:S)$  is not ambiguous since  $I^{R:S}(\Upsilon_{SRBE}) = I^{R:S}(\Psi_{SRA})$ . Plugging into (22) the chain rule  $I(R:SE) = I(R:S) + I(R:E|S)$ , we obtain  $I(R:B) = I(R:A) - I(R:E|S)$ . A second application of the chain rule leads to the estimate  $I(R:E|S) = I(E:R|S) \leq I(E:RS) = S(SR) + S(E) - S(B) = S(A) + S(E) - S(B)$ , hence to

$$I(R:B) \geq I_c^{A \rightarrow R}(\varrho_{RA}) + S(B) - S(E). \quad (23)$$

Along exactly the same lines, we also obtain

$$I(R:E) \geq I_c^{A \rightarrow R}(\varrho_{RA}) + S(E) - S(B). \quad (24)$$

The case of  $\varepsilon$ -PQD requires  $I(R:E) \leq \varepsilon$  and  $I(R:E) \leq I(R:B)$ . The first condition, plugged into (24), gives  $S(B) - S(E) \geq I_c^{A \rightarrow R}(\varrho_{RA}) - \varepsilon$ , which in turns, plugged into (23), gives  $I(R:B) \geq 2I_c^{A \rightarrow R}(\varrho_{RA}) - \varepsilon$ . The second condition, together with Eqs. (23) and (24), gives  $I(R:B) \geq I_c^{A \rightarrow R}(\varrho_{RA})$ . This proves Eq. (20). The case of advantage preserving PQD, on the other hand, only requires the second condition  $I(R:E) \leq I(R:B)$ , which proves Eq. (21). ■

The following Proposition refines the upper bound (16):

**Proposition 2** *For any given state  $\varrho_{RA}$ , it holds that*

$$\Xi_A(\varrho_{RA}) \leq \frac{I^{R:A}(\varrho_{RA})}{2}. \quad \square \quad (25)$$

**Proof.** Let us consider isometries of the form  $V_{\mathbf{P}} := \sum_m (|m_B\rangle \otimes |m_E\rangle) \langle \phi_A^m|$ , where the (in general neither normalized nor orthogonal) vectors  $\{|\phi_A^m\rangle\}_m$  form a rank-one POVM (positive operator valued measure), i. e.  $\sum_m \phi_A^m = \mathbb{1}_A$ , while the vectors  $\{|m\rangle\}_m$  are orthonormal. Isometries of such a form give  $I(R:B) = I(R:E)$  by construction. This means that the application of an isometry like  $V_{\mathbf{P}}$  automatically constitutes a suitable candidate for advantage preserving PQD. This means that  $\Xi_A(\varrho_{RA}) \leq \min_{\mathbf{P}} I(R:B)$ , where the minimum is taken over all rank-one POVM  $\mathbf{P}$ . To conclude the proof, we just notice that, by its very definition, the quantity  $\min_{\mathbf{P}} I(R:B)$  turns out to be equal to the so-called *unlocalizable entanglement*  $E_u^{\leftarrow}(\varrho_{RA})$  defined in Ref. [10], where it is also proved to satisfy  $E_u^{\leftarrow}(\varrho_{RA}) \leq I(R:A)/2$ . ■

Due to Proposition 2, we discover the following:

**Corollary 1** According to definition (14), it is unnecessary to consider values for the privacy parameter  $\varepsilon > I^{R:A}(\varrho_{RA})/2$ .  $\square$

Another interesting consequence of Proposition 2 is the following:

**Corollary 2 (Monogamy relation)** For any given tripartite pure state  $|\Psi_{RAB}\rangle$ , for  $\rho_{RA(B)} := \text{Tr}_{B(A)}[\Psi_{RAB}]$ , it holds that

$$\Xi_A(\rho_{RA}) + \Xi_B(\rho_{RB}) \leq S(R), \quad (26)$$

namely, ineliminable correlations are monogamous.  $\square$

**Proof.** Due to Proposition 2,  $\Xi_A(\rho_{RA}) \leq I(R:A)/2$  and  $\Xi_B(\rho_{RB}) \leq I(R:B)/2$ . Simply by the definition of quantum mutual information then, we obtain

$$\begin{aligned} & \Xi_A(\rho_{RA}) + \Xi_B(\rho_{RB}) \\ & \leq \frac{1}{2} [S(R) + S(A) - S(RA) + S(R) + S(B) - S(RB)] \\ & = \frac{1}{2} [S(R) + S(A) - S(B) + S(R) + S(B) - S(A)] \\ & = S(R), \end{aligned}$$

where we have made use of the fact that the joint state  $|\Psi_{RAB}\rangle$  is pure, so that  $S(RA) = S(B)$  and  $S(RB) = S(A)$ .  $\blacksquare$

A relation like that in (26) is usually referred to as a *monogamy* relation, in that it implies that ineliminable correlations cannot be shared freely among the parties of a multipartite state. Such a property, highly desirable for candidate measures of ‘quantum’ correlations, is a distinctively quantum feature—indeed, classical correlations can be freely distributed. In Section 7 we will discuss in more detail about the possibility, encouraged by Corollary 2, of considering ineliminable correlations as a measure of the ‘quantumness’ of the correlations present in an arbitrary bipartite quantum state.

## 5. Asymptotic scenario and achievable rates region

As it often happens, the analysis of asymptotic scenarios is considerably easier than its finite counterpart. In particular, when infinitely many i.i.d. copies of the same resource are provided, a wealth of exact results are known in the literature. In this case, we define the  $\varepsilon$ -*ineliminable information rate* by regularizing definition (14) as follows:

$$\Xi_A^\infty(\varrho_{RA}; \varepsilon) := \lim_{n \rightarrow \infty} \frac{1}{n} \min_{V_{A_n} \in \mathcal{V}_{\varepsilon_n}(\varrho_{R_n A_n}^{\otimes n})} I^{R_n:B_n}(\varsigma_{R_n B_n E_n}^{(n)}), \quad (27)$$

where  $\varsigma_{R_n B_n E_n}^{(n)} := (\mathbb{1}_R^{\otimes n} \otimes V_{A_n}) \varrho_{R_n A_n}^{\otimes n} (\mathbb{1}_R^{\otimes n} \otimes V_{A_n}^\dagger)$ ,  $\mathcal{V}_{\varepsilon_n}(\varrho_{R_n A_n}^{\otimes n})$  is the set of isometries  $V_{A_n} : \mathcal{H}_A^{\otimes n} \mapsto \mathcal{H}_{B_n} \otimes \mathcal{H}_{E_n}$  such that  $I^{R_n:E_n}(\varsigma_{R_n B_n E_n}^{(n)}) \leq \varepsilon_n$  and (without loss of generality, as noticed before)  $I^{R_n:E_n}(\varsigma_{R_n B_n E_n}^{(n)}) \leq I^{R_n:B_n}(\varsigma_{R_n B_n E_n}^{(n)})$ , and  $\varepsilon := \lim_{n \rightarrow \infty} \varepsilon_n/n$ . According to this definition,  $\varepsilon$  becomes the *privacy rate*: the case where only the constraint  $I^{R_n:E_n}(\varsigma_{R_n B_n E_n}^{(n)}) \leq I^{R_n:B_n}(\varsigma_{R_n B_n E_n}^{(n)})$  is considered will be denoted as  $\Xi_A^\infty(\varrho_{RA})$ . Again,  $\Xi_A^\infty(\varrho_{RA}; \varepsilon) = 0$  if and only if  $\Xi_A^\infty(\varrho_{RA}) = 0$ . In what follows, we will characterize the achievable rates region for PQD, that is, the set of allowed pairs  $(\Xi_A^\infty(\varrho_{RA}; \varepsilon), \varepsilon)$ , for any given initial state  $\varrho_{RA}$ .

A first characterization is given by Proposition 1, which, due to the extensivity of QMI and coherent information, i. e.  $I^{R_n:A_n}(\varrho_{R_n A_n}^{\otimes n}) = nI^{R:A}(\varrho_{RA})$  and  $I_c^{A_n \rightarrow R_n}(\varrho_{R_n A_n}^{\otimes n}) = nI_c^{A \rightarrow R}(\varrho_{RA})$ , implies that

$$\Xi_A^\infty(\varrho_{RA}; \varepsilon) \geq \max\{2I_c^{A \rightarrow R}(\varrho_{RA}) - \varepsilon, I_c^{A \rightarrow R}(\varrho_{RA}), 0\}, \quad (28)$$

and

$$\Xi_A^\infty(\varrho_{RA}) \geq \max\{I_c^{A \rightarrow R}(\varrho_{RA}), 0\}. \quad (29)$$

In fact, the bound (29) can be proved to be an equality:

**Proposition 3** *For any given state  $\rho_{RA}$ , it holds that*

$$\Xi_A^\infty(\varrho_{RA}) = \max\{I_c^{A \rightarrow R}(\varrho_{RA}), 0\}. \quad \square \quad (30)$$

**Proof.** We continue here from where the proof of Proposition 2 ended. There, we showed that  $\Xi_A(\varrho_{RA}) \leq \min_{\mathbf{P}} I(R:B)$ , where the minimum is taken over all rank-one POVM  $\mathbf{P}$ . The quantity  $\min_{\mathbf{P}} I(R:B)$  is itself a well-defined quantity with its own well-defined regularized version, which we denote by  $\tilde{\Xi}_A^\infty(\varrho_{RA}) \geq \Xi_A^\infty(\varrho_{RA})$ . Let us now introduce a purification  $|\Psi_{SRA}\rangle$  of  $\varrho_{RA}$  and define  $\varrho_{SR} := \text{Tr}_A[\Psi_{SRA}]$ . As shown in Ref. [18], the monogamy formula holds  $\tilde{\Xi}_A^\infty(\varrho_{RA}) + E_A^\infty(\varrho_{SR}) = S(R)$ , where  $E_A^\infty(\varrho_{SR})$  is the so-called *rate of entanglement of assistance*, which has been proved in Ref. [19] to be equal to  $\min\{S(S), S(R)\}$ . Since  $S(S) = S(RA)$ , we have  $\tilde{\Xi}_A^\infty(\varrho_{RA}) = \max\{I_c^{A \rightarrow R}(\varrho_{RA}), 0\}$ , and, due to Eq. (29), we obtain the statement of the proposition. ■

Our analysis hence led us to a situation like the one depicted in Figure 1, where the achievable rates region for a given initial state  $\varrho_{RA}$  is sketched.

As we noticed before, the condition  $\Xi_A^\infty(\varrho_{RA}) = 0$  is equivalent to saying that  $A$  can be privately decoupled from  $R$ , in the limit of infinitely many copies provided. On the other hand, it is known that, for any separable state  $\varrho_{RA}$ ,  $\max\{I_c^{R \rightarrow A}, I_c^{A \rightarrow R}\} \leq 0$ , [24]. This provides an intriguing connection between PQD and entanglement theory, stated in the following corollary of Proposition 3:

**Corollary 3 (Ineliminable versus separable correlations)** *For any separable state  $\varrho_{RA}$ ,  $\Xi_A^\infty(\varrho_{RA}) = 0$ . In other words, the presence of asymptotically ineliminable information is a signature of quantum entanglement. □*

## 6. Some examples

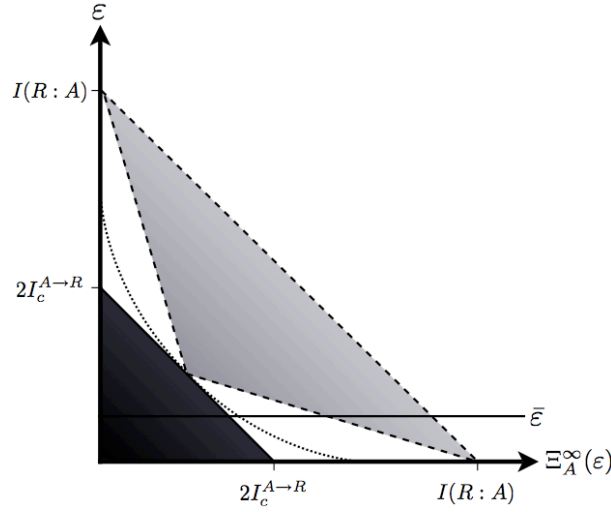
The following examples are presented in order to show that the notion of ineliminable correlations cannot be straightforwardly explained in terms of entanglement only, as soon as one leaves the pure state case. It is however very hard to find explicit counterexamples, as the minimization in Eq. (14) is difficult to be explicitly solved in general.

### 6.1. Pure states

As we already noticed, Propositions 1-3 imply that, for any pure bipartite state  $|\Psi_{RA}\rangle$ , it holds

$$\Xi_A(\Psi_{RA}) = \Xi_A^\infty(\Psi_{RA}) = S(R), \quad (31)$$

namely, ineliminable correlations equal the entropy of entanglement.



**Figure 1.** The figure depicts the asymptotically achievable rates region for PQD for a given  $\varrho_{RA}$ , that is, the set of allowed pairs  $(\Xi_A^\infty(\varrho_{RA}; \varepsilon), \varepsilon)$ , for any given initial state  $\varrho_{RA}$ . The symmetry about the bisector reflects the possibility of exchanging the roles of subsystems  $B$  and  $E$  in Eq. (14). The dark-grey shaded area around the origin corresponds to rates which are forbidden due to Proposition 1. The light-grey shaded area, instead, corresponds to rates achievable via the result in Proposition 3 and time-sharing. The white areas in between are not characterized yet, as well as the boundary of the achievable rates region, which could well be given by some curve similar to the dotted one. When the privacy rate is set to some  $\bar{\varepsilon} < \infty$ , the corresponding achievable rates region is further constrained to lie below the line  $\varepsilon = \bar{\varepsilon}$ . Finally, note that, for pure states,  $I(R:A) = 2I_c^{R \rightarrow A}$ , namely, the achievable rates region collapses onto the most external dashed line, according to the fact that correlations carried by bipartite pure states constitute a conserved quantity. On the other hand, for separable states,  $I_c^{R \rightarrow A} \leq 0$ , namely, the achievable rates region fills the octant: in this case, perfect PQD, i. e. the origin  $(0, 0)$ , is achievable (see Corollary 3).

### 6.2. Classically correlated states

When  $A$  possesses purely classical information about  $R$ , i. e. when the shared state  $\varrho_{RA}$  is classically  $A \rightarrow R$  correlated, that is [3, 22]

$$\varrho_{RA} = \sum_i p_i \varrho_R^i \otimes |i\rangle\langle i|_A, \quad (32)$$

for orthonormal  $|i\rangle$ 's, we already saw at the end of Section 2 that

$$\Xi_A(\varrho_{RA}) = \Xi_A(\varrho_{RA}; \varepsilon) = 0, \quad (33)$$

that is, classical correlations can be perfectly shredded.

### 6.3. Random-unitary channels

Let us consider a quantum system  $A$ , whose state is initially described by the density matrix  $\sigma$ , undergoing a channel  $\mathcal{T} : A \rightarrow B$ . Let  $|\Psi_{RA}\rangle$  be the purification of  $\sigma_A$ , where the system  $R$  plays the role of a reference that does not change in time. Moreover, let  $W_A : A \rightarrow BE$  be the Stinespring's isometry [17] purifying the channel  $\mathcal{T}$ , that is

$$\mathcal{T}_A(\sigma_A) = \text{Tr}_E[W_A \sigma_A W_A], \quad \forall \sigma. \quad (34)$$

Let us denote as  $|\Phi_{RBE}\rangle := (\mathbb{1}_R \otimes W_A)|\Psi_{RA}\rangle$  the tripartite pure state finally shared among the output  $B$ , the environment  $E$ , and the reference  $R$ .

If the channel  $\mathcal{T}$  is a closed evolution, namely, if it is described by one isometry only, then the reference  $R$  is completely decoupled from the environment  $E$ . Let us suppose now that the only error occurring in the whole process is due to a classical shuffling, resulting in a classical randomization of different possible isometries: then, the resulting evolution will not be described by one particular isometry, as in the closed evolution case, but rather by a mixture of such isometries. This kind of noisy evolutions are called *random-unitary channels* and act like

$$\mathcal{R} : \sigma \mapsto \sum_i p_i V_i \sigma V_i^\dagger, \quad (35)$$

where  $p_i$  is a probability distribution and  $V_i : A \rightarrow B$  are isometries. The following questions arise naturally: which kind of correlations between the reference and the environment cause (or, depending on the point of view, are caused by) such a ‘classical’ error? Which properties do these correlations satisfy? Can we ascribe a ‘classical character’ to these correlations?

It is known [23] that a channel  $\mathcal{R} : A \rightarrow B$  admits (on the support of the input state  $\sigma$ ) a random-unitary Kraus representation as in Eq. (35) if and only if there exists a rank-one POVM  $\mathbf{P}_E := \{\varphi_E^m\}_m$ ,  $\sum_m \varphi_E^m = \mathbb{1}_E$ , on the environment  $E$  such that

$$\varrho_R^m \propto \varrho_R, \quad \forall m, \quad (36)$$

where  $\varrho_R^m := \text{Tr}_{BE}[\Phi_{RBE} (\mathbb{1}_{RB} \otimes \varphi_E^m)]$ . This implies that

$$\mathcal{R} \text{ random-unitary} \Rightarrow \Xi^{A_2}(\tau^{A_2 B}; \varepsilon) = 0, \quad \forall \varepsilon \geq 0. \quad (37)$$

In other words, random-unitary channels create, between the reference system  $R$  and the environment  $E$ , correlations that are perfectly eliminable with a local action on  $E$  only.

It is important now to stress that, in general, the form of the reference-environment joint state  $\text{Tr}_B[\Phi_{RBE}]$ , originating from the purification of a random-unitary channel  $\mathcal{R} : A \rightarrow B$ , can in principle be different from that of a classically  $E \rightarrow R$  correlated state as in Eq. (32). In other words, random-unitary channels induce a class of states for which perfect PQD is possible that is in principle *larger* than the class of classically correlated states.

**Open problem.** Since the implication in (37) is in one direction only, it would be interesting to characterize the class of channels inducing only perfectly eliminable correlations between the reference and the environment: is such a class strictly larger than the class of random-unitary channels? If so, does it admit an easier characterization ¶?

#### 6.4. Mixed entangled states

We already saw, in Subsection 3.3, that there exist entangled mixed states that can be securely decoupled for all  $\varepsilon \geq 0$ . There, we needed two extra-bits of private randomness in order to securely decouple whatever two-qubits state, in agreement

¶ In fact, there is no known constructive algorithm to check whether a given channel is random-unitary or not. Only the necessary condition of being unital can be easily checked, but it is also sufficient only in the simple case of qubit channels.

with the fact that a two-qubits state contains at most two bits of total correlations. However, before rushing to the conclusion that we *always* need at least  $n$  extra-bits of randomness to perfectly eliminate  $n$  bits of total correlations, we should consider the following example where *just one* extra-bit of randomness is required to securely decouple a maximally entangled pure state of two qubits (hence carrying two bits of total correlations).

Let us consider indeed the state acting on  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$  defined as

$$\sigma_{RA\tilde{A}} := \Psi_{RA}^+ \otimes \frac{\mathbb{1}_{\tilde{A}}}{2}, \quad (38)$$

where  $|\Psi_{RA}^+\rangle := 2^{-1/2}(|00\rangle + |11\rangle)$ . For this state, even if  $\tilde{A}$  carries only *one* bit of extra-private randomness, one can show that  $\Xi_{A\tilde{A}}(\sigma_{RA\tilde{A}}) = 0$ . The proof is easy, as the null value is achieved by the isometry  $M_{A\tilde{A}} : A\tilde{A} \rightarrow BE$ , with  $B \cong E \cong \mathbb{C}^4$ , defined as

$$M_{A\tilde{A}} := \sum_{i=1}^4 |i_B\rangle \langle e_{A\tilde{A}}^i| \otimes |i_E\rangle, \quad (39)$$

where

$$\begin{aligned} |e^1\rangle &:= 2^{-1/2}(|00\rangle + |11\rangle), \\ |e^2\rangle &:= 2^{-1/2}(|00\rangle - |11\rangle), \\ |e^3\rangle &:= 2^{-1/2}(|10\rangle + |01\rangle), \\ |e^4\rangle &:= 2^{-1/2}(|10\rangle - |01\rangle). \end{aligned}$$

In fact, the isometry  $M_{A\tilde{A}}$  is coherently performing the measurement needed to teleport the maximally mixed state  $\mathbb{1}/2$  from  $\tilde{A}$  to  $R$ . Hence, for every outcome  $i$ , the reduced state on  $R$  is equal to  $\mathbb{1}/2$ , so that, written  $\varsigma_{RBE} = (\mathbb{1}_R \otimes M_{A\tilde{A}})\sigma_{RA\tilde{A}}(\mathbb{1}_R \otimes M_{A\tilde{A}}^\dagger)$ , we get  $\varsigma^{RB} = \frac{\mathbb{1}_R}{2} \otimes \frac{\mathbb{1}_B}{4}$  and  $\varsigma^{RE} = \frac{\mathbb{1}_R}{2} \otimes \frac{\mathbb{1}_E}{4}$ , which yields  $\Xi_{A\tilde{A}}(\sigma_{RA\tilde{A}}; \varepsilon) = 0$ , for all  $\varepsilon \geq 0$ .

## 7. Discussion: ineliminable correlations, entanglement, and the ‘quantumness’ of correlations

Through PQD, we found a non-trivial division of total correlations,  $I(A : B)$ , into ineliminable ones, measured by  $\Xi_A(\varrho_{RA})$ , and eliminable ones, representing the rest, that is,  $I(A : B) - \Xi_A(\varrho_{RA})$ .

At this point, it is tempting to speculate a bit about hypothetical relations between the division of correlations into ineliminable and eliminable ones, versus the division into quantum and classical correlations [3, 20, 21, 22]. We already saw how random-unitary noise, that is classical noise in the sense explained in Subsection 6.3, only induces perfectly eliminable correlations between the reference and the environment. Moreover, ineliminable correlations satisfy the two axioms required in Ref. [22] for a measure of quantumness: they are zero for classically correlated states (32) and they are invariant under local unitary transformations (15).

Also, being upper bounded by one half of the quantum mutual information and being equal to the entropy of entanglement for pure states, ineliminable correlations fall under the hypotheses of Theorem 2 in Ref. [25], which proves that, for an arbitrary bipartite state  $\varrho_{RA}$  with  $S(A) \leq S(R)$ , it holds

$$0 \leq S(A) - I_c(A \rightarrow R) \leq f\left(2\sqrt{S(A) - \Xi_A(\varrho_{RA})}\right), \quad (40)$$

where  $f(x)$  is a Fannes-type function [8], that is a positive, concave, continuous, monotonically increasing function which depends on the dimension of the underlying Hilbert space only logarithmically and satisfies  $\lim_{x \rightarrow 0} f(x) = 0$ . Eq. (40) shows that, whenever the amount of ineliminable correlations in a bipartite state is sufficiently large, then such a state is necessarily entangled, since also coherent information has to be correspondingly close to the upper bound  $S(A)$ .

In this sense, ineliminable correlations can be considered ‘genuinely quantum’ correlations, since Eq. (40) tells us that they constitute an entanglement *parameter*, in the sense explained in [27], namely, the more ineliminable correlations are present, the more the state is entangled (coherent information is the paramount example of an entanglement parameter), even though ineliminable correlations do not satisfy many natural requirements to be a proper entanglement *measure*. In reinforcing this interpretation, it stands the fact, expressed by Corollary 2, that ineliminable correlations indeed satisfy a monogamy constraint, which is another strongly distinctive feature of quantum correlations versus classical ones.

Another interesting feature of ineliminable correlations is that, for every state  $\rho_{RA}$ , they always represent (already at the level of a single copy) *at most one half* of the total amount of correlations, that is,  $\Xi_A(\rho_{RA}) \leq I(R:A)/2$  always. This fact is to be compared, once again, with what happens for different measures of ‘quantum vs classical’ correlations: according to different definitions, there exist quantum states exhibiting quantum correlations *without* classical correlations, hence representing a strikingly counterintuitive situation [21, 26]. On the contrary, assuming for a while the definition of quantum correlations as the ineliminable ones, every quantum state would turn out to be always more correlated classically than quantum, hence reinforcing the common-sense intuition about correlations.

However, in spite of this encouraging list of properties, the existence of entangled—even maximally entangled—states with perfectly eliminable correlations only (recall the examples analyzed in Subsections 3.3 and 6.4) seems to stand as an insurmountable argument against the maybe naive statement ‘what is ineliminable is quantum’. We however think that the dichotomy proposed here can contribute to the program of understanding the structure of total correlations, as coming from the *operational* paradigm of distant laboratories, versus the notion of entanglement, which is the *formal* property of not being separable.

## 8. Conclusions

We introduced the operational task of private quantum decoupling (PQD), which naturally arises as a model-independent description of secure disposal of information. Partial results suggest that there may be a deep connection between the theory of PQD and the theory of quantum entanglement. Further research in this direction would be in order. Moreover, it could be useful to generalize the asymptotic results presented here to the one-shot scenario, by exploiting some recently introduced tools [28]. Also, PQD could turn out to be useful in designing quantum cryptographic protocols, where the possibility of securely erasing old data and keys is required [29].

## Acknowledgments

Stimulating discussions with N. Datta, G. Gour, M. Horodecki, and J. Oppenheim are gratefully acknowledged. This research was supported by the Program

for Improvement of Research Environment for Young Researchers from Special Coordination Funds for Promoting Science and Technology (SCF) commissioned by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan.

## References

- [1] A. K. Pati and S. L. Braunstein, *Nature* **404**, 164 (2000); M. Horodecki, R. Horodecki, A. Sen(De), and U. Sen, *Found. of Phys.* **35**, 2041 (2005); R. Jozsa, *IBM J. Res. & Dev.* **48**, 79 (2004); S. L. Braunstein and A. K. Pati, *Phys. Rev. Lett.* **98**, 080502 (2007); P. Hayden and J. Preskill, *J. High En. Phys.* **9**, 120 (2007).
- [2] B. Groisman, S. Popescu, and A. Winter, *Phys. Rev. A* **72**, 032317 (2005).
- [3] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke, *Phys. Rev. A* **71**, 062307 (2005).
- [4] R. L. Stratonovich, *Probl. Inf. Transm.* **2**, 35 (1965); C. Adami and N. J. Cerf, *Phys. Rev. A* **56**, 3470 (1997).
- [5] B. Schumacher and M. A. Nielsen, *Phys. Rev. A* **54**, 2629 (1996); S. Lloyd, *Phys. Rev. A* **55**, 1613 (1997).
- [6] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proc. 41st FOCS, 2000*, 547 (unpublished), e-print arXiv:quant-ph/0003101v2; P. O. Boykin and V. Roychowdhury, *Phys. Rev. A* **67**, 042317 (2003); P. Hayden, D. Leung, P. W. Shor, and A. Winter, *Comm. Math. Phys.* **250**, 371 (2004).
- [7] G. M. D'Ariano, R. Demkowicz-Dobrzański, P. Perinotti, and M. F. Sacchi, *Phys. Rev. Lett.* **99**, 070501 (2007).
- [8] M. Hayashi, *Quantum Information: an Introduction* (Springer-Verlag, Berlin, Heidelberg, 2006).
- [9] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, *Phys. Rev. Lett.* **90**, 100402 (2003).
- [10] F. Buscemi, G. Gour, and J. S. Kim, *Phys. Rev. A* **80**, 012324 (2009).
- [11] M. Horodecki, J. Oppenheim, and A. Winter, *Nature* **436**, 673 (2005); M. Horodecki, J. Oppenheim, and A. Winter, *Comm. Math. Phys.* **269**, 107 (2007); J. Oppenheim, arXiv:0805.1065v1 [quant-ph].
- [12] I. Devetak and J. Yard, arXiv:quant-ph/0612050v1; J. Yard and I. Devetak, arXiv:0706.2907v1 [quant-ph].
- [13] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, *Proc. R. Soc. A* **465**, 2537–2563 (2009).
- [14] See the special issue of *Open Systems and Information Dynamics*, **15**, n. 1 (2008), entirely dedicated to various quantum capacity coding proofs achieved via decoupling arguments.
- [15] F. Buscemi and N. Datta, arXiv:0902.0158v4 [quant-ph]. To appear on *IEEE Trans. Inf. Th.* (2009).
- [16] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, 1991).
- [17] W. F. Stinespring, *Proc. Am. Math. Soc.* **6**, 211 (1955).
- [18] M. Koashi and A. Winter, *Phys. Rev. A* **69**, 022309 (2004).
- [19] J. A. Smolin, F. Verstraete, and A. Winter, *Phys. Rev. A* **72**, 052317 (2005).
- [20] L. Henderson and V. Vedral, *J. Math. Phys.* **34**, 6899 (2001); H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **99**, 017901 (2001).
- [21] A. Grudka, M. Horodecki, P. Horodecki, and R. Horodecki, arXiv:0805.3060v1 [quant-ph].
- [22] B. Groisman, D. Kenigsberg, and T. Mor, arXiv:quant-ph/0703103v1.
- [23] M. Gregoratti and R. F. Werner, *J. Mod. Opt.* **50**, 915 (2003); F. Buscemi, *Phys. Rev. Lett.* **99**, 180501 (2007).
- [24] R. Horodecki and P. Horodecki, *Phys. Lett. A* **194**, 147 (1994).
- [25] F. Buscemi, *Phys. Rev. A* **77**, 012309 (2008).
- [26] L. Pankowski and B. Synak-Radtke, *J. Phys. A: Math. Theor.* **41**, 075308 (2008); D. Kaszlikowski, A. Sen(De), U. Sen, V. Vedral, and A. Winter, *Phys. Rev. Lett.* **101**, 070502 (2008).
- [27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).
- [28] R. Koenig, R. Renner, and C. Schaffner, arXiv:0807.1338v1 [quant-ph].
- [29] R. Canetti, D. Eiger, S. Goldwasser, and D.-Y. Lim, *LNCS* **5126**, 511 (2008).