Erasable and Unerasable Correlations

G. M. D'Ariano,[1] R. Demkowicz-Dobrzański,[2] P. Perinotti,[1] and M. F. Sacchi[1,3]

[1]*QUIT Group, Dipartimento di Fisica "A. Volta" and CNISM, via Bassi 6, I-27100 Pavia, Italy*
[2]*Center for Theoretical Physics of the Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warszawa, Poland*
[3]*CNR - Istituto Nazionale per la Fisica della Materia, Unità di Pavia, Italy*
(Received 19 March 2007; published 15 August 2007)

We address the problem of removing correlation from sets of states while preserving as much local quantum information as possible. We prove that states obtained from universal cloning can only be decorrelated at the expense of complete erasure of local information (i.e., information about the copied state). We solve analytically the problem of decorrelation for two qubits and two qumodes (harmonic oscillators in Gaussian states), and provide sets of decorrelable states and the minimum amount of noise to be added for decorrelation.

The laws of quantum mechanics impose a number of restrictions on the processing of *quantum information*. Examples of such impossible tasks are provided by the famous no-cloning theorem [1] or by the theorem on non-existence of the universal-NOT gate [2]. Despite their discouraging appearance, such limitations can sometimes be proved useful. This is the case with the no-cloning theorem which is at the core of quantum cryptography, as it prevents an eavesdropper from creating perfect copies of a transmitted quantum state.

In this Letter we attempt to broaden our understanding of the limitations imposed on the quantum information processing, by investigating the possibility of *decorrelating quantum states*—i.e., removing unwanted correlations between quantum subsystems while preserving local information encoded in each of them.

To be more specific, we say that an operation $\mathcal{D}$ *faithfully decorrelates* an N-partite state ρ if the following equation holds

$$\mathcal{D}(\rho) = \rho_1 \otimes \ldots \otimes \rho_N, \qquad (1)$$

where ρ_i is the ith party reduced density matrix of ρ. Now, the problem of decorrelability can be stated as follows: given a set of states $S = \{\rho\}$, we ask whether there exists a *single* physically realizable operation (completely positive map) $\mathcal{D}$ that satisfies (1) for every state ρ in S.

Analogously, as in the case of the no-cloning theorem, the answer will strongly depend on the chosen set of states. In particular, if the set S consists of only one element ρ, then the problem of decorrelability is trivial. One can always choose $\mathcal{D}$ to be a map producing $\otimes_{i=1}^{N}\rho_i$ out of any input. Such a map is completely positive and hence every single-element set is decorrelable.

Moving to the other extreme, and asking whether a set S consisting of all density matrices is decorrelable, one finds out that due to linearity of quantum mechanics it is not [3]. Actually, from the proof of [3] one can easily draw a stronger conclusion, namely, the following: If a set S

contains the states ρ', ρ'' and their convex combination $\lambda\rho' + (1 - \lambda)\rho''$, and the reduced states of ρ' and ρ'' are different at least for two parties, then faithful decorrelability of the set S is impossible.

Moreover, in [3] nondecorrelability of certain two-element sets was shown using the fact that after decorrelation distinguishability of states cannot increase (see also [4] for some results on disentangling rather than decorrelating states). Apart from the above particular cases, very little is known on the decorrelability of general sets of quantum states. In this Letter we search for explicit solutions to the decorrelation problem in interesting settings.

The key factor for deciding on decorrelability and nondecorrelability is the choice of the set of states. In this Letter such a choice is motivated by the need of considering the problem of decorrelation in the information-processing context. We stress that we decorrelate quantum *states* by keeping the quantum *signals*. We propose the following paradigm.

Consider an N-partite *correlated* "seed" state ρ, which should be regarded as the initial state where information is encoded. Let U_g be a unitary representation of a group G, acting on the Hilbert space of a single party. The representation describes the encoding procedure of a piece of information (the group element g) on the state of a subsystem. Acting with unitary operations $U_{g_1} \otimes \ldots \otimes U_{g_N}$ on the seed state ρ should be regarded as encoding N pieces of information (N signals [5]) $\boldsymbol{g} = (g_1, \ldots, g_N) \in G^N$:

$$\rho_{\boldsymbol{g}} := U_{g_1} \otimes \ldots \otimes U_{g_N} \rho U_{g_1}^{\dagger} \otimes \ldots \otimes U_{g_N}^{\dagger}. \qquad (2)$$

The above state is clearly correlated due to the correlation of the seed state ρ. The problem of decorrelation is to find a single operation $\mathcal{D}$ that would decorrelate [see Eq. (1)] all states belonging to the set

$$S(U_g, \rho) = \{\rho_{\boldsymbol{g}}, \forall_{\boldsymbol{g}} \in G^N\}. \qquad (3)$$

If we have additional constraints on the signals (e.g., we know that they are identical $g_1 = \ldots = g_N$) the above set

is smaller, and eventually the problem of decorrelation becomes easier. Notice that the reduced density matrices of ρ_g are related to the reduced density matrices of ρ by $U_{g_i}\rho_i U_{g_i}^\dagger$, and as a result the decorrelated state still carries the same signals as the initial one. We stress that we do not deal here with decorrelation of *signals*, but rather with decorrelation of states carrying them (hence, there is no contradiction in performing decorrelation and still claiming, e.g., that the encoded signals are identical).

To motivate our work further let us recall some facts about cloning and state estimation. We know that quantum information cannot be copied or broadcast exactly, due to the no-cloning theorem. Nevertheless, one can find approximate optimal cloning operations which increase the number of copies of a state at the expense of the quality. In the presence of noise, however, (i.e., when transmitting "mixed" states), it can happen that we are able to increase the number of copies without losing the quality, if we start with sufficiently many identical originals. Indeed, it is even possible to *purify* in such a broadcasting process—the so-called *superbroadcasting* [6]. Clearly, a larger number of copies cannot increase the available information about the original input state, and this is due to the fact that the final copies are not statistically independent, and the correlations between them limit the extractable information [7]. It is now natural to ask if we can remove such correlations and make them independent again (notice that in this decorrelation problem, the signals g_i—which in this case correspond to the cloned states—are identical). Clearly, such quantum decorrelation cannot be achieved exactly, otherwise we would increase the information on the state. *A priori* it is not excluded, however, that it is possible to decorrelate clones at the expense of introducing some additional noise. One of the results of this Letter is that clones by universal cloning cannot be decorrelated even within this relaxed condition. Apart from this negative result, we provide in this Letter examples of states for which decorrelation is possible.

Thanks to the structure of the set of states (3) that we want to decorrelate, a covariant decorrelation must satisfy the following conditions: (i) $\mathcal{D}$ decorrelates the seed state; (ii) $\mathcal{D}$ fulfills the covariance condition

$$\mathcal{D}(U_{g_1}\otimes\ldots\otimes U_{g_N}\rho U_{g_1}^\dagger\otimes\ldots\otimes U_{g_N}^\dagger)$$
$$= U_{g_1}\otimes\ldots\otimes U_{g_N}\mathcal{D}(\rho)U_{g_1}^\dagger\otimes\ldots\otimes U_{g_N}^\dagger. \quad (4)$$

We will more generally consider decorrelation with additional noise on the output local states, namely,

$$\mathcal{D}(\rho)=\tilde{\rho}_1\otimes\ldots\tilde{\rho}_N, \quad (5)$$

where $\tilde{\rho}_i\neq\rho_i$. As a result, subsystems are still perfectly decorrelated, but some information about reduced density matrices is lost. Additionally, in what follows we will assume that the seed state is permutationally invariant—in other words we treat all encoded signals on equal footing. This simplifies the situation since in this case all single party reduced density matrices of the seed state are equal and the same should hold for the noisy reduced density matrices after decorrelation. This assumption allows us, without loss of generality, to impose permutational covariance on the decorrelating operation $\mathcal{D}$.

We now present the solution for some interesting bipartite situations. We analyze *qubits*, in which information is encoded through general unitaries in $\mathbb{SU}(2)$, and *qumodes* (harmonic oscillators in Gaussian states), with information encoded by the representation of the Weyl-Heisenberg group of displacements. In our analysis we consider the two situations in which the unitaries representing signals on the two systems are either independent or equal. The latter case is relevant for the decorrelability of output states of cloning and broadcasting machines. It turns out that decorrelation is indeed possible in some cases, at the expense of increasing local noise. The optimal decorrelating map adding the minimum amount of noise is derived in the qubit case, and the optimal depolarization factor is evaluated as a function of the input seed state. For Gaussian states we show that it is always possible to erase correlations by means of a suitable Gaussian map.

Consider a couple of qubits A and B. Permutational invariance of the seed state means that it is block diagonal with respect to singlet and triplet subspaces. For qubits the state is conveniently described in the Bloch form. Without loss of generality we may assume that the reduced density matrices $\rho_A=\rho_B=\frac{1}{2}(\mathbb{1}+\eta\sigma_z)$ of the seed state ρ_{AB} are diagonal in the σ_z basis. The information (α,β) is encoded via the action of $U(\alpha)\otimes U(\beta)$:

$$\rho_{AB}(\alpha,\beta)=U(\alpha)\otimes U(\beta)\rho_{AB}U(\alpha)^\dagger\otimes U(\beta)^\dagger, \quad (6)$$

where α and β are elements of $\mathbb{SU}(2)$. In other words it is encoded on the direction of the Bloch vectors $\boldsymbol{n}_A(\alpha)$ and $\boldsymbol{n}_B(\beta)$ of the marginal states

$$\rho_A(\alpha)=\text{Tr}_B[\rho_{AB}(\alpha,\beta)]=\tfrac{1}{2}[\mathbb{1}+\eta\boldsymbol{n}_A(\alpha)\cdot\boldsymbol{\sigma}],$$
$$\rho_B(\beta)=\text{Tr}_A[\rho_{AB}(\alpha,\beta)]=\tfrac{1}{2}[\mathbb{1}+\eta\boldsymbol{n}_B(\beta)\cdot\boldsymbol{\sigma}], \quad (7)$$

where $\boldsymbol{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$ is the vector of Pauli matrices. Covariance of the decorrelation map means that the direction of the Bloch vectors $\boldsymbol{n}_A(\alpha)$ and $\boldsymbol{n}_B(\beta)$ should be preserved in the output states, i.e.,

$$\tilde{\rho}_A(\alpha)=\tfrac{1}{2}[\mathbb{1}+\tilde{\eta}\boldsymbol{n}_A(\alpha)\cdot\boldsymbol{\sigma}],$$
$$\tilde{\rho}_B(\beta)=\tfrac{1}{2}[\mathbb{1}+\tilde{\eta}\boldsymbol{n}_B(\beta)\cdot\boldsymbol{\sigma}], \quad (8)$$

namely only the length of the Bloch vector (i.e., the purity of the state) is changed $\eta\to\tilde{\eta}$. The additional noise of the output states corresponds to a reduced length of the Bloch vector $\tilde{\eta}<\eta$. The directions of the Bloch vectors $\boldsymbol{n}_A(\alpha)$ and $\boldsymbol{n}_B(\alpha)$ are completely arbitrary. The optimal decorrelation map will maximize the length $\tilde{\eta}$ of the Bloch vector; namely, it will produce the highest purity of decorrelated states. It can be shown [8] that the general form of a two-

qubit channel $\mathcal{D}$ covariant under $U(\alpha) \otimes U(\beta)$ and invariant under permutations of the two qubits can be parameterized with three positive parameters only (effectively two due to normalization)

$$\mathcal{D}(\rho_{AB}) = a\rho_{AB} + b\mathcal{D}_1(\rho_{AB}) + c\mathcal{D}_2(\rho_{AB}), \quad (9)$$

where $\mathcal{D}_1$ and $\mathcal{D}_2$ are given by

$$\mathcal{D}_1(\rho_{AB}) = \tfrac{1}{3}(\rho_A \otimes \mathbb{1} + \mathbb{1} \otimes \rho_B - \rho_{AB}), \quad (10)$$

$$\mathcal{D}_2(\rho_{AB}) = \tfrac{1}{9}(4\mathbb{1} \otimes \mathbb{1} - 2\rho_A \otimes \mathbb{1} - 2\mathbb{1} \otimes \rho_B + \rho_{AB}), \quad (11)$$

and the trace preserving condition gives $a + b + c = 1$. This is a very restricted set of operations, due to the fact that the covariance condition is very strong. As a consequence the condition for decorrelating the seed state

$$\mathcal{D}(\rho_{AB}) = \tilde{\rho}^{\otimes 2} = [\tfrac{1}{2}(\mathbb{1} + \tilde{\eta}\sigma_z)]^{\otimes 2} \quad (12)$$

cannot be satisfied for a generic seed state ρ_{AB} (apart from the trivial decorrelation to a maximally mixed state).

The seed states for which nontrivial decorrelation is possible [which means that we can find such a, b, c and $\tilde{\eta} > 0$ satisfying Eq. (12)] have the form [8]

$$\rho_{AB} = \tfrac{1}{4}[\mathbb{1} \otimes \mathbb{1} + \eta(\sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z) - \lambda\sigma_z \otimes \sigma_z]. \quad (13)$$

We emphasize that for a generic seed state ρ_{AB} one can reduce correlations, but only sets arising from the seed state of the form (13) can be decorrelated completely in a nontrivial way (apart from the cases when $\eta = 0$ or $\lambda = 0$). The noise of the decorrelated states depends on parameters η and λ as depicted in Fig. 1.

In order to study the decorrelability of the output states of cloning machines, we consider now the case where the same unitary is encoded on the two qubits (identical signals). Differently from the case of independent signals, $\mathcal{D}$ has to be covariant with respect to $U(\alpha)^{\otimes 2}$, which is a weaker condition than covariance with respect to $U(\alpha) \otimes U(\beta)$. Using the methods from [6] one can parameterize these class of operations with six parameters $s_{j,l,J}$ satisfying two constraints, so effectively one enjoys a four parameter freedom on covariant operations. Thanks to this larger freedom it can be shown [8] that the decorrelation condition $\mathcal{D}(\rho_{AB}) = \tilde{\rho}^{\otimes 2}$ is non trivially satisfied (i.e. for $\tilde{\eta} > 0$) for a generic state ρ_{AB} which is diagonal in the singlet triplet basis. Such a state can be written in the form

$$\rho_{AB} = p|\Psi^-\rangle\langle\Psi^-| + (1 - p)\rho_{\text{sym}}, \quad (14)$$

where ρ_{sym} is a state supported on the triplet (symmetric) subspace, and $|\Psi^-\rangle$ is the singlet state. Analogously to Eq. (13), ρ_{sym} can be written with the help of Pauli matrices
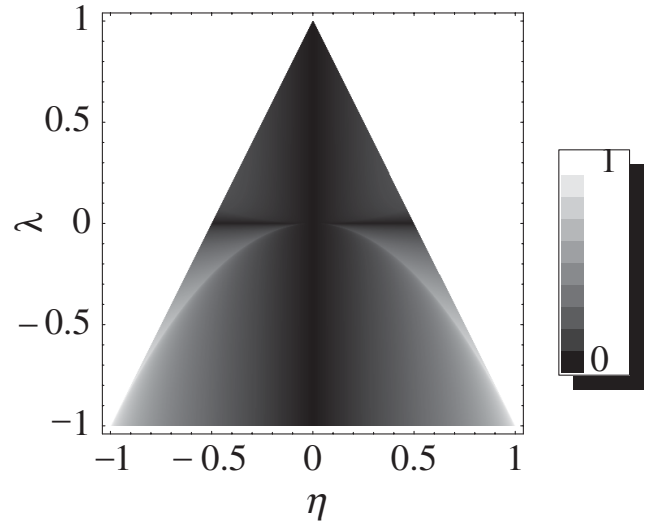

FIG. 1. Length $\tilde{\eta}$ of the Bloch vectors of the decorrelated states of two qubits starting from the joint state in Eq. (13). The plot depicts the maximal achievable $\tilde{\eta}$ in gray scale versus the parameters η and λ of the input state.

$$\rho_{\text{sym}} = \tfrac{1}{4}[\mathbb{1} \otimes \mathbb{1} + \eta(\sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z)$$
$$+ (1 + \lambda)/2(\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y) - \lambda\sigma_z \otimes \sigma_z]. \quad (15)$$

The only states that cannot be nontrivially decorrelated are those with either $p = 1$ or $\eta = 0$ or $\lambda = -1/3$. For $p = 0$ (i.e., for seed states supported on the symmetric space) the plot for achievable $\tilde{\eta}$ is analogous to Fig. 1, but now the black horizontal line containing nondecorrelable states lays at $\lambda = -1/3$. Interestingly, these nondecorrelable states are states which can be obtained via universal cloning machines producing two copies out of one copy of a qubit state. Hence, clones obtained by 1-to-2 universal cloning cannot be nontrivially decorrelated.

Such a result can be shown in general for N-to-M universal cloning of d-dimensional systems (*qudits*) along the following lines. Without loss of generality, we can restrict ourselves to $M = N + 1$ and consider cloning of pure states [9]. The universal covariance of the cloning and decorrelation procedure implies that for every pure state $|\phi\rangle$ of a qudit the desired transformation has the form

$$\Lambda[(|\phi\rangle\langle\phi|)^{\otimes N}] = \left(\eta|\phi\rangle\langle\phi| + \frac{1 - \eta}{2}\mathbb{1}\right)^{\otimes N+1} \quad (16)$$

The transformation (16) is only possible for $\eta = 0$. Indeed, let us consider these transformation for "equatorial states", i.e., $|\phi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$, where $|0\rangle$, $|1\rangle$ are some arbitrary orthogonal states. If $\eta \neq 0$ entries of the operator on the right hand side of (16) are polynomials of degree at most $N + 1$ of $e^{\pm i\phi}$ (and some entries actually achieve this degree). On the other hand, thanks to linearity of Λ, the entries on left-hand side are polynomials of

degree at most N of $e^{\pm i\phi}$. Since equality (16) should be satisfied for all phases ϕ we arrive at a contradiction, since no polynomial of degree N can be equal to a polynomial of degree $N + 1$ in an infinite number of points. The above reasoning holds true also for asymmetric cloning with different η for each output, where one can prove that at least one coefficient η must be null [10].

We consider now the case of decorrelation for qumodes. For a couple of qumodes in a joint seed state ρ_{AB} the information (α, β) (with α and β complex) is encoded as follows

$$D(\alpha) \otimes D(\beta) \rho_{AB} D(\alpha)^\dagger \otimes D(\beta)^\dagger, \qquad (17)$$

$D(z) = \exp(za^\dagger - z^*a)$ for $z \in \mathbb{C}$ denoting a single-mode displacement operator, a and $a^\dagger$ being the annihilation and creation operators of the mode. Here we show that it is always possible to decorrelate any joint state of the form (17), with ρ_{AB} representing a two-mode Gaussian state, namely,

$$\rho_{AB} = \frac{1}{\pi^4} \int d^4q \, e^{-(1/2)q^T M q} D(q), \qquad (18)$$

where $q = (q_1, q_2, q_3, q_4)$, $D(q) = D(q_1 + iq_2) \otimes D(q_3 + iq_4)$, and M is the 4×4 (real, symmetric, and positive) correlation matrix of the state, that satisfies the Heisenberg uncertainty relation [11] $M + \frac{i}{4}\Omega \geq 0$, with $\Omega = \oplus_{k=1}^2 \omega$ and

$$\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

A Gaussian decorrelation channel covariant under $D(\alpha) \otimes D(\beta)$ is given by

$$\mathcal{D}(\rho) = \frac{\sqrt{\det G}}{(2\pi)^2} \int d^4x \, e^{-(1/2)x^T G x} D(x) \rho D^\dagger(x), \qquad (19)$$

with suitable positive matrix G [8], and the resulting state $\mathcal{D}(\rho_{AB})$ is still Gaussian, with a new block-diagonal covariance matrix $\tilde{M}$, thus corresponding to a decorrelated state.

A special example of Gaussian state of two qumodes is the so-called *twin beam*, which can be generated in a quantum optical lab by parametric down-conversion of vacuum. In this case M is given by

$$M = \frac{1 + \lambda^2}{1 - \lambda^2} \mathbb{1} - \frac{2\lambda}{1 - \lambda^2} \begin{pmatrix} 0 & \sigma_z \\ \sigma_z & 0 \end{pmatrix}, \qquad (20)$$

with $0 \leq \lambda < 1$. The map (19) with

$$G = \frac{2\lambda}{1 - \lambda^2} \left[\mathbb{1} + \begin{pmatrix} \varepsilon & \sigma_z \\ \sigma_z & \varepsilon \end{pmatrix} \right], \qquad (21)$$

and arbitrary $\varepsilon > 0$, provides two decorrelated states with $\tilde{M} = (\frac{1+\lambda}{1-\lambda} + \varepsilon)\mathbb{1}$, which correspond to two thermal states with mean photon number $\bar{n} = \frac{\lambda}{1-\lambda} + \frac{\varepsilon}{2}$ each. Since the

channel in Eq. (19) is covariant also for $D(\alpha)^{\otimes 2}$, the above derivation then holds for the case of encryption with the same unitary on both qumodes as well.

The striking difference between the qubit and the qumode cases is that for qubits only few states can be decorrelated, whereas for qumodes any joint Gaussian state can be decorrelated. This is due to the fact that the covariance group for qubits comprises all local unitary transformations, whereas for qumodes it includes only local displacements, which is a very small subset of all possible local unitary transformations in infinite dimension. In particular it can be checked that unlike qudits, states obtained via Gaussian cloning of coherent states can be decorrelated and the no-go proof valid for finite dimensional cases does not apply here.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[2] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A, **60**, R2626 (1999).

[3] D. R. Terno, Phys. Rev. A **59**, 3320 (1999).

[4] T. Mor, Phys. Rev. Lett. **83**, 1451 (1999).

[5] The word signal suggests sometimes a sequence of pieces of information being transmitted. In our case, this will simply correspond to repeated preparation of the state ρ_g with varying set $g = \{g_1, \ldots, g_N\}$ in each shot.

[6] G. M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. Lett. **95**, 060503 (2005).

[7] R. Demkowicz-Dobrzanski, Phys. Rev. A **71**, 062321 (2005); J. Bae, and A. Acin, Phys. Rev. Lett. **97**, 030402 (2006).

[8] G. M. D'Ariano, R. Demkowicz-Dobrzanski, P. Perinotti, and M. F. Sacchi (to be published).

[9] For the proof of impossibility it is enough to consider $M = N + 1$ since if cloning without correlations were possible for $M' > N + 1$, then by partial trace over $M' - N - 1$ output copies we would obtain a cloning operation with $M = N + 1$. Moreover, we can restrict attention to pure states, since if cloning were possible for mixed states, then it would be possible for pure states, too. Indeed one could apply depolarizing channels to the input pure states before cloning.

[10] Strictly speaking the above statement can be proved without the use of the covariance condition (see [8]). Covariance condition was used here for the sake of simplicity and consistency with the general approach taken in the Letter.

[11] R. Simon, E. C. G. Sudarshan, and N. Mukunda, Phys. Rev. A **36**, 3868 (1987); R. Simon, N. Mukunda, and B. Dutta, Phys. Rev. A **49**, 1567 (1994).