

Asymptotically optimal quantum channel reversal for qudit ensembles and multimode Gaussian states

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2012 New J. Phys. 14 113041

(<http://iopscience.iop.org/1367-2630/14/11/113041>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 128.243.253.114

This content was downloaded on 17/03/2014 at 16:58

Please note that [terms and conditions apply](#).

Asymptotically optimal quantum channel reversal for qudit ensembles and multimode Gaussian states

P Bowles, M Guță and G Adesso¹

School of Mathematical Sciences, The University of Nottingham,
University Park, NG7 2RD Nottingham, UK
E-mail: gerardo.adesso@nottingham.ac.uk

New Journal of Physics **14** (2012) 113041 (17pp)

Received 17 August 2012

Published 29 November 2012

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/14/11/113041

Abstract. We investigate the problem of optimally reversing the action of an arbitrary quantum channel C which acts independently on each component of an ensemble of n identically prepared d -dimensional quantum systems. In the limit of large ensembles, we construct the optimal reversing channel R_n^* which has to be applied at the output ensemble state, to retrieve a smaller ensemble of m systems prepared in the input state, with the highest possible rate m/n . The solution is found by mapping the problem into the optimal reversal of Gaussian channels on multimode quantum-classical continuous variable systems, which is solved here as well. Our general results can be readily applied to improve the implementation of robust long-distance quantum communication. As an example, we investigate the optimal reversal rate of phase flip channels acting on a multi-qubit register.

¹ Author to whom any correspondence should be addressed.



Content from this work may be used under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike 3.0 licence](https://creativecommons.org/licenses/by-nc-sa/3.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Contents

1. Introduction	2
2. Optimal reversal of a Gaussian channel	4
2.1. Gaussian states and channels	5
2.2. Optimal Gaussian channel reversal	6
3. Quick review of local asymptotic normality	8
4. Optimal channel reversal on mixed qudit ensembles	10
5. Example: reversal of the phase flip qubit channel	12
6. Conclusions	13
Acknowledgments	14
Appendix A. Proof that the Gaussian channel G in the diagram (3) exists	15
Appendix B. Proof of theorem 4.2	16
References	16

1. Introduction

Quantum channels are completely positive, trace-preserving maps which describe the state change of a quantum system undergoing a noisy evolution. Operationally, a channel on a d -dimensional system $C : M(\mathbb{C}^d) \rightarrow M(\mathbb{C}^d)$ can be implemented by first coupling the system with state ρ to the ‘environment’ with initial state ρ_E , letting the two evolve together as a closed system with unitary operator U , and subsequently tracing out the environmental degrees of freedom [1, 2]

$$C : \rho \longmapsto \text{Tr}_E(U(\rho \otimes \rho_E)U^*). \quad (1)$$

Due to the last step, the dynamics described by a quantum channel is typically irreversible, a basic fact which is related to several no-go theorems in quantum information [3–6]. In fact, a channel is reversible *on all states* if and only if it is unitary i.e. $C(\rho) = U\rho U^*$.

However, the reversibility problem has non-trivial solutions if the channel is required to be reversible on a given *family of states* [6]. From a mathematical perspective, this scenario is captured by the statistical concepts of quantum *sufficiency* and *equivalence of statistical models*. In the latter, two families of states

$$\mathcal{Q} := \{\rho_\theta : \theta \in \Theta\} \quad \text{and} \quad \mathcal{R} := \{\sigma_\theta : \theta \in \Theta\}$$

are said to be statistically equivalent if there exist two channels T and S such that $\sigma_\theta = T(\rho_\theta)$ and $\rho_\theta = S(\sigma_\theta)$ for all θ . In other words the channel T is reversible on \mathcal{Q} , with an inverse S . Sufficiency is a special case of this, where $T(\rho)$ is the restriction of the state ρ to a subalgebra of observables, which is then called sufficient with respect to \mathcal{Q} . A general mathematical characterization of equivalence and sufficiency has been given in [7], where a quantum analogue of the classical factorization theorem for sufficient statistics has been established.

In this paper we consider a different but related channel reversal problem, see figure 1. Consider an ensemble consisting of $n \gg 1$ independent and identically prepared quantum systems which undergo separate noisy evolutions described by the channel C . The question is whether the original state can be distilled from the noisy output by means of a reversing channel,

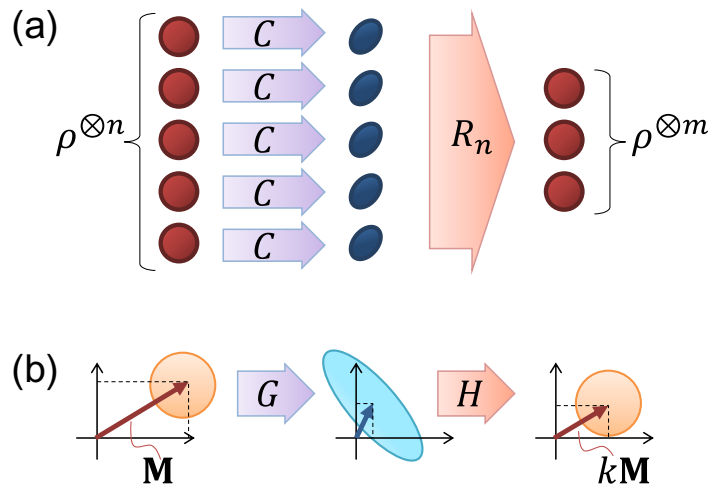


Figure 1. Graphical depiction of the problem addressed in this paper. (a) Reversal of arbitrary channels C acting independently on a register of n qudits, each initialized in the state ρ . The optimal reversing channel R_n allows to recover m qudits exactly in the state ρ , with the maximum possible output/input rate m/n . (b) The problem can be recast into the reversal of a Gaussian channel G acting on a set of generally multimode Gaussian states with unknown mean \mathbf{M} . The optimal reversing channel H restores the initial known covariance and maximizes the output/input displacement ratio k . More details are provided in the diagram (3) and in the accompanying text.

albeit at the expense of reducing the size of the ensemble due to the loss of information. More precisely, we would like to find the maximum rate $\Gamma = m/n$ for which there exist reversing channels $R_n : M(\mathbb{C}^d)^{\otimes n} \mapsto M(\mathbb{C}^d)^{\otimes m}$ such that the following holds:

$$\rho^{\otimes n} \xrightarrow{C^{\otimes n}} C(\rho)^{\otimes n} \xrightarrow{R_n} \rho^{\otimes m} \quad (2)$$

asymptotically with n (see section 4 for the mathematical formulation). This and other related questions have been considered in [4, 8] for the specific case of a qubit depolarizing channel, but to our knowledge the case of a general qudit channel has not been investigated elsewhere. The answer to our question is directly relevant to applications in quantum memories [9, 10], distributed quantum computation [11], quantum key distribution [12], and long-distance quantum communication [13]. Given a register of many qudits prepared off-line, in order to securely store it or transmit it over lossy media, one needs to incorporate modules that perform state purification or counteract decoherence effects, e.g. *quantum repeaters* [14].

The key to solving the problem lies in the quantum extension of a fundamental statistical tool known as local asymptotic normality (LAN) [15, 16]. The quantum version of LAN [17–20] shows that the joint state of an ensemble of identically prepared systems can be approximated by a Gaussian state of a continuous variable system. More precisely, we parametrize the states in a neighbourhood of size $n^{-1/2+\epsilon}$ of ρ as $\rho_{\mathbf{M}/\sqrt{n}}$ where \mathbf{M} is a $(d^2 - 1)$ -dimensional vector of expectations such that $\rho_0 \equiv \rho$; then there exists a channel T_n which maps the collective state $\rho_{\mathbf{M}/\sqrt{n}}^{\otimes n}$ into a Gaussian state $\Phi(\mathbf{M}, \mathbf{V})$ of a quantum-classical continuous variable system, with mean \mathbf{M} and known fixed covariance \mathbf{V} which depends only on ρ . Such a system is comprised

of $d(d-1)/2$ quantum modes and $d-1$ classical variables. Conversely, given the (multimode) Gaussian state, there exists a channel S_n which converts it into the multiple-qudits state with asymptotically vanishing norm-one error, without the knowledge of the parameter \mathbf{M} .

The schematic of the complete problem considered in this paper and its resolution using LAN is shown below (see figure 1 for a visual summary):

$$\begin{array}{ccccc}
 \rho_{(\mathbf{M}, \lambda)}^{\otimes n} & \xrightarrow{C^{\otimes n}} & \rho_{(\mathbf{M}', \lambda')}^{\otimes n} & \xrightarrow{R_n} & \rho_{(\mathbf{M}, \lambda)}^{\otimes m} \\
 T_n \downarrow & & T_n \downarrow & & \uparrow S_m \\
 \Phi(\mathbf{M}, \mathbf{V}) & \xrightarrow{G} & \Phi(\mathbf{M}', \mathbf{V}') & \xrightarrow{H} & \Phi(k\mathbf{M}, \mathbf{V})
 \end{array} \quad (3)$$

Using the LAN correspondence between the multiple-qudits states and the Gaussian states, we demonstrate specifically the following results.

- The action of $C^{\otimes n}$ on the qudits can be mimicked by the action of a Gaussian channel on the Gaussian states, i.e. the rightmost square loop of the diagram (3) is (asymptotically) commutative (cf theorem 4.1).
- The optimal qudit reversal problem for the channel C is effectively recast into a much handier Gaussian one, of reversal of the Gaussian channel G [21–25] where the length of the final displacement vector is allowed to be a fraction k of the initial length as illustrated in the bottom row of the diagram (3); the problem is to find the maximum possible k and the corresponding reversing channel H (cf theorem 4.2).
- The Gaussian reversal problem has an explicit solution (k^*, H^*) as described in theorem 2.1. The optimal reversal of a general Gaussian channel is in its own right an important problem for continuous variable quantum communication and key distribution [26, 27], which we solve in a specific case of input states associated with qudit ensembles.
- Putting together the above findings we prove that the concatenation $R_n := S_m \circ H \circ T_n$ realizes the *optimal* strategy for reversal of the channel $C^{\otimes n}$ applied to n independent and identically prepared qudits, and that the maximal qudit rate m/n in the top row of the diagram (3) is equal to $(k^*)^2$, where k^* is the maximum possible value of k for which the Gaussian reversal is possible.

The paper is organized as follows. In section 2 we find the optimal procedure and rate for reversing the action of general Gaussian channels on a family of Gaussian states with fixed covariance and unknown mean. Section 3 contains a short review of LAN motivated by the quantum central limit theorem (CLT). In section 4 we solve the problem of finding the optimal rate and procedure for the reversal of a qudit channel by reducing it to the Gaussian problem via LAN. In section 5 we illustrate the general results with a specific application to reversing phase flip channels acting on a multiqubit register, a common source of errors arising in quantum computation [1]. We draw our concluding remarks in section 6. Some technical proofs are deferred to appendices.

2. Optimal reversal of a Gaussian channel

In order to solve the qudit channel reversal problem, it is necessary to obtain the solution to the corresponding Gaussian problem. We begin with a short review of Gaussian states and channels, referring the reader to [26–29] for more comprehensive accounts.

2.1. Gaussian states and channels

Let $\mathbf{Z} = (\mathbf{A}, \mathbf{B})^T$ be the (column vector of) coordinates of a continuous variable system where the components $\mathbf{A}^T = (Q_1, P_1, \dots, Q_K, P_K)$ are the canonical observables of K modes, and $\mathbf{B}^T = (B_1, \dots, B_C)$ is a classical \mathbb{R}^C -valued random variable. In other words, the canonical variables satisfy the commutation relations $[Z_k, Z_l] = i\Omega_{kl}\mathbf{1}$ where Ω is the block-diagonal symplectic form

$$\Omega = \text{Diag}(\sigma, \dots, \sigma, \mathbf{0}_C), \quad \text{with} \quad \sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Throughout, we consider that the quantum variables are represented in the standard fashion on the multi-mode Hilbert space $\mathcal{H}^{\otimes K} := L^2(\mathbb{R})^{\otimes K}$ and the classical variables are realized as coordinate multiplication operators on $\mathcal{H}^{\otimes C}$ so that the full Hilbert space is $\mathcal{H}^{\otimes(K+C)}$.

Any state Φ of the continuous variable system is completely determined by its *characteristic function*

$$\chi_\Phi(z) := \Phi\left(e^{iz^T \mathbf{Z}}\right),$$

where $\Phi(X)$ denotes the expectation of X with respect to Φ . In particular, for every mean $\mathbf{M} = \Phi(\mathbf{Z})$ and covariance matrix \mathbf{V} with elements

$$V_{kl} = \Phi(Z_k * Z_l) - \Phi(Z_k)\Phi(Z_l), \quad Z_k * Z_l := \frac{Z_k Z_l + Z_l Z_k}{2},$$

there is a unique Gaussian state $\Phi(\mathbf{M}, \mathbf{V})$ with characteristic function

$$\chi_{\mathbf{M}, \mathbf{V}}(z) = e^{iz^T \mathbf{M} - \frac{1}{2} z^T \mathbf{V} z}, \quad (4)$$

provided that \mathbf{V} satisfies the uncertainty principle $\mathbf{V} \geq -\frac{i}{2}\Omega$. For later use, we will denote by $\phi(\mathbf{M}, \mathbf{V}) \in \mathcal{T}_1(\mathcal{H}^{\otimes K}) \otimes L^1(\mathbb{R}^C)$ the density matrix of the state $\Phi(\mathbf{M}, \mathbf{V})$.

A Gaussian quantum channel is a channel as in (1), where the environment is a bosonic continuous variable system whose initial state is Gaussian, and the unitary U is determined by a quadratic Hamiltonian in the system and environment coordinates [21–25]. In the Heisenberg picture, the action of a Gaussian channel G is

$$\begin{aligned} G^* &: \mathcal{B}(\mathcal{H}^{\otimes K}) \otimes L^\infty(\mathbb{R}^{\otimes C}) \rightarrow \mathcal{B}(\mathcal{H}^{\otimes K}) \otimes L^\infty(\mathbb{R}^{\otimes C}), \\ G^* &: W_z \longmapsto W_{\mathbf{X}_G z} e^{-\frac{1}{2} z^T \mathbf{Y}_G z}, \end{aligned} \quad (5)$$

where $W_z := e^{iz^T \mathbf{Z}}$ are the ‘Weyl operators’, $\mathbf{X}_G, \mathbf{Y}_G$ are real matrices of dimension $2K + C$, with \mathbf{Y}_G positive and satisfying the matrix inequality

$$\mathbf{Y}_G \geq i(\mathbf{X}_G^T \Omega \mathbf{X}_G - \Omega).$$

In particular, from (4) and (5) we find that when G acts on the state $\Phi(\mathbf{M}, \mathbf{V})$, it produces a new Gaussian state $\Phi(\mathbf{M}', \mathbf{V}')$ with mean $\mathbf{M}' = \mathbf{X}_G^T \mathbf{M}$ and covariance $\mathbf{V}' = \mathbf{X}_G^T \mathbf{V} \mathbf{X}_G + \mathbf{Y}_G$. While the first term in \mathbf{V}' describes the change in variance due to the linear transformation X_G , the second term comes from the covariance of the ancillary ‘environment’ used to realize G . For more details on Gaussian channels and their classification we refer to [22, 30].

2.2. Optimal Gaussian channel reversal

Our problem can be stated as follows: given a Gaussian channel G , and a family of Gaussian states

$$\mathcal{G}_V := \{\Phi(\mathbf{M}, \mathbf{V}) : \mathbf{M} \in \mathbb{R}^{2K+C}\} \quad (6)$$

with fixed covariance matrix \mathbf{V} and unknown mean \mathbf{M} , we would like to find the maximum value k^* of a constant k for which there exists a (not necessarily Gaussian) channel H such that for all $\mathbf{M} \in \mathbb{R}^{2K+C}$ the following holds (see figure 1(b)):

$$H \circ G(\phi(\mathbf{M}, \mathbf{V})) = \phi(k\mathbf{M}, \mathbf{V}). \quad (7)$$

A special case of this problem, for single-mode attenuation and amplification channels, has been considered in [8]. Our first main result is to find k^* and the optimal channel for the general set-up.

Theorem 2.1. *Let G be the Gaussian channel (5), and assume that \mathbf{X}_G is an invertible matrix. The largest value of k for which G can be reversed on the family of states (6) is*

$$k^* = \left[\lambda_{\max} \left(\boldsymbol{\varsigma}^{-\frac{1}{2}} \boldsymbol{\varrho} \boldsymbol{\varsigma}^{-\frac{1}{2}} \right) \right]^{-\frac{1}{2}}, \quad (8)$$

where $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue, and

$$\boldsymbol{\varrho} = (\mathbf{X}_G^{-1})^T \left(\mathbf{X}_G^T \mathbf{V} \mathbf{X}_G + \mathbf{Y}_G + \frac{i}{2} \Omega \right) \mathbf{X}_G^{-1}, \quad \boldsymbol{\varsigma} = \mathbf{V} + \frac{i}{2} \Omega$$

are positive matrices.

Equivalently, k^* can be expressed in terms of the ‘max-relative entropy’ [31] as

$$\log_2(k^{*-2}) = D_{\max}(\boldsymbol{\varrho} \parallel \boldsymbol{\varsigma}) := \log_2(\min \{k^{-2} : \boldsymbol{\varrho} \leq k^{-2} \boldsymbol{\varsigma}\}).$$

For every $k \leq k^*$ there exists a reversing Gaussian channel H , of the form (5), with

$$\begin{aligned} \mathbf{X}_H &= k\mathbf{X}_G^{-1}, \\ \mathbf{Y}_H &= \mathbf{V} - k^2(\mathbf{X}_G^{-1})^T(\mathbf{X}_G^T \mathbf{V} \mathbf{X}_G + \mathbf{Y}_G)\mathbf{X}_G^{-1}. \end{aligned} \quad (9)$$

Proof. Following a standard argument [8, 32], it can be shown that without loss of generality we can restrict our attention to a certain class of *displacement covariant* reversing channels of the form

$$T^*(W_z) = f(z)W_{\mathbf{X}z},$$

where $\mathbf{X} = k\mathbf{X}_G^{-1}$ and $f(z) = \text{Tr}(\tau W_z)$ is the characteristic function of some ancillary state τ with zero mean. A displacement covariant channel H satisfies (7) if and only if

$$H \circ G(\phi(\mathbf{0}, \mathbf{V})) = \phi(\mathbf{0}, \mathbf{V}).$$

In terms of the characteristic functions, this means

$$\begin{aligned} \chi_{\Phi}(z) &= \text{tr}(e^{iz^T \mathbf{Z}} H(\phi')) \\ &= \text{tr}(H(e^{iz^T \mathbf{Z}} \phi')) = \text{Tr}(\tau W_z) \text{Tr}(\phi' e^{i(\mathbf{X}_H z)^T \mathbf{Z}}) \\ &= f(z) e^{-\frac{1}{2}(\mathbf{X}_H z)^T \mathbf{V} (\mathbf{X}_H z)}. \end{aligned}$$

Since χ_Φ is a Gaussian characteristic functions, $f(z) = \text{tr}(\tau W_z)$ must also be a Gaussian characteristic function. Hence H is a Gaussian channel.

Now, from (5) we see Gaussian channels are in one-to-one correspondence with two matrices: the linear transformation on the means and the covariance (noise) matrix. The Gaussian channel G and the reversal H are therefore completely characterized by $G \Leftrightarrow (\mathbf{X}_G, \mathbf{Y}_G)$ and $H \Leftrightarrow (\mathbf{X}_H, \mathbf{Y}_H)$. For an initial state $\Phi(\mathbf{M}, \mathbf{V})$, we have that the first and second moments are mapped by $(H^\circ G)$ as

$$(\mathbf{M}, \mathbf{V}) \mapsto (\mathbf{X}_H^T \mathbf{X}_G^T \mathbf{M}, \mathbf{X}_H^T (\mathbf{X}_G^T \mathbf{V} \mathbf{X}_G + \mathbf{Y}_G) \mathbf{X}_H + \mathbf{Y}_H).$$

By equating this with the target state moments $(k\mathbf{M}, \mathbf{V})$, we obtain immediately $\mathbf{X}_H = k\mathbf{X}_G^{-1}$. Now, denoting $\mathbf{V}' = \mathbf{X}_G^T \mathbf{V} \mathbf{X}_G + \mathbf{Y}_G$, we have that the reverse outputs a covariance

$$\mathbf{V} = \mathbf{X}_H^T \mathbf{V}' \mathbf{X}_H + \mathbf{Y}_H = k^2 (\mathbf{X}_G^{-1})^T \mathbf{V}' \mathbf{X}_G^{-1} + \mathbf{Y}_H. \quad (10)$$

Positivity of the quantum channel states that

$$\mathbf{Y}_H + \frac{i}{2} \Omega - \frac{i}{2} k^2 (\mathbf{X}_G^{-1})^T \Omega \mathbf{X}_G^{-1} \geq 0. \quad (11)$$

We would like to find the maximum k for which there exists some \mathbf{Y}_H which satisfies this inequality. Rearranging (10) as

$$\mathbf{Y}_H = \mathbf{V} - k^2 (\mathbf{X}_G^{-1})^T \mathbf{V}' \mathbf{X}_G^{-1},$$

then substituting in (11) gives

$$\mathbf{V} + \frac{i}{2} \Omega \geq k^2 (\mathbf{X}_G^{-1})^T \left(\mathbf{V}' + \frac{i}{2} \Omega \right) \mathbf{X}_G^{-1}. \quad (12)$$

This gives us a necessary and sufficient condition for a Gaussian channel G to be reversible up to a factor k in the displacement. The optimal reversing channel H^* is the one for which k takes its maximum possible value k^* . To find k^* , we can recast (12) in terms of a max-relative entropy and use the results of [31] to obtain equation (8). \square

This result shows that any Gaussian channel G acting on Gaussian states with given covariance, can be reversed up to a constant factor k by means of another *Gaussian* channel H , whose construction is provided explicitly. The link between the threshold value k^* and the max-relative entropy [31] is intriguing, as it reveals that k^* is operationally related to the optimal Bayesian error probability in determining which covariance matrix our system is mapped into by the channel G [33].

Explicit examples of Gaussian channel reversal on single-mode Gaussian states can be found in [8], where the practically relevant cases of attenuation and amplification are discussed in detail. We remark that the channel reversal is particularly effective in the realistic case of mixed input states, while it can become of trivial use for pure input states. For instance, a pure coherent state subject to attenuation cannot be deterministically re-amplified to another pure state with a longer displacement vector, without adding extra noise (and thus altering the covariance matrix). The optimal reversing G^* in this case turns out to be, simply, the identity channel, meaning that the incurred attenuation is not reversible. Additional error correction techniques [34] to revert the action of various sources of errors on registers of pure and weakly mixed Gaussian states could be necessary in practical implementations of continuous variable quantum communication, possibly requiring non-Gaussian operations [35].

3. Quick review of local asymptotic normality

The main tool used to solve the channel reversal problem on n -qudit ensembles in the next section of this paper is that of quantum LAN, which was developed in [17–20] as an extension of a key concept from classical asymptotic statistics [15]. For the reader's convenience we give here an intuitive explanation of LAN based on the quantum CLT.

In general terms, *classical* LAN means that given data consisting of n samples from a probability distribution \mathbb{P}_θ with unknown parameter $\theta \in \mathbb{R}^k$, there exist classical channels (randomizations) which map the data into a *single* sample from a Gaussian distribution whose mean is (locally) equal to θ , and whose variance is the inverse Fisher information matrix $I(\theta)^{-1}$. A consequence of this is the fact that the maximum likelihood estimator $\widehat{\theta}_n$ is asymptotically normal (Gaussian) with asymptotic variance $I(\theta)^{-1}$, i.e. the following convergence in distribution holds:

$$\sqrt{n}(\widehat{\theta}_n - \theta) \xrightarrow{\mathcal{L}} N(0, I(\theta)^{-1})$$

and therefore saturates the Cramér–Rao bound [16].

Quantum LAN means that the joint quantum state of independent, identically prepared finite-dimensional systems can be approximated in a strong sense by a quantum-classical Gaussian state of fixed variance, whose mean encodes the information about the parameters of the original state. In this way, a number of asymptotic problems can be reformulated in terms of Gaussian states, for which the explicit solution can be found. Examples so far include state estimation [36], system identification [37], teleportation benchmarks [38], state purification and dilution [8] and quantum learning [39].

Suppose we are given n independent d -dimensional quantum systems (qudits) each prepared in the unknown but mixed (full rank) state $\rho \in M(\mathbb{C}^d)$ with *distinct eigenvalues*. By means of an adaptive estimation strategy, we can effectively localize the initial state of each qudit within a neighborhood of size $n^{-\frac{1}{2}+\epsilon}$ centred at an estimate ρ_0 . If $\lambda_1 > \dots > \lambda_d$ are the eigenvalues of ρ_0 then with respect to its eigenbasis, any neighbouring state can be written as

$$\rho_{(\mathbf{M}/\sqrt{n}, \lambda)} = \rho_0 + \frac{1}{\sqrt{n}} \begin{pmatrix} u_1 & \Lambda_{1,2} z_{1,2}^* & \dots & \Lambda_{1,d} z_{1,d}^* \\ \Lambda_{1,2} z_{1,2} & u_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \Lambda_{d-1,d} z_{d-1,d}^* \\ \Lambda_{1,d} z_{1,d} & \dots & \Lambda_{d-1,d} z_{d-1,d} & -\sum_{i=1}^{d-1} u_i \end{pmatrix}, \quad (13)$$

where $\mathbf{M} = (\mathbf{z}, \mathbf{u}) \in \mathbb{C}^{d(d-1)/2} \times \mathbb{R}^{d-1}$ is a displacement parameter, and $\Lambda_{jk} = \sqrt{(\lambda_j - \lambda_k)/2}$ are constant coefficients chosen for later convenience. We can then define the local quantum statistical model around ρ_0 as

$$\mathcal{Q}_n = \left\{ \rho_{(\mathbf{M}/\sqrt{n}, \lambda)}^{\otimes n} : \|\mathbf{M}\| \leq n^\epsilon \right\}. \quad (14)$$

Let

$$\{O_1, \dots, O_{d^2-1}\} = \{q_{1,2}, p_{1,2}, \dots, q_{d-1,d}, p_{d-1,d}, b_1, \dots, b_{d-1}\} \quad (15)$$

be the self-adjoint operators in $M(\mathbb{C}^d)$ defined as

$$q_{j,k} := \frac{|j\rangle\langle k| + |j\rangle\langle k|}{\sqrt{2(\lambda_j - \lambda_k)}}, \quad p_{j,k} := \frac{i(|k\rangle\langle j| - |j\rangle\langle k|)}{\sqrt{2(\lambda_j - \lambda_k)}}, \quad b_i := |i\rangle\langle i| - \lambda_i \mathbf{1}. \quad (16)$$

One can verify easily that O_a satisfy the following properties.

- (i) $\{O_1, \dots, O_{d^2-1}\}$ is a basis in the space of operators with $\text{Tr}(\rho_0 O) = 0$.
- (ii) $\text{Tr}(\rho_0 [O_a, O_b]) = i\Omega_{a,b}$ where Ω is the $(d^2 - 1) \times (d^2 - 1)$ block diagonal symplectic matrix $\Omega = \text{Diag}(\sigma, \dots, \sigma, \mathbf{0}_{d-1})$.
- (iii) The covariance matrix \mathbf{V} with

$$V_{ab} := \text{Tr}(\rho_0 O_a * O_b) \quad (17)$$

has all elements equal to zero except

$$\text{Tr}(\rho_0 q_{j,k}^2) = \text{Tr}(\rho_0 p_{j,k}^2) = v_{j,k} := \frac{\lambda_j + \lambda_k}{2(\lambda_j - \lambda_k)}, \quad \text{Tr}(\rho_0 b_j b_k) := V_{jk}^{\text{cl}} := \delta_{jk} \lambda_j - \lambda_j \lambda_k. \quad (18)$$

Let $O_i(n) \in M(\mathbb{C}^d)^{\otimes n}$ denote the corresponding collective (fluctuation) observables

$$O_i(n) := \sum_{s=1}^n O_i^{(s)}, \quad O_i^{(s)} := \mathbf{1} \otimes \dots \otimes O_i \otimes \dots \otimes \mathbf{1}, \quad (19)$$

with $O_i^{(s)}$ acting on the position s of the tensor product. The collective observables play the role of sufficient statistics for our model, and we would like to understand their asymptotic behaviour. Since all systems are independent and identically prepared, and the terms in each collective observable commute, we can apply classical central limit techniques to show that the following convergence in distribution holds for the collective states $\rho_{\mathbf{M}/\sqrt{n}, \lambda}^{\otimes n}$:

$$\begin{aligned} \frac{q_{j,k}(n)}{\sqrt{n}} &\xrightarrow{\mathcal{L}} N(\text{Re}(z_{j,k}), v_{j,k}), \quad 1 \leq j < k \leq d, \\ \frac{p_{j,k}(n)}{\sqrt{n}} &\xrightarrow{\mathcal{L}} N(\text{Im}(z_{j,k}), v_{j,k}), \quad 1 \leq j < k \leq d, \\ \frac{b_l(n)}{\sqrt{n}} &\xrightarrow{\mathcal{L}} N(u_l, \lambda_l(1 - \lambda_l)), \quad 1 \leq l \leq d - 1. \end{aligned}$$

The key observation is that the unknown parameters $M = (\mathbf{z}, \mathbf{u})$ are recovered as means of the limit Gaussian distributions. However the limit model is *not* a classical one due to the fact that the collective variables do not commute with each other. Therefore we need to take into account the commutation relations of the limit variables by using the quantum CLT. These form a general continuous variable system as described in section 2.1, with $d^2 - 1$ coordinates $\mathbf{Z} = (Z_1, \dots, Z_{d^2-1}) = (Q_{j,k}, P_{j,k}, B_i)$ having the commutation relations

$$[Z_a, Z_b] = \text{Tr}(\rho_0 [O_a, O_b]) \mathbf{1}.$$

By property (ii), this means that $(Q_{j,k}, P_{j,k})$ are canonical coordinates of $d(d - 1)/2$ mutually commuting one-mode systems, and B_i are classical random variables in the sense that they commute with each other and with the quantum coordinates $(Q_{j,k}, P_{j,k})$. By the CLT the limit state is the Gaussian $\Phi(\mathbf{M}, \mathbf{V})$ with mean \mathbf{M} and covariance matrix \mathbf{V} defined in property (iii), equation (18). In particular, the individual modes $(Q_{j,k}, P_{j,k}, B_i)$ are independent of each other and of the classical variables B_i , and the latter have covariance matrix \mathbf{V}^{cl} , cf (18).

We define now the quantum-classical Gaussian statistical model \mathcal{P} as

$$\mathcal{P} := \{ \Phi(\mathbf{M}, \mathbf{V}) : \mathbf{M} \in \mathbb{R}^{d-1} \times \mathbb{C}^{d(d-1)/2} \} \quad (20)$$

and enunciate the LAN Theorem [19] which is used in establishing the optimality results in section 4.

Theorem 3.1. *The sequence of qudit models \mathcal{Q}_n defined in (14) converges to the quantum-classical Gaussian model \mathcal{P} defined in (20), in the sense that there exist $\epsilon > 0$ and channels*

$$\begin{aligned} T_n &: M(\mathbb{C}^d)^{\otimes n} \rightarrow \mathcal{T}_1(L^2(\mathbb{R})^{\otimes d(d-1)/2}) \otimes L^1(\mathbb{R}^{d-1}), \\ S_n &: \mathcal{T}_1(L^2(\mathbb{R})^{\otimes d(d-1)/2}) \otimes L^1(\mathbb{R}^{d-1}) \rightarrow M(\mathbb{C}^d)^{\otimes n}, \end{aligned}$$

such that

$$\begin{aligned} \lim_{n \rightarrow \infty} \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| T_n(\rho_{(\mathbf{M}/\sqrt{n}, \lambda)}^{\otimes n}) - \phi(\mathbf{M}, \mathbf{V}) \right\|_1 &= 0, \\ \lim_{n \rightarrow \infty} \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| \rho_{(\mathbf{M}/\sqrt{n}, \lambda)}^{\otimes n} - S_n(\phi(\mathbf{M}, \mathbf{V})) \right\|_1 &= 0. \end{aligned} \quad (21)$$

Note that the statement of the above theorem is different from that of the CLT in that theorem 3.1 shows that the collective state of the ensemble can be transferred by means of physical quantum channels to a Gaussian state, with vanishing norm-one error uniformly over the unknown parameters. The CLT is instead a statement about the convergence in law, for a fixed state and does not have an immediate operational interpretation. In the next section we will use LAN to transform the qudit reversal problem into a corresponding Gaussian reversal one, thus exploiting the solution to the latter obtained in section 2.

4. Optimal channel reversal on mixed qudit ensembles

We now focus on the main aim of this paper, that is to find optimal channels

$$R_n : M(\mathbb{C}^d)^{\otimes n} \rightarrow M(\mathbb{C}^d)^{\otimes m}$$

which reverse (at rate $\Gamma = m/n$) the action of the tensor product channel $C^{\otimes n}$ acting on n identically prepared qudits, cf (2) (see figure 1(a)). The performance of channel reversal can be quantified by a figure of merit, or risk, given by the trace-norm error $\|R_n(\rho^{\otimes n}) - \rho^{\otimes m}\|_1$. We adopt a frequentist approach and look to minimize the maximum risk over all input states. We actually work with a more refined version of the maximum risk known as the *local* maximum risk, which was already employed in other quantum statistical problems [8, 17, 18, 39]. For each state ρ , this is defined by

$$\mathcal{R}_{\max}(R_n, \rho, \Gamma) := \sup_{\|\tau - \rho\| \leq n^{-\frac{1}{2} + \epsilon}} \|R_n(\tau^{\otimes n}) - \tau^{\otimes m}\|_1$$

and quantifies the worst performance of R_n in a $n^{-\frac{1}{2} + \epsilon}$ -neighbourhood of ρ . This restriction does not amount to making an assumption about the location of the unknown state, since using a small sample $n^{1-\epsilon} \ll n$ of the systems, one can effectively localize the unknown state within a confidence region of size $n^{-\frac{1}{2} + \epsilon}$. We aim to find an optimal reversing strategy whose asymptotic risk is equal to the local minimax risk

$$\mathcal{R}_{\min\max}(\rho, \Gamma) := \limsup_{n \rightarrow \infty} \inf_{R_n} \mathcal{R}_{\max}(R_n, \rho, \Gamma). \quad (22)$$

The problem of finding the optimal reversing channel is thus reformulated as follows. For a given state ρ and output rate $\Gamma = m/n$, what is the minimax risk $\mathcal{R}_{\min\max}(\rho, \Gamma)$ and which procedure achieves it? We will not solve this problem for all (ρ, Γ) , but rather we will show that for each ρ there is an interval $[0, \Gamma^*]$ for which the reversal can be performed perfectly (i.e. with asymptotically vanishing risk $\mathcal{R}_{\min\max}(\rho, \Gamma) = 0$), and we will subsequently identify

an asymptotically optimal sequence of reversing channels R_n^* which achieves the maximum rate Γ^* .

As anticipated, the quantum LAN theory [17–20], reviewed in section 3 is the key tool in solving this problem. For technical reasons related to the validity of LAN, we assume that the state ρ is not on the boundary of the state space, and is not degenerate so that its spectrum $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_d)$ satisfies $\lambda_1 > \dots > \lambda_d$. A typical random state satisfies these assumptions. Following equations (13)–(16) we can parametrize the states in the $n^{-1/2+\epsilon}$ neighbourhood of ρ as $\rho_{\mathbf{M}/\sqrt{n}, \boldsymbol{\lambda}}$ where $\mathbf{M} = (\mathbf{z}, \mathbf{u}) \in \mathbb{C}^{d(d-1)/2} \times \mathbb{R}^{d-1}$ is a vector of expectations for the matrices $\{O_1, \dots, O_{d^2-1}\}$. By LAN, the sequence of input quantum statistical models

$$\mathcal{Q}_n := \left\{ \rho_{(\mathbf{M}/\sqrt{n}, \boldsymbol{\lambda})}^{\otimes n} : \|\mathbf{M}\| \leq n^\epsilon \right\}$$

is asymptotically equivalent in the sense of theorem 3.1, to the sequence of Gaussian models \mathcal{P}_n over a quantum-classical continuous variable system with coordinates \mathbf{Z}

$$\mathcal{P}_n := \{ \Phi(\mathbf{M}, \mathbf{V}) : \|\mathbf{M}\| \leq n^\epsilon \},$$

where $\Phi(\mathbf{M}, \mathbf{V})$ which is a tensor product between $d(d-1)/2$ independent one-mode displaced thermal equilibrium states $\Phi(z_{j,k}, v_{j,k})$ (one for each pair $j < k$) with mean $z_{j,k}$ and covariance $v_{j,k}$ (cf equation (18)), and a classical $(d-1)$ -dimensional Gaussian probability density $\mathcal{N}(\mathbf{u}, \mathbf{V}^{\text{cl}})$.

We apply the same procedure to the output state $\rho' := C(\rho)$ and denote by

$$\rho_{\mathbf{M}'/\sqrt{n}, \boldsymbol{\lambda}'} := C(\rho_{\mathbf{M}/\sqrt{n}, \boldsymbol{\lambda}}),$$

the transformed state belonging to the neighbourhood of $C(\rho)$. The corresponding Gaussian model with coordinates \mathbf{Z}' is

$$\mathcal{P}'_n := \{ \Phi(\mathbf{M}', \mathbf{V}') : \|\mathbf{M}'\| \leq n^\epsilon \},$$

where \mathbf{V}' depends solely on the spectrum of ρ' . The displacements of the two Gaussian models are related by a linear transformation

$$\mathbf{X}^T : \mathbf{M} \mapsto \mathbf{M}',$$

which describes the local action of C around ρ , and hence depends only on these two objects. The ensemble transformation $C^{\otimes n}$ acts on the localized states as

$$C^{\otimes n} : \rho_{(\mathbf{M}/\sqrt{n}, \boldsymbol{\lambda})}^{\otimes n} \mapsto \rho_{(\mathbf{M}'/\sqrt{n}, \boldsymbol{\lambda}')^{\otimes n}}. \quad (23)$$

Since both the input and the output can be approximated by Gaussian states and the transformation between the displacements is linear, one can expect that the two Gaussian states are connected by a Gaussian channel G as depicted in diagram (3). The following theorem states that this is indeed the case and the proof can be found in appendix A.

Theorem 4.1. *There exists a Gaussian channel G such that*

$$G : \phi(\mathbf{M}, \mathbf{V}) \mapsto \phi(\mathbf{X}^T \mathbf{M}, \mathbf{V}').$$

The matrices $(\mathbf{X}_G, \mathbf{Y}_G)$ characterizing G (cf (5)) are $\mathbf{X}_G = \mathbf{X}$ and $\mathbf{Y}_G = \mathbf{V}' - \mathbf{X}^T \mathbf{V} \mathbf{X}$.

We now move to the problem of finding the optimal reversing channel for multiple qudits. As illustrated in the right side of the diagram (3), the solution relies on LAN to recast the problem into the Gaussian one solved in theorem 2.1. We now state the second main result of this paper, whose proof is in appendix B .

Theorem 4.2. *Let $\rho \in M(\mathbb{C}^d)$ be a full rank state with non-degenerate spectrum, and let $C : M(\mathbb{C}^d) \rightarrow M(\mathbb{C}^d)$ be a quantum channel which is invertible as a linear map. Let (k^*, H^*) be the optimal rate and channel for the Gaussian reversal problem (cf theorem 2.1)*

$$\phi(\mathbf{M}, \mathbf{V}) \xrightarrow{G} \phi(\mathbf{X}^T \mathbf{M}, \mathbf{V}') \xrightarrow{H} \phi(k\mathbf{M}, \mathbf{V}) \quad \mathbf{M} \in \mathbb{R}^{d-1} \times \mathbb{C}^{d(d-1)/2},$$

where $\mathbf{V}, \mathbf{V}', X$ depend on C and ρ as above.

Then the maximum reversal rate for the qudit ensemble is $\Gamma^* = (k^*)^2$ and

$$R_n^* := S_{\Gamma^* n} \circ H^* \circ T_n$$

is a sequence of optimal reversing channels i.e.

$$\limsup_{n \rightarrow \infty} \sup_{\|\tau - \rho\|_1 \leq n^{-\frac{1}{2} + \epsilon}} \|R_n(\tau^{\otimes n}) - \tau^{\otimes n}\|_1 = 0.$$

This result shows, in full generality, that in order to reverse the action of an arbitrary channel acting on a large ensemble of n qudits, independent and identically prepared in an unknown mixed state ρ , the optimal strategy is to take a shortcut through phase space², optimally reverse the corresponding Gaussian channel, and then map the output back onto m qudits (with rate $m/n = \Gamma^*$).

This kind of digital–analogue interconversion might prove handy when it comes to counteract the effect of noisy channels affecting quantum states of, say, n -atom ensembles: the best strategy ought to be transferring their state onto light modes (e.g. using quantum non-demolition interactions [10]), implementing corrective procedures on the obtained Gaussian beams in phase space (according to the recipe of theorem 2.1), and then mapping the restored state back onto the atomic storage unit. We will now showcase our results on a specific example.

5. Example: reversal of the phase flip qubit channel

The qubit phase flip channel is defined by $C(\rho) = \sum_k E_k \rho E_k^\dagger$, with $E_0 = \sqrt{p} \text{Diag}(1, 1)$ and $E_1 = \sqrt{1-p} \text{Diag}(1, -1)$ [1]. Phase flip is a common source of error in quantum computation and several algorithms have been developed for its correction [34]. According to theorem 4.2, an optimal way to reverse the composite action of individual phase flips on a n -qubit register is to map the state of the qubit register onto a Gaussian state (which in this case comprises a single quantum mode and one real classical random variable), reverse the corresponding Gaussian channel (up to a rescaling factor k^*), and map the output back onto the qubits.

As described in the previous section we consider states in a neighbourhood of ρ ; the latter has in general the Bloch vector representation

$$\rho = \frac{1}{2} \begin{pmatrix} 1 + r_z & r_x + i r_y \\ r_x - i r_y & 1 - r_z \end{pmatrix}. \quad (24)$$

² Shortcuts through higher dimensions are also useful to simplify quantum computing logic, see [40].

The neighbourhood of ρ is parametrized as in (13) with $\mathbf{M} = (z, u) \in \mathbb{C} \times \mathbb{R}$. The action of the channel C is

$$C : \mathbf{r} = (r_x, r_y, r_z) \mapsto \mathbf{r}' = ((2p - 1)r_x, (2p - 1)r_y, r_z).$$

From this we can compute the covariance matrices

$$\mathbf{V} = \text{Diag} \left(\frac{1}{2\|\mathbf{r}\|}, \frac{1}{2\|\mathbf{r}\|}, 1 - \|\mathbf{r}\|^2 \right), \quad \mathbf{V}' = \text{Diag} \left(\frac{1}{2\|\mathbf{r}'\|}, \frac{1}{2\|\mathbf{r}'\|}, 1 - \|\mathbf{r}'\|^2 \right),$$

where $\|\mathbf{r}'\|^2 = (2p - 1)^2(r_x^2 + r_y^2) + r_z^2$. Similarly the matrix \mathbf{X}_G^T is obtained after computing the transformation of the local states under C

$$\mathbf{X}_G^T = \begin{pmatrix} (2p - 1)\sqrt{\frac{\|\mathbf{r}\|}{\|\mathbf{r}'\|}} & 0 & 0 \\ 0 & (2p - 1)\left(\frac{\|\mathbf{r}\|}{\|\mathbf{r}'\|}\right)^{\frac{3}{2}} & 0 \\ 0 & -\frac{4(1-p)r_x r_z}{\|\mathbf{r}'\|\|\mathbf{r}\|} & \frac{\|\mathbf{r}'\|}{\|\mathbf{r}\|} \end{pmatrix}. \quad (25)$$

We are interested in evaluating the threshold factor k^* as given by (8), which is associated to the optimal rate $m/n = (k^*)^2$ for phase flip reversal on the qubit register. Due to the inherent symmetry of the channel, we may set $r_y = 0$ without any loss of generality, and assume $\frac{1}{2} \leq p \leq 1$. Therefore k^* will depend on p, r_x, r_z . The results are summarized as follows.

For $p = 1$ the channel is trivially the identity, therefore $k^* = 1$ for any \mathbf{r} . For $p = 1/2$ the channel is never reversible, and $k^* = 0$ for any \mathbf{r} . In the limit of pure input states of each qubit ($\|\mathbf{r}\| \rightarrow 1$), we find that $k^* \rightarrow 2p - 1$ if $r_x \rightarrow 0$, and $k^* \rightarrow 0$ otherwise (i.e. the channel is not reversible for any pure state, if there is a non-zero component on the x -axis). In case $r_x = 0$, we find $k^*(p, r_x = 0, r_z) = 2p - 1$, which means that, as intuitively expected, the rate does not depend on r_z . On the other hand, in case $r_z = 0$, we have

$$k^*(p, r_x, r_z = 0) = \sqrt{[(2p - 1)^2(1 - r_x^2)] / [1 - (-1 + 2p)^2 r_x^2]}.$$

We observe that for small values of r_x this tends again to the line $2p - 1$; for r_x close to 1, k^* is instead a sublinear function of p , as depicted in figure 2, showing that the reversal becomes inefficient in terms of the number of perfectly retrieved copies. In general, if a non-zero r_x is present as well, the behaviour of k^* as a function of p is qualitatively similar to the previous case, but typically k^* increases, at fixed $\|\mathbf{r}\|$ and p , with increasing ratio $|r_z/r_x|$. The general shape of k^* as a function of the Bloch vector components interpolates among the various limits discussed above, and is plotted in figure 3.

6. Conclusions

In this paper we have solved the general problem of optimal channel reversal for an ensemble of generally mixed independent and identically prepared qudits. This substantially extends our earlier work [8] on the particular instance of state purification (and dilution) of qubit ensembles. To accomplish our task, we have employed the versatile statistical tool of LAN [17, 19] to recast the problem in terms of Gaussian states and channels, then solved the open problem of optimal reversal of a general Gaussian channel acting on a multimode quantum-classical Gaussian state with a given covariance.

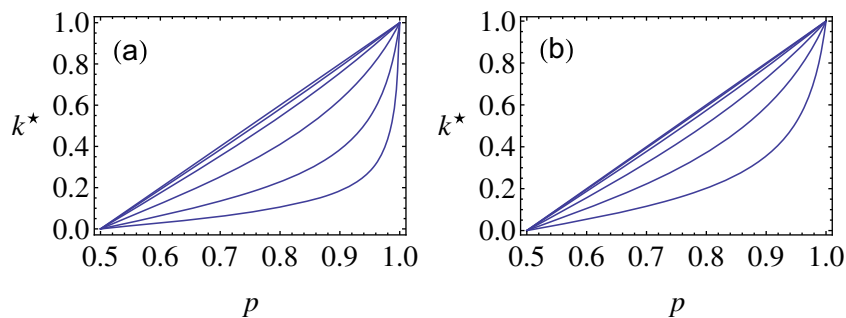


Figure 2. Plots of k^* as a function of p for different values of $\|\mathbf{r}\|$. From top to bottom in both panels: $\|\mathbf{r}\| = 0, 0.3, 0.5, 0.8, 0.95, 0.99$. In panel (a), $r_z = 0$; in panel (b), $r_z = 2r_x$.

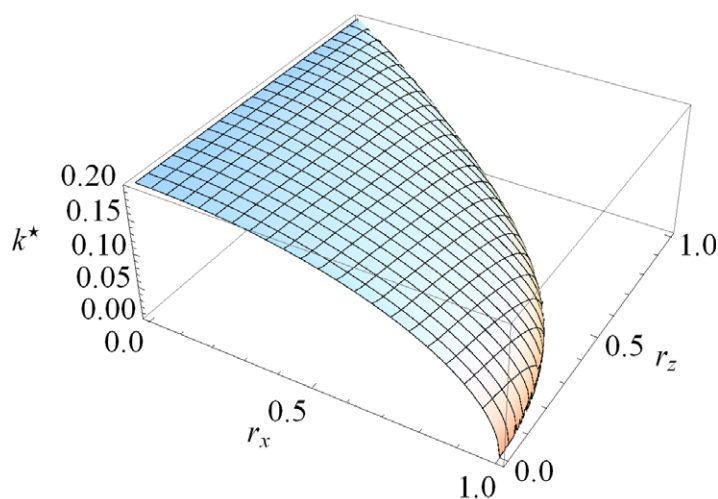


Figure 3. Plot of k^* as a function of r_x and r_z for $p = 0.6$.

The methods demonstrated in this paper provide powerful strategies for counteracting undesired noise effects in quantum memories and long-distance quantum communications, based on interfaces between discrete ensembles and continuous modes [9, 10, 13]. A further generalization of our work, worth addressing in the future, could be that of considering the optimal reversal of quantum channels acting on *correlated* copies of n qudits, possibly requiring an extension of the LAN theory beyond the paradigm of independent and identically prepared systems.

Acknowledgments

We thank M Mosonyi and N Datta for discussions. We acknowledge the University of Nottingham funding through ECRKTA/2011 and the Additional Sponsorship grant RDF/BtG/0612b/31. MG was supported by the EPSRC Fellowship EP/E052290/1.

Appendix A. Proof that the Gaussian channel G in the diagram (3) exists

Note that by the LAN construction the coordinates \mathbf{Z} and \mathbf{Z}' of the input and output Gaussian continuous variable systems have the same symplectic matrix Ω ,

$$[Z_a, Z_b] = \text{Tr}(\rho[O_a, O_b])\mathbf{1} = i\Omega_{a,b}\mathbf{1} = \text{Tr}(\rho[O'_a, O'_b]) = [Z'_a, Z'_b] \quad (\text{A.1})$$

and the covariance matrices are determined by the states ρ and $\rho' = C(\rho)$

$$\langle Z_a * Z_b \rangle = \text{Tr}(\rho O_a * O_b), \quad \langle Z'_a * Z'_b \rangle = \text{Tr}(\rho' O'_a * O'_b). \quad (\text{A.2})$$

Recall that any Gaussian channel from the input to the output is of the form

$$G^* : W_z \mapsto W_{\mathbf{X}_G z} e^{-\frac{1}{2}z^T \mathbf{Y}_G z},$$

where $\mathbf{X}_G, \mathbf{Y}_G$ are real matrices of dimension $d^2 - 1$, with \mathbf{Y}_G positive and satisfying the matrix inequality

$$\mathbf{Y}_G \geq i(\mathbf{X}_G^T \Omega \mathbf{X}_G - \Omega). \quad (\text{A.3})$$

Since the means are transformed as $\mathbf{M} \mapsto \mathbf{X}_G^T \mathbf{M}$ the matrix \mathbf{X}_G must be equal to \mathbf{X} . Moreover the output variance is

$$\mathbf{V}' = \mathbf{X}^T \mathbf{V} \mathbf{X} + \mathbf{Y}_G,$$

which determines the second matrix $\mathbf{Y}_G = \mathbf{V}' - \mathbf{X}^T \mathbf{V} \mathbf{X}$. It remains to show that \mathbf{Y}_G satisfies (A.3) which is equivalent to

$$\mathbf{V}' + i\Omega \geq \mathbf{X}^T (\mathbf{V} + i\Omega) \mathbf{X}. \quad (\text{A.4})$$

By using (A.1) and (A.2) the latter can be translated into the following property of C :

$$\tilde{\mathbf{V}}' \geq \mathbf{X}^T \tilde{\mathbf{V}} \mathbf{X}, \quad (\text{A.5})$$

where $\tilde{\mathbf{V}}'_{a,b} = \text{tr}(C(\rho) O'_a O'_b)$ and $\tilde{\mathbf{V}}_{a,b} = \text{tr}(\rho O_a O_b)$. Finally, to verify this inequality note that for all \mathbf{M}

$$\text{Tr}(\rho_{(\mathbf{M}, \lambda)} \mathbf{X}^T \mathbf{O}) = \mathbf{X}_G^T \mathbf{M} = \text{Tr}(C(\rho_{(\mathbf{M}, \lambda)}) \mathbf{O}') = \text{tr}(\rho_{(\mathbf{M}, \lambda)} C(\mathbf{O}'))$$

which implies $\mathbf{O}' = \mathbf{X}^T \mathbf{O}$. This result together with the inequality $T(A^* A) \geq T(A^*) T(A)$ valid for any channel T imply (A.5):

$$\begin{aligned} \mathbf{c}^\dagger \tilde{\mathbf{V}}' \mathbf{c} &= \sum_{a,b} c_a^* c_b \text{Tr}(C(\rho) O'_a O'_b) = \sum_{a,b} c_a^* c_b \text{Tr}(\rho C^*(O'_a O'_b)) \\ &\geq \sum_{a,b} c_a^* c_b \text{Tr}(\rho C(O'_a) C(O'_b)) \\ &= \mathbf{c}^\dagger \mathbf{X}^T \tilde{\mathbf{V}} \mathbf{X} \mathbf{c}. \end{aligned} \quad (\text{A.6})$$

Hence if C is a completely positive map then G is a Gaussian channel.

Appendix B. Proof of theorem 4.2

We need to show that the reversal of C is possible on the interval $[0, \Gamma^*]$ and not possible for $\Gamma > \Gamma^*$. Beginning with the qudit state

$$C(\rho_{(\mathbf{M}/\sqrt{n}, \lambda)})^{\otimes n} = \rho_{(\mathbf{M}'/\sqrt{n}, \lambda')}^{\otimes n},$$

where $\mathbf{M}' = \mathbf{X}_G^T \mathbf{M}$, we apply the LAN channel T_n (cf theorem 3.1) followed by H^* (cf theorem 2.1) to obtain a state which is asymptotically undistinguishable from the Gaussian state $\Phi(k^* \mathbf{M}, \mathbf{V})$. To this we apply the inverse LAN map $S_m = S_{k^{*2}n}$ to achieve the corrected state

$$R_n \left(\rho_{(\mathbf{M}'/\sqrt{n}, \lambda')}^{\otimes n} \right) = S_m \circ H^* \circ T_n \circ C^{\otimes n} \left(\rho_{(\mathbf{M}/\sqrt{n}, \lambda)} \right).$$

We first show that R_n^* is an (asymptotic) reversing channel for $\rho^{\otimes n}$:

$$\begin{aligned} \mathcal{R}_{\max}(R_n^*, \rho, \Gamma) &= \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| \rho_{(\mathbf{M}/\sqrt{n}, \lambda)}^{\otimes m} - R_n^* \left(\rho_{(\mathbf{M}'/\sqrt{n}, \lambda')}^{\otimes m} \right) \right\|_1 \\ &\leq \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| \rho_{(\mathbf{M}/\sqrt{m}, \lambda)}^{\otimes m} - S_m \left(\phi(k^* \mathbf{M}, \mathbf{V}) \right) \right\|_1 \\ &\quad + \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| S_m \left(\phi(k^* \mathbf{M}, \mathbf{V}) \right) - S_m \circ H^* \circ T_n \left(\rho_{(\mathbf{M}', \lambda')}^{\otimes n} \right) \right\|_1 \\ &\leq \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| \phi(k^* \mathbf{M}, \mathbf{V}) - H^* \circ T_n \left(\rho_{(\mathbf{M}', \lambda')}^{\otimes n} \right) \right\|_1 + o(1) \\ &= \left\| \Phi(k^* \mathbf{M}, \mathbf{V}) - H^* \left(\phi(\mathbf{M}', \mathbf{V}') \right) \right\|_1 + o(1) = o(1), \end{aligned}$$

where we have used the contractivity of the trace norm under quantum operations, the properties of LAN and the fact that H^* is a Gaussian reversing channel for G , cf (7).

We now show that it is impossible to obtain asymptotically exact reversal for $\Gamma > \Gamma^*$. Indeed, suppose there exists a sequence of reversing channels $\tilde{R}_n : M(\mathbb{C}^d)^{\otimes n} \rightarrow M(\mathbb{C}^d)^{\otimes \Gamma n}$ such that

$$\limsup_{n \rightarrow \infty} \sup_{\|\mathbf{M}\| \leq n^\epsilon} \left\| \tilde{R}_n \left(\rho_{(\mathbf{M}', \lambda')}^{\otimes n} \right) - \rho_{(k \mathbf{M}, \lambda)}^{\otimes m} \right\|_1 = 0.$$

We then use LAN again to show that there exists a G -reversing channel $T_m \circ \tilde{R}_n \circ S_n$ with rate $k > k^*$, which is impossible:

$$\begin{aligned} &\left\| T_m \circ \tilde{R}_n \circ S_n \left(\phi(\mathbf{M}', \mathbf{V}') \right) - \phi(k \mathbf{M}, \mathbf{V}) \right\|_1 \\ &\leq \left\| \tilde{R}_n \left(\rho_{(\mathbf{M}', \lambda')}^{\otimes n} \right) - \rho_{(k \mathbf{M}, \lambda)}^{\otimes m} \right\|_1 + \left\| S \left(\phi(\mathbf{M}', \mathbf{V}') \right) - \rho_{(k \mathbf{M}, \lambda)}^{\otimes m} \right\|_1 + \left\| T_m \left(\rho_{(k \mathbf{M}, \lambda)}^{\otimes m} \right) - \phi(k \mathbf{M}, \mathbf{V}) \right\|_1 \\ &= o(1). \end{aligned} \quad \square$$

References

- [1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
- [2] Breuer H P and Petruccione F 2007 *The Theory of Open Quantum Systems* (Oxford: Oxford University Press)

- [3] Wootters W K and Zurek W H 1982 *Nature* **299** 802
- [4] Keyl M and Werner R F 2001 *Ann. Henri Poincaré* **2** 1
- [5] Jenčová A 2006 *Phys. Rev. A* **74** 032305
- [6] Shirokov M E 2012 arXiv:1203.026
- [7] Jenčová A and Petz D 2006 *Commun. Math. Phys.* **263** 259
- [8] Bowles P, Guță M and Adesso G 2011 *Phys. Rev. A* **84** 022320
- [9] Cirac J I, Zoller P, Kimble H J and Mabuchi H 1996 *Phys. Rev. Lett.* **78** 3221
Simon C *et al* 2010 *Eur. Phys. J. D* **58** 1
- [10] Julsgaard B, Sherson J, Cirac J I, Fiurášek J and Polzik E S 2004 *Nature* **432** 482
Jensen *et al* 2011 *Nature Phys.* **7** 13
Hammerer K, Sørensen A S and Polzik E S 2010 *Rev. Mod. Phys.* **82** 1041
- [11] Serafini A, Mancini S and Bose S 2006 *Phys. Rev. Lett.* **96** 010503
- [12] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [13] Duan L M, Lukin M D, Cirac J I and Zoller P 2001 *Nature* **414** 413
Kimble H J 2008 *Nature* **453** 1023
- [14] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
- [15] Le Cam L 1986 *Asymptotic Methods in Statistical Decision Theory* (New York: Springer)
- [16] Young G A and Smith R L 2005 *Essentials of Statistical Inference* (Cambridge: Cambridge University Press)
- [17] Guță M and Kahn J 2006 *Phys. Rev. A* **73** 052108
- [18] Guță M, Janssens B and Kahn J 2008 *Commun. Math. Phys.* **277** 127
- [19] Kahn J and Guță M 2009 *Commun. Math. Phys.* **289** 597
- [20] Guță M and Jenčová A 2007 *Commun. Math. Phys.* **276** 341
- [21] Eisert J and Wolf M M 2007 Gaussian quantum channels *Quantum Information with Continuous Variables of Atoms and Light* ed N J Cerf, G Leuchs and E S Polzik (London: Imperial College Press) pp 23–42
- [22] Holevo A S 2007 *Problems Inform. Transm.* **43** 1
- [23] Holevo A S and Werner R F 2001 *Phys. Rev. A* **63** 032312
- [24] Serafini A, Paris M G A, Illuminati F and De Siena S 2005 *J. Opt. B: Quantum Semiclass. Opt.* **71** R19
- [25] Ivan S J, Sabapathy K K and Simon R 2011 *Phys. Rev. A* **84** 042311
- [26] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 513
- [27] Weedbrook C *et al* 2012 *Rev. Mod. Phys.* **84** 621
- [28] Eisert J and Plenio M B 2003 *Int. J. Quantum Inform.* **1** 479
- [29] Adesso G and Illuminati F 2007 *J. Phys. A: Math. Theor.* **40** 7821
- [30] Caruso F, Giovannetti V and Holevo A S 2006 *New J. Phys.* **8** 310
- [31] Datta N 2009 *IEEE Trans. Inform. Theory* **55** 2816
- [32] Owari M, Plenio M B, Polzik E S and Serafini A 2008 *New J. Phys.* **10** 113014
- [33] Mosonyi M and Datta N 2009 *J. Math. Phys.* **50** 072104
- [34] Gottesman D 2010 An introduction to quantum error correction and fault-tolerant quantum computation *Quantum Information Science and its Contributions to Mathematics (Proc. Symp. Applied Mathematics vol 68)* (Providence, RI: American Mathematical Society) p 13
- [35] Niset J, Fiurášek J and Cerf N J 2009 *Phys. Rev. Lett.* **102** 120501
- [36] Gill R D and Guță M 2011 On asymptotic quantum statistical inference *From Probability to Statistics and Back: High-Dimensional Models and Processes—A Festschrift in Honor of Jon Wellner (IMS Collections)* vol 9 pp 105–27 (arXiv:1112.2078)
- [37] Guță M 2011 *Phys. Rev. A* **83** 062324
- [38] Guță M, Bowles P and Adesso G 2010 *Phys. Rev. A* **82** 042310
- [39] Guță M and Kotlowski W 2010 *New J. Phys.* **12** 12303
- [40] Lanyon B P *et al* 2009 *Nature Phys.* **5** 134