PHYSICAL REVIEW A **70**, 030301(R) (2004)

Quantum reverse engineering and reference-frame alignment without nonlocal correlations

E. Bagan, M. Baig, and R. Muñoz-Tapia
Grup de Física Teòrica & IFAE, Facultat de Ciències, Edifici Cn, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona) Spain
(Received 17 May 2004; published 7 September 2004)

The estimation of unknown qubit elementary gates and the alignment of reference frames are formally the same problem. Using quantum states made out of N qubits, we show that the theoretical precision limit for both problems, which behaves as $1/N^2$, can be asymptotically attained with a covariant protocol that exploits the quantum correlation of internal degrees of freedom instead of the more fragile entanglement between distant parties. This cuts by half the number of qubits needed to achieve the precision of the dense covariant coding protocol.

DOI: 10.1103/PhysRevA.70.030301 PACS number(s): 03.67.Hk, 03.65.Ta

Quantum resources are scarce goods and, as such, one has to make sure they are used in the most efficient way. Optimal management of systems and resources in quantum communication and state estimation is, hence, a must. This subject has been addressed extensively in the literature but only recently for the specific type of problems that we will deal with: the estimation of unitary transformations on qubits. Given an unknown one-qubit gate (a black box) which we may apply N times over a number of qubits, we are confronted with the reverse-engineering problem of finding out the hidden SU(2) transformation performed by the gate. It was shown in Ref. [1] that the optimal estimation is attained by acting on a suitable maximally entangled state of $2N$ qubits [see Eq. (7) below] and performing a collective measurement on them. Note that in this protocol half of the qubits are left untouched before the final measurement.

Closely linked to this reverse-engineering issue is the problem of transmitting data that cannot be digitalized. This arises, for instance, when someone (Alice) attempts to transmit the direction of an arrow to a distant party (Bob) with whom there is no shared reference frame [2]. In this situation, the transmission of the information is only possible if the quantum carrier is itself an arrow of some sort (e.g., an electron, which has spin and magnetic dipole moment pointing along a specific direction). A generalization of this problem consists of transmitting the orientation of three orthogonal axes, i.e., a trihedron, which we may view as a spatial reference frame (throughout this paper we will use the word trihedron for brevity). This problem is easily seen to be formally equivalent to that of estimating a SU(2) transformation. This is not at all surprising because the group of proper rotations and SU(2) are locally isomorphic. It is important to realize that, likewise the arrow example, the carrier of the information must be a quantum system with intrinsic orientation (e.g., a hydrogen atom or a system of electrons in a sufficiently asymmetric angular momentum state), since Alice and Bob are assumed not to share any reference frame.

This problem was first tackled in Refs. [3,4] for a hydrogen atom or a system of N spins under the simplification assumption that the set of all the allowed signal states spans each SU(2) irreducible representation exactly once. The transmission error of the best covariant protocol was shown to vanish as $1/N$. This is a somewhat puzzling result, because one can easily devise noncovariant protocols that perform much better [5] (the corresponding error vanishes as $1/N^2$), despite the fact that covariance and optimality are generally regarded as compatible requirements [6].

In Ref. [7] (see also Ref. [8]), the authors introduced the (ultimate) optimal protocol for transmitting orientations using a quantum channel consisting of a system of spins. This protocol is covariant and uses entanglement much in the same way as dense coding [9,10] does by requiring Alice and Bob to share the maximal entangled state of Ref. [1] [see Eq. (7) below]. The results include the calculation of the transmission error for large N (or equivalently, the error in the optimal estimation of a unitary transformation), which shows an outstanding reduction as compared with the previously known protocols. It should be emphasized, however, that the improvement is achieved at the cost of keeping nonlocal correlations between sender and recipient which, of course, is an additional resource.

The aim of this paper is to show that we can cut down the number of spins to N and still achieve a transmission error asymptotically equal to that of the dense covariant coding protocol. We will show that this is not at odds with Ref. [7] despite the apparent contradiction with the comments in the previous paragraph. This economy of resources is mainly the result of using efficiently the Hilbert space of the N spins, which span a number of equivalent irreducible representations of SU(2), as apposed to the protocol in Ref. [3]. Note, however, that the latter is optimal if a hydrogen atom (for which no repeated representations are available [4]) is used instead of N spins. We should also stress that the present approach is entirely covariant. Thus, we resolve the covariance-optimality puzzle discussed above.

From the point of view of estimating SU(2) transformations our results also mean an equally outstanding reduction of the resources required to achieve an asymptotically optimal estimation. Let us assume that Alice has N qubits at her disposal with which she would like to either estimate an unknown SU(2) transformation or communicate to Bob the orientation of a trihedron. As mentioned above, the latter can, in principle, be achieved regardless of the existence of a shared reference frame if we choose the N qubits to be particles with spin. From now on we will always refer to these N

qubits as spins for simplicity. The most general preparation Alice can make is

$$|\Psi\rangle = \sum_{j,m,\alpha} \Psi^j_{m\alpha} |jm\alpha\rangle, \quad \sum_{j,m,\alpha} |\Psi^j_{m\alpha}|^2 = 1, \tag{1}$$

where j labels the irreducible representations of SU(2) [i.e., $j(j+1)$ are the eigenvalues of $\mathbf{J}^2$, the total angular momentum squared], m are the $2j+1$ eigenvalues of J_z—which label the elements of the standard orthonormal basis spanning the $\mathbf{j}$ representation of SU(N) of dimension $d_j = 2j+1$—and α labels the n_j different equivalent representations of spin j that show up in the Clebsch-Gordan series of $(\mathbf{1}/\mathbf{2})^{\otimes N}$. One can compute n_j to be

$$n_j = \binom{N}{N/2+j} \frac{2j+1}{N/2+j+1}. \tag{2}$$

We wish to view $|\Psi\rangle$ as a reference state to which Alice will apply the unitary operation $U(g) = u^{\otimes N}(g)$; $u(g) \in \mathbf{1}/\mathbf{2}$. Throughout this paper, g will stand for SU(2) group parameters, such as the standard Euler angles $g = (\alpha, \beta, \gamma)$. We will use the notation gg' to denote the parameters of the composition (product) $U(g)U(g') \equiv U(gg')$, and dg will stand for the Haar measure of SU(2), which is left and right invariant under the above composition, namely $d(gg') = d(g'g) = dg$, and normalized so that $\int dg = 1$.

If the operation (or one-qubit gate) $u(g)$ is unknown to Alice, she can gain some knowledge about it by applying it to $|\Psi\rangle$ to obtain a state $|\Psi(g)\rangle = U(g)|\Psi\rangle$ and by performing an appropriate measurement over $|\Psi(g)\rangle$ afterwards. We will allow Alice to perform a completely general positive operator valued measure (POVM), characterized by the set of operators $\{O_r\}$, each one of them associated to a possible outcome r. Alice can make a guess or have an estimate of the parameter g which will depend on the outcome she obtains. Let us call g_r the guess corresponding to outcome r. A quantitative assessment of Alice's performance is given by the averaged fidelity, defined as

$$\langle F \rangle = \sum_r \int dg F(g_r, g) p(r|g), \tag{3}$$

where $F(g_r, g) \equiv |\mathrm{tr}[u^\dagger(g_r)u(g)]|^2/4$ is an (squared) average over all input qubit $|\phi\rangle$ of how well $u(g_r)|\phi\rangle$ compares to $u(g)|\phi\rangle$ [1], and $p(r|g)$ is the probability of obtaining the outcome r if the unknown transformation is $u(g)$. In terms of group characters $F(g_r, g)$ can also be written as

$$F(g_r, g) = \frac{\chi^2_{1/2}(g_r^{-1}g)}{4} = \frac{1 + \chi_1(g_r^{-1}g)}{4}, \tag{4}$$

where $\chi_j(g)$ is the character of the representation $\mathbf{j}$. Quantum mechanics tell us that $p(r|g) = \mathrm{tr}[O_r \rho(g)]$, where $\rho(g) = |\Psi(g)\rangle\langle\Psi(g)|$. Note that we compute $\langle F \rangle$ assuming that the *a priori* probability for $u(g)$ is uniform with respect to the SU(2) Haar measure.

Somewhat more speculatively, Alice could also use her N spins to transmit the orientation of an orthogonal trihedron, $\mathsf{n} = \{\vec{n}^{(1)}, \vec{n}^{(2)}, \vec{n}^{(3)}\}$. In this case, she would choose the state $|\Psi\rangle$ in such a way that the system of spins had a physically observable magnitude that she could correlate to n [11] (e.g., a magnetic or electric quadrupole moment). She would simply rotate the system so that its orientation were that of n and would send it to Bob. He would then perform a generalized measurement $\{O_r\}$ and infer from the outcomes the orientation of the N-spin system and, hence, of Alice's trihedron n. Referred to an observer's reference frame $\mathsf{n}_0 = \{\vec{x}, \vec{y}, \vec{z}\}$, Alice's trihedron is $\mathsf{n}(g) = R(g)\mathsf{n}_0$, where $R(g)$ is a rotation in three-dimensional space. If $R(g)$ has the unitary representation $u(g)$, the state Alice has prepared and sent to Bob is again $|\Psi(g)\rangle$. Referred to the same frame, the trihedron $\{\vec{n}_r^{(1)}, \vec{n}_r^{(2)}, \vec{n}_r^{(3)}\}$ Bob guesses from the outcome r of his measurement should correspond to some $\mathsf{n}(g_r) = R(g_r)\mathsf{n}_0$. (Note that Bob does not know the actual value of g_r, since we assume he does not know n_0.) The quality of the transmission can, thus, be quantified through the averaged Holevo's error [3,6]

$$\langle h \rangle = \sum_r \int dg h(g_r, g) p(r|g), \tag{5}$$

where $h(g_r, g) = \Sigma_{a=1}^3 |\vec{n}^{(a)}(g_r) - \vec{n}^{(a)}(g)|^2 = 6 - 2\chi_1(g_r^{-1}g)$. This shows that the two problems we are dealing with, i.e., estimation of SU(2) transformations and transmission of frames and trihedra, are formally the same. Throughout the rest of the paper, we will concentrate in $\langle \chi_1 \rangle$

$$\langle \chi_1 \rangle = \sum_r \int dg \chi_1(g_r^{-1}g) \mathrm{tr}[O_r \rho(g)], \tag{6}$$

from which we immediately obtain either $\langle F \rangle = (1 + \langle \chi_1 \rangle)/4$ or $\langle h \rangle = 6 - 2\langle \chi_1 \rangle$, depending on the problem we are interested in. Our conclusions directly apply to the two problems above, which we may simply regard as two different aspects of the same topic.

As mentioned in the introductory comments, the optimal scheme (the one that leads to the maximal $\langle \chi_1 \rangle$) requires the signal state to be the maximally entangled $2N$-spin state

$$|\Phi\rangle = \sum_j a_j |\Phi^j\rangle \equiv \sum_j \frac{a_j}{\sqrt{d_j}} \sum_{m=-j}^{j} |jm\rangle_A |jm\rangle_B, \tag{7}$$

where j runs from the highest total spin $J \equiv N/2$ to $1/2$ (0) for N odd (even), and the action of SU(2) to be

$$U(g) = U_A(g) \otimes \mathbb{I}_B = [u(g)]_A^{\otimes N} \otimes \mathbb{I}_B, \tag{8}$$

where A refers to the first N (active) spins and B to the other N (spectator) spins (in the dense covariant coding approach of Ref. [7], A and B refer to Alice and Bob, respectively). Within this framework we obtain for large N [7]

$$\langle \chi_1^{\mathrm{entgl}} \rangle = 3 - \frac{4\pi^2}{N^2} + \frac{24\pi^2}{N^3} + \ldots. \tag{9}$$

We now realize that we can make do with just N spins if we replace the d_j degrees of freedom involved in each one of the $|jm\rangle_B$ by those corresponding to the multiplicity of the equivalent representations $\mathbf{j}$ in Eq. (1). More precisely, we assign to each m a unique α [see Eq. (1)], which we denote

by α_m, and entangle these two degrees of freedom. Clearly, the quantum correlations of Eq. (7) are exactly those of $|\Psi\rangle=\Sigma_j a_j|\Psi^j\rangle$, where

$$|\Psi^j\rangle = \frac{1}{\sqrt{d_j}}\sum_{m=-j}^{j}|jm\alpha_m\rangle. \tag{10}$$

It is important to note that this entanglement of degrees of freedom can be established in any of the **j** invariant subspaces but in the **J** subspace (the one corresponding to the highest spin, $N/2$), since Eq. (2) implies $n_j \geqslant d_j$ if $j<J$ and $n_J=1$. Hence $|\Phi^j\rangle$ and $|\Psi^j\rangle$ have the same entanglement for $j<J$, whereas $|\Psi^J\rangle=\Sigma_m \Psi^J_m|Jm\rangle$ has no entanglement at all (the **J** representation occurs only once in the Clebsch-Gordan series of $\mathbf{1}/\mathbf{2}^{\otimes N}$). It is also important to note that the index α that labels the equivalent representations does not transform under SU(2). Hence, the action of this group over $|\Psi\rangle$ is still given by Eq. (8), where now B refers to the "α degrees of freedom."

We would like to stress that the n_j-d_j equivalent representations that do not show up in Eq. (10) are actually sterile. They cannot be used for the problems at hand, as shown by the following argument. The action of Eq. (8) on a general state belonging to the direct sum of all the equivalent representations **j** yields $|w(u)\rangle=\Sigma_{m\alpha}w_{m\alpha}u^{\otimes N}|jm\alpha\rangle$. Let $|\phi\rangle=\Sigma_{m'\alpha'}\phi_{m'\alpha'}|jm'\alpha'\rangle$ be another state belonging to the same subspace. We have $\langle\phi|w(u)\rangle=\Sigma_{mm'}(\Sigma_\alpha \phi^*_{m'\alpha}w_{m\alpha})\mathfrak{D}^{(j)}_{mm'}(u)$, where $\mathfrak{D}^{(j)}_{mm'}$ is the standard d_j-dimensional unitary matrix representation of SU(2). We can find at least n_j-d_j (n_j-dimensional) "vectors" $(\eta_{a1},\eta_{a2},\eta_{a3},\ldots)$, $a=1,2,\ldots,n_j-d_j$ orthogonal to all the d_j "vectors" $(w_{m1},w_{m2},w_{m3},\ldots)$, $m=-j,-j+1,\ldots,j$. Defining $\phi_{m\alpha}=\varphi_{pm}\eta_{a\alpha}$, where the complex numbers φ_{pm}, $p=1,2,\ldots,d_j$, are chosen so that $\Sigma_m\varphi^*_{pm}\varphi_{qm}=\delta_{pq}$, we see that the orthogonal complement of $\{|w(u)\rangle\}_{u\in SU(2)}$ has at least dimension $d_j(n_j-d_j)$, since $\langle\phi|w(u)\rangle=0$ for all $u\in$ SU(2). Hence, the signal state can span at most d_j **j**-invariant subspaces.

Keeping all the above in mind and recalling from Ref. [3] that $|JJ\rangle$ is optimal when only one of the equivalent representations **j** is allowed, it is tempting to state that

$$|\Psi_{\{a\}}\rangle = a_J|JJ\rangle + \sum_{j<J}\frac{a_j}{\sqrt{d_j}}\sum_{m=-j}^{j}|jm\alpha_m\rangle \tag{11}$$

is optimal for both the estimation of SU(2) transformations and the transmission of frames (for a suitable set of real coefficients $\{a\}$ obeying $\Sigma_j|a_j|^2=1$). This is not entirely (but almost) right because of the small asymmetry introduced by the highest spin component $|\Psi^J\rangle$. However, we will show below that the maximal $\langle\chi_1\rangle$ we can obtain using Eq. (11) differs from the optimal one (9) only by terms that vanish asymptotically as $1/N^3$. This means that N spins suffice to asymptotically attain the dense covariant coding bound, which uses $2N$ spins.

We first show that a continuous rank one POVM does exist for signal states of the type (11). Using Schur's lemma, one can readily see that

$$\int dg U(g)O^jU^\dagger(g) = \frac{\mathbb{I}^j_A\otimes \mathrm{tr}_A O^j}{d_j} \tag{12}$$

over each irreducible subspace of SU(2) of dimension d_j. Here tr_A is the partial trace over subsystem A (the "m degrees of freedom"). If O^j is rank one, we have $O^j=d_j^2|\phi^j\rangle\langle\phi^j|$ and (12) is $\mathbb{I}$ only if $\mathrm{tr}_A(|\phi^j\rangle\langle\phi^j|)=\mathbb{I}^j_B/d_j$, which implies that $|\phi^j\rangle$ is a maximally entangled state over each irreducible representation (except **J**). We may choose it to be of the form (11) without any loss of generality. Hence, the continuous POVM is

$$O(g) = U(g)|\Psi_{\{b\}}\rangle\langle\Psi_{\{b\}}|U^\dagger(g), \tag{13}$$

where $|\Psi_{\{b\}}\rangle$ is defined as in Eq. (11), and the set $\{b\}$ is given by $b_j=d_j$ for $j<J$, $b_J=\sqrt{d_J}$. POVMs with a finite number of outcomes can also be found following [3].

We are now in the position to compute $\langle\chi_1\rangle$ for the signal states (11). This will provide a lower bound for $\langle\chi_1^{\mathrm{opt}}\rangle$, the averaged χ_1 of the optimal N-spin scheme. Recalling the invariance of dg and Schur's lemma one gets

$$\begin{aligned}\langle\chi_1\rangle &= \int dg\int dg'\,\chi_1(g^{-1}g')\mathrm{tr}[O(g)\rho(g')]\\ &= \int dg\int dg'\,\chi_1(g^{-1}g')\mathrm{tr}[|\Psi_{\{b\}}\rangle\langle\Psi_{\{b\}}|\rho(g^{-1}g')]\\ &= \int dg\chi_1(g)|\langle\Psi_{\{a\}}|U(g)|\Psi_{\{b\}}\rangle|^2\\ &= \frac{1}{3}\sum_{jl}a^jb^l[b^jb^l\,\mathrm{tr}_1(\rho^j\otimes\tilde{\rho}^l)],\end{aligned} \tag{14}$$

where we have defined the operators ρ^j and $\tilde{\rho}^l$ through the relations $\Sigma_j a^jb^j\rho^j=\mathrm{tr}_B(|\Psi_{\{b\}}\rangle\langle\Psi_{\{a\}}|)$ and $\Sigma_l a^lb^l\tilde{\rho}^l=\mathrm{tr}_B(|\tilde{\Psi}_{\{b\}}\rangle\times\langle\tilde{\Psi}_{\{a\}}|)$. The state $|\tilde{\Psi}_{\{a\}}\rangle$ is the transformed of $|\Psi_{\{a\}}\rangle$ under time reversal and tr_1 is the trace over the representation **1** invariant subspace, i.e., $\mathrm{tr}_1 O=\Sigma_{m=-1}^1\langle 1m|O|1m\rangle$. For $j<J$ we see that $\rho^j=\tilde{\rho}^j=\mathbb{I}^j/d_j$, whereas $\rho^J=|JJ\rangle\langle JJ|$ and $\tilde{\rho}^J=|J-J\rangle\langle J-J|$. Using that

$$\mathrm{tr}_1(|jm\rangle\langle jm'|\otimes\mathbb{I}^l) = \frac{3\delta_{mm'}}{d_j} \tag{15}$$

for $j+l\geqslant 1\geqslant|j-l|$ (it vanishes otherwise), along with $d_J\langle JJ;J-J|10\rangle^2=3J/(J+1)$, we obtain

$$\langle\chi_1\rangle = 1+\mathsf{a}^t\mathsf{M}\mathsf{a}, \tag{16}$$

where $\mathsf{a}^t=(a^J,a^{J-1},\ldots)$ is the transpose of a, and M is the $n\times n$ tridiagonal matrix

$$\mathsf{M}=\begin{pmatrix} \frac{-1}{J+1} & \frac{1}{\sqrt{d_J}} & & & & & & \\ \frac{1}{\sqrt{d_J}} & 0 & 1 & & & \underline{0} & & \\ & 1 & 0 & 1 & & & & \\ & & 1 & \ddots & \ddots & & & \\ & & & \ddots & & 1 & & \\ & \underline{0} & & & 1 & 0 & 1 & \\ & & & & & 1 & 0 & \end{pmatrix}, \quad (17)$$

where here and throughout the rest of the paper we will only consider N odd (J half-integer, $n=J+1/2$) for simplicity. The maximum value of $\langle\chi_1\rangle$ is

$$\langle\chi_1\rangle = 1 - 2\lambda_0, \quad (18)$$

where $-2\lambda_0$ is the largest eigenvalue of M. This can be computed easily by noticing that the characteristic polynomial of M, defined to be $P_n^J(\lambda)=\det(\mathsf{M}+2\lambda\mathbb{I})$, satisfies the recursive relation of the Tchebychev polynomials [12], namely, $P_n^J(\lambda)=2\lambda P_{n-1}^J(\lambda)-P_{n-2}^J(\lambda)$. Hence, $P_n^J(\lambda)$ is a linear combination of them. One can check that the explicit solution is

$$P_n(\lambda) = U_n(\lambda) - \frac{2}{2n+1}U_{n-1}(\lambda) + \frac{2n-1}{2n}U_{n-2}(\lambda), \quad (19)$$

where we have defined $P_n(\lambda)\equiv P_n^{n-1/2}(\lambda)$ and $U_n(\cos\theta)=\sin[(n+1)\theta]/\sin\theta$ are the Tchebychev polynomials of the second kind. Hence, the smallest zero of $P_n(\lambda)$, which is $\lambda_0\equiv\cos\theta_0$ in Eq. (18), can be easily computed in the large n limit expanding around $\lambda_0=-1$, i.e, $\theta_0=\pi(1-n^{-1}+an^{-2}+bn^{-3}+\ldots)$. We find

$$\langle\chi_1\rangle = 3 - \frac{4\pi^2}{N^2} + \frac{8\pi^2}{N^3} + \ldots . \quad (20)$$

Recalling that $\langle\chi_1\rangle\leqslant\langle\chi_1^{\mathrm{opt}}\rangle\leqslant\langle\chi_1^{\mathrm{entgl}}\rangle$ and Eq. (9), we conclude that

$$\chi_1^{\mathrm{opt}} = 3 - \frac{4\pi^2}{N^2} + O(1/N^3). \quad (21)$$

Therefore, the theoretical limit imposed by Eq. (9) is asymptotically reached with just half the number of spins and without nonlocal correlations being shared between Alice and Bob. Very recently, the same result has been derived from a maximum likelihood approach [13] (see also Ref. [14]).

In summary, the internal "α" degrees of freedom associated to repeated irreducible representations in the Clebsch-Gordan series of $(\mathbf{1}/\mathbf{2})^{\otimes N}$ do not transform under the SU(2) group or rotations and, therefore, they are not directly useful to encode such transformations. However, they can be entangled to proper SU(2) degrees of freedom, such as m, to yield an outstanding improvement over some previously known estimation and communication protocols. This entanglement is formally the same as that of dense covariant coding, but it is achieved with half the number of spins and without preestablished quantum correlations between distant parties. Furthermore, since these degrees of freedom are invariant under rotations, the resulting protocol is manifestly covariant.

We acknowledge financial support from Spanish Ministry of Science and Technology project BFM2002-02588, CIRIT project SGR-00185, and QUPRODIS working group EEC Contract No. IST-2001-38877. RMT acknowledges the hospitality of the Quantum Information Theory group at Pavia.

[1] A. Acin, E. Jane, and G. Vidal, Phys. Rev. A **64**, 050302 (2001).

[2] E. Bagan *et al.*, Phys. Rev. Lett. **85**, 5230 (2000); Phys. Rev. A **63**, 052309 (2001); A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001); E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **64**, 022305 (2001).

[3] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. Lett. **87**, 257903 (2001).

[4] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001).

[5] A. Peres and P. F. Scudo, J. Mod. Opt. **49**, 1235 (2002).

[6] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North Holland, Amsterdam, 1982).

[7] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **69**, 050303 (2004).

[8] M. Hayashi, *Proceedings of the IX Quantum Information Technology Symposium*, QIT9 (NTT Basic Research Laboratories, Atsugi, Kangawa, Japan, 2003), pp. 9–13.

[9] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[10] G. M. D'Ariano, P. LoPresti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).

[11] N. H. Lindner, A. Peres, and D. R. Terno, Phys. Rev. A **68**, 042308 (2003).

[12] M. Abramowitz and I. S. Stegun, *Handbook of Mathematical Functions* (Dover, New York 1972).

[13] G. Chiribella *et al.*, e-print quant-ph/0405095.

[14] M. Hayashi, Proceedings of the 7th International Conference on Quantum Communication, Measurement and Computing, QCMC04 (Glasgow, UK, 2004), AIP Conf. Proc. (to be published).